





Universitat Autònoma de Barcelona

ADVERTIMENT. L'accés als continguts d'aquesta tesi queda condicionat a l'acceptació de les condicions d'ús establertes per la següent llicència Creative Commons:  http://cat.creativecommons.org/?page_id=184

ADVERTENCIA. El acceso a los contenidos de esta tesis queda condicionado a la aceptación de las condiciones de uso establecidas por la siguiente licencia Creative Commons:  <http://es.creativecommons.org/blog/licencias/>

WARNING. The access to the contents of this doctoral thesis it is limited to the acceptance of the use conditions set by the following Creative Commons license:  <https://creativecommons.org/licenses/?lang=en>



Tesis doctoral:

La gestión del riesgo aplicada a la gestión de documentos y su impacto en la rendición de cuentas pública

Autora: Anahí Casadesús de Mingo

Directora: Remei Perpinyà Morera

Programa de Doctorado en Historia Comparada, Política y Social

Línea de investigación: Gestión Documental

Departamento de Historia Moderna y Contemporánea

Universitat Autònoma de Barcelona

2018

UAB

**Universitat Autònoma
de Barcelona**

Tesis doctoral:

La gestión del riesgo aplicada a la gestión de documentos y su impacto en la rendición de cuentas pública

Autora: Anahí Casadesús de Mingo

Directora: Remei Perpinyà Morera

Programa de Doctorado en Historia Comparada, Política y Social

Línea de investigación: Gestión Documental

Departamento de Historia Moderna y Contemporánea

Universitat Autònoma de Barcelona

2018



* Imagen portada: Joel Filipe

* Diseño gráfico: numarta

This report, by its very length, defends itself against the risk of being read.

(Wiston Churchill)

Índice

Índice de figuras	p. 6
Agradecimientos.....	p. 10
Introducción	p. 11
Capítulo 1.	
Marco teórico de la gestión documental	p. 18
1.1 El concepto de documento.....	p. 19
1.1.1 Propiedades del documento de archivo.....	p. 24
1.2 El ciclo de vida y la teoría del <i>Records continuum</i>	p. 25
1.3 La gestión de documentos.....	p. 30
1.3.1 Procesos de gestión documental.....	p. 33
1.3.2 Instrumentos de gestión documental.....	p. 38
1.4 Transversalidad de la gestión documental	p. 43
1.5 Normalización y certificación de la gestión de documentos	p. 46
Capítulo 2.	
Marco teórico y metodológico de la gestión de riesgos documentales	p. 49
2.1 Estándares de gestión del riesgo.....	p. 52
2.2 El proceso de gestión del riesgo.....	p. 54
2.2.1 Comunicación y consulta	p. 57
2.2.2 Establecimiento del contexto.....	p. 58
2.2.3 Apreciación del riesgo (<i>Risk assessment</i>)	p. 60
2.2.4 Tratamiento del riesgo	p. 68
2.2.5 Seguimiento y revisión	p. 70
2.2.6 Documentación del proceso de gestión del riesgo.....	p. 70
2.3 Enfoques para la identificación de riesgos documentales.....	p. 73
2.3.1 Metodología de identificación de riesgos propuesta por la organización ARMA.....	p. 74
2.3.2 Metodología de identificación de riesgos propuesta por ISO en el informe técnico ISO/TR 18128.....	p. 83
2.3.3 Comparativa entre las metodologías ARMA e ISO.....	p. 90
2.4 Implementación y mejora del proceso de gestión de riesgos documentales.....	p. 92
Capítulo 3.	
Marco teórico de la Transparencia y la Rendición de cuentas.....	p. 97
3.1 Transparencia	p. 97
3.1.1 El principio de publicidad	p. 100
3.1.2 Tipos de transparencia.....	p. 104
3.2 Rendición de cuentas.....	p. 108
3.2.1 Fases de la rendición de cuentas	p. 116
3.2.2 Tipos de rendición de cuentas	p. 117
3.3 Gestión documental, transparencia y rendición de cuentas.....	p. 124

Capítulo 4.

Análisis de las percepciones de los profesionales sobre la gestión de riesgos documentales a través de la metodología del <i>Focus Group</i>	p. 129
4.1 Propuesta y Objetivos	p. 130
4.2 Composición de los grupos	p. 131
4.3 Participación	p. 139
4.4 Análisis y Resultados	p. 140
4.4.1 Análisis del debate – Grupo A	p. 141
4.4.2 Análisis del debate – Grupo B	p. 150
4.4.3 Análisis comparativo entre los grupos A y B	p. 160

Capítulo 5.

La gestión de riesgos documentales en una administración pública: metodología, aplicación y resultados	p. 164
5.1 Metodología	p. 165
5.2 Fase 1. Contexto	p. 169
5.2.1 Análisis preliminar: Entrevistas	p. 169
5.2.2 Descripción de la Organización X	p. 175
5.2.3 Estructura organizativa	p. 178
5.2.4 Descripción de las metodologías de gestión de riesgos existentes en la Organización X	p. 183
5.2.5 Sistema de Gestión Documental	p. 187
5.3 Fase 2. Apreciación del riesgo	p. 190
5.3.1 Identificación de riesgos documentales	p. 190
5.3.2 Análisis de riesgos	p. 208
5.3.3 Evaluación de riesgos	p. 238
5.4 Fase 3. Propuesta para el tratamiento del riesgo	p. 251
5.5 Fase 4. Propuesta de seguimiento y revisión	p. 261
5.6 Documentación del proceso	p. 265
5.6.1 Visualización de los datos	p. 294
5.7 Valoración y resultados	p. 301
Conclusiones	p. 304
Aportaciones de la investigación	p. 308

Bibliografía	p. 312
---------------------------	--------

Anexo A.

Consentimiento Informado	p. 331
---------------------------------------	--------

Anexo B.

Documento para la comunicación previa a las partes interesadas	p. 332
---	--------

Anexo C.

Transcripción no literal de las entrevistas semi-estructuradas	p. 333
---	--------

Índice de figuras

Figura 1 - Relaciones entre los ámbitos de estudio de la investigación.....	p. 12
Figura 2 - Ciclo de vida de los documentos	p. 27
Figura 3 - <i>Records Continuum</i>	p. 28
Figura 4 - Proceso de gestión del riesgo	p. 56
Figura 5 - Enfoques para la identificación y gestión de riesgos de información y documentos	p. 63
Figura 6 - Fortalezas y debilidades de los enfoques de identificación de riesgos según Lemieux	p. 64
Figura 7 - Factores para el análisis de riesgos	p. 65
Figura 8 - Ejemplo de una entrada de un registro de riesgos	p. 72
Figura 9 - Cuadrante de riesgos según la metodología ARMA	p. 74
Figura 10 - Múltiples capas de contexto de los documentos y los procesos de gestión documental en una organización.....	p. 83
Figura 11 - Modelo conceptual de la transparencia según Schnackenberg	p. 99
Figura 12 - Diagrama de Venn - Cuatro direcciones de la transparencia	p. 105
Figura 13 - Proceso de rendición de cuentas pública según Bovens	p. 110
Figura 14 - Los pilares de la rendición de cuentas según Schedler	p. 112
Figura 15 - Transparencia vertical	p. 118
Figura 16 - Transparencia horizontal	p. 118
Figura 17 - Transparencia diagonal	p. 119
Figura 18 - Transparencia transnacional	p. 119
Figura 19 - Transparencia recursiva	p. 120
Figura 20 - Tipos de rendición de cuentas según Bovens	p. 121
Figura 21 - Tipos de rendición de cuentas según Lindberg	p. 122
Figura 22 - Comparativa entre años de experiencia para el Grupo A	p. 134
Figura 23 - Formación de los participantes del Grupo A	p. 134
Figura 24 - Comparativa entre años de experiencia para el Grupo B	p. 136
Figura 25 - Formación de los participantes del Grupo B	p. 137
Figura 26 - Correlación entre preguntas y objetivos para el <i>Focus Group</i>	p. 139
Figura 27 - Participantes del Grupo A	p. 141
Figura 28 - Participantes del Grupo B	p. 151
Figura 29 - Correlación entre objetivos y preguntas de las entrevistas estructuradas	p. 171
Figura 30 - Correlación entre la metodología de gestión del riesgo ISO y la metodología de prevención de riesgos laborales de la Organización X	p. 184
Figura 31 - Correlación entre la metodología de gestión del riesgo ISO y la metodología de gestión del riesgo según el Plan de adecuación al ENS de la Organización X.....	p. 185
Figura 32 - Correlación entre las metodologías de gestión del riesgo de la Organización X.....	p. 186
Figura 33 - Identificación de riesgos documentales de la Organización X siguiendo la Técnica A	p. 192
Figura 34 - Número de apariciones de cada riesgo identificado según la Técnica A	p. 194
Figura 35 - Identificación de riesgos documentales de la Organización X siguiendo la Técnica R	p. 199

Figura 36 - Número de apariciones de cada riesgo identificado según la Técnica R p. 202

Figura 37 - Comparación de la recurrencia según la técnica empleada p. 203

Figura 38 - Riesgos identificados y técnica empleada p. 204

Figura 39 - Líneas de recurrencia en la identificación de riesgos según la técnica empleada p. 205

Figura 40 - Desviación típica y real entre las Técnicas A y R p. 206

Figura 41 - Ejemplo de una matriz de consecuencia/probabilidad p. 209

Figura 42 - Niveles de probabilidad p. 211

Figura 43 - Niveles de consecuencia p. 211

Figura 44 - Matriz de consecuencia/probabilidad p. 212

Figura 45 - Niveles de riesgo p. 212

Figura 46 - Análisis de riesgos de la Organización X siguiendo la matriz de consecuencia/probabilidad p. 213

Figura 47 - Niveles de riesgo de la Organización X p. 214

Figura 48 - Distribución de porcentajes según el nivel de riesgo p. 215

Figura 49 - Ejemplo de un diagrama de pajarita p. 216

Figura 50 - Controles de prevención existentes en la Organización X p. 218

Figura 51 - Controles correctivos existentes en la Organización X p. 219

Figura 52 - Análisis de pajarita para el riesgo 1 p. 220

Figura 53 - Análisis de pajarita para el riesgo 2 p. 220

Figura 54 - Análisis de pajarita para el riesgo 3 p. 221

Figura 55 - Análisis de pajarita para el riesgo 4 p. 221

Figura 56 - Análisis de pajarita para el riesgo 5 p. 222

Figura 57 - Análisis de pajarita para el riesgo 6 p. 222

Figura 58 - Análisis de pajarita para el riesgo 7 p. 223

Figura 59 - Análisis de pajarita para el riesgo 8 p. 223

Figura 60 - Análisis de pajarita para el riesgo 9 p. 224

Figura 61 - Análisis de pajarita para el riesgo 10 p. 224

Figura 62 - Análisis de pajarita para el riesgo 11 p. 225

Figura 63 - Análisis de pajarita para el riesgo 12 p. 225

Figura 64 - Análisis de pajarita para el riesgo 13 p. 226

Figura 65 - Análisis de pajarita para el riesgo 14 p. 226

Figura 66 - Análisis de pajarita para el riesgo 15 p. 227

Figura 67 - Análisis de pajarita para el riesgo 16 p. 227

Figura 68 - Análisis de pajarita para el riesgo 17 p. 228

Figura 69 - Análisis de pajarita para el riesgo 18 p. 228

Figura 70 - Análisis de pajarita para el riesgo 19 p. 229

Figura 71 - Análisis de pajarita para el riesgo 20 p. 229

Figura 72 - Análisis de pajarita para el riesgo 21 p. 230

Figura 73 - Análisis de pajarita para el riesgo 22 p. 230

Figura 74 - Análisis de pajarita para el riesgo 23 p. 231

Figura 75 - Análisis de pajarita para el riesgo 24 p. 231

Figura 76 - Análisis de pajarita para el riesgo 25	p. 232
Figura 77 - Análisis de pajarita para el riesgo 26	p. 232
Figura 78 - Análisis de pajarita para el riesgo 27	p. 233
Figura 79 - Listado general de causas identificadas	p. 234
Figura 80 - Recurrencia de las causas identificadas, con valor medio.....	p. 235
Figura 81 - Listado general de consecuencias identificadas	p. 236
Figura 82 - Recurrencia de las consecuencias identificadas, con valor medio	p. 237
Figura 83 - Comparación entre el número y el valor de las causas.....	p. 240
Figura 84 - Comparación entre el número y el valor de las consecuencias.....	p. 242
Figura 85 - Evaluación de riesgos	p. 243
Figura 86 - Valor y prioridad del riesgo definidos por la Organización X	p. 245
Figura 87 - Correspondencia entre los valores de riesgo y la prioridad de tratamiento	p. 245
Figura 88 - Correspondencia entre la prioridad definida en el estudio de caso y la definida por la Organización X	p. 246
Figura 89 - Evaluación de riesgos documentales de la Organización X	p. 247
Figura 90 - Distribución de porcentajes según el valor del riesgo	p. 248
Figura 91 - Comparación de porcentajes entre niveles y valores del riesgo	p. 248
Figura 92 - Comparación entre valores y niveles del riesgo	p. 249
Figura 93 - Tipos de acciones preventivas definidas por la Organización X	p. 252
Figura 94 - Acciones preventivas sobre las causas de riesgo con mayor recurrencia.....	p. 255
Figura 95 - Cronograma de tratamiento de las causas de riesgo	p. 256
Figura 96 - Acciones preventivas sobre los riesgos	p. 259
Figura 97 - Cronograma para el tratamiento de riesgos	p. 260
Figura 98 - Cronograma para el tratamiento y revisión de las causas de riesgo	p. 263
Figura 99 - Cronograma del tratamiento y revisión de riesgos	p. 264
Figura 100 - Ficha de riesgo	p. 266
Figura 101 - Ficha del riesgo 1	p. 267
Figura 102 - Ficha del riesgo 2	p. 268
Figura 103 - Ficha del riesgo 3.....	p. 269
Figura 104 - Ficha del riesgo 4	p. 270
Figura 105 - Ficha del riesgo 5	p. 271
Figura 106 - Ficha del riesgo 6.....	p. 272
Figura 107 - Ficha del riesgo 7	p. 273
Figura 108 - Ficha del riesgo 8.....	p. 274
Figura 109 - Ficha del riesgo 9.....	p. 275
Figura 110 - Ficha del riesgo 10.....	p. 276
Figura 111 - Ficha del riesgo 11	p. 277
Figura 112 - Ficha del riesgo 12	p. 278
Figura 113 - Ficha del riesgo 13	p. 279
Figura 114 - Ficha del riesgo 14.....	p. 280
Figura 115 - Ficha del riesgo 15	p. 281

Figura 116 - Ficha del riesgo 16	p. 282
Figura 117 - Ficha del riesgo 17	p. 283
Figura 118 - Ficha del riesgo 18	p. 284
Figura 119 - Ficha del riesgo 19	p. 285
Figura 120 - Ficha del riesgo 20	p. 286
Figura 121 - Ficha del riesgo 21	p. 287
Figura 122 - Ficha del riesgo 22	p. 288
Figura 123 - Ficha del riesgo 23	p. 289
Figura 124 - Ficha del riesgo 24	p. 290
Figura 125 - Ficha del riesgo 25	p. 291
Figura 126 - Ficha del riesgo 26	p. 292
Figura 127 - Ficha del riesgo 27	p. 293
Figura 128 - Mapa de relaciones entre los riesgos documentales identificados	p. 295
Figura 129 - Visualización de las relaciones entre riesgos	p. 300
Figura 130 - Aportaciones de la gestión de riesgos documentales	p. 308
Figura 131 - Índice de entrevistas realizadas en la Organización X	p. 333

Agradecimientos

Agradezco a mi directora, Remei Perpinyà, el apoyo y los consejos recibidos durante estos años (sobre todo en la intensidad de los últimos meses). Agradezco a los miembros de las comisiones de doctorado, Alfred Mauri y M^a José Recoder, sus ideas y su energía en este largo periodo. Agradezco a los compañeros y la dirección de la Escuela Superior de Archivística y Gestión de Documentos su apoyo desde el inicio. En especial, a Ramon Alberch, por la confianza depositada en mí desde el primer momento, por todo lo compartido y todo lo aprendido, que me ha permitido crecer como persona y como profesional.

Agradezco a la Organización X la aceptación y la colaboración en el desarrollo del estudio de caso de esta investigación. Agradezco también a los participantes de los debates llevados a cabo su gran disposición y generosidad. Pese al anonimato, tenéis un protagonismo muy importante.

Gracias Betty y Numa, sin vosotras el resultado no sería el mismo. Claudia, gracias por darme el mejor consejo en el mejor momento posible. A todos los demás (ya sabéis quienes sois) gracias por la enorme paciencia y por seguir ahí pese a mi poca disponibilidad.

Françoise y Jordi os agradezco también vuestro apoyo desde la distancia en estos meses.

Por último, mamá, papá, Xavi y Enric, no tengo palabras para expresar mi agradecimiento por **todo** en estos años en que mi vida solo ha sido, prácticamente, doctorado y pese a la contradicción de no querer hablar nunca de ello. Cualquier intento de plasmar por escrito el agradecimiento que siento se quedaría corto.

¡Mil gracias a todos, de corazón!

Introducción

La presente investigación se centra en el estudio, teórico y práctico, de la metodología de gestión del riesgo aplicada a la gestión de documentos y cómo puede afectar esta integración en los procesos de rendición de cuentas pública.

La gestión documental no es una práctica aislada en las organizaciones sino, que, de manera transversal, influye y se ve influenciada por otras metodologías de gestión. Por ejemplo, la gestión de proyectos, la gestión de la calidad o la gestión de riesgos, entre otras. Por este motivo, no debe entenderse ni estudiarse la gestión de documentos de manera aislada sino, al contrario, en correspondencia con otros ámbitos de los que además puede beneficiarse.

Esta investigación tiene su primer punto de partida en la experiencia personal en diversos proyectos de consultoría, en diferentes organizaciones, tanto públicas como privadas, donde se detectaban, de manera constante, situaciones de riesgo relacionadas con la documentación y la información, que afectaban de un modo directo a su correcto funcionamiento. Estas situaciones se relacionaban con los documentos y su gestión, pero las consecuencias iban más allá, influyendo en otros ámbitos organizacionales. Por ejemplo, en cuestiones económicas, de recursos humanos, prestigio, credibilidad, cumplimiento de objetivos, entre otras.

Esta situación recurrente llevó a una reflexión teórica que, junto con los hallazgos de la experiencia profesional, descubrió un ámbito de estudio poco trabajado hasta el momento pero con un gran potencial para la profesión: la gestión de riesgos documentales. De hecho, son muy pocos los autores (Lemieux, Bearman o Hay-Gibson son algunos ejemplos) que han explorado la gestión de riesgos aplicada a la gestión de documentos, pero sus reflexiones han permitido no partir de cero. Cabe mencionar la tesis doctoral de Hay-Gibson sobre la gestión del riesgo en contextos de gestión de documentos electrónicos del año 2011. Si bien existen investigaciones sobre la seguridad de la información, la preservación digital y otras cuestiones que pueden relacionarse con riesgos documentales, no se ha encontrado un repertorio bibliográfico amplio sobre el tema de estudio ni sobre su aplicación en entornos cercanos.

Frente a este escenario, es paradójico el desarrollo de un estándar internacional dedicado exclusivamente a la gestión de riesgos documentales, como es el informe técnico ISO/TR 18128¹ publicado en el año 2014 y que engloba los procesos de identificación, análisis y evaluación de riesgos en procesos y sistemas (entendidos, según dicho informe, por cualquier aplicación de negocio que cree o almacene documentos) de gestión documental. Este estándar no se dirige exclusivamente a organizaciones de gran tamaño, sino que puede aplicarse a cualquier tipo de organización e incluso a funciones o departamentos concretos que interese controlar de manera especial. Su objetivo principal es el de proporcionar herramientas para gestionar los riesgos documentales en entornos actuales, donde los documentos y otra información estratégica de las organizaciones puede encontrarse en repositorios, bases de datos, aplicaciones web, redes sociales, aplicaciones de negocio o en la nube. El informe parte de la idea de que la identificación y la gestión de este tipo de riesgos, en este entorno global, puede conllevar beneficios significativos para las organizaciones. La existencia de este estándar implica interés en la metodología aplicada a la gestión de

¹– UNE-ISO/TR 18128. Información y documentación. Identificación y evaluación de riesgos para sistemas de documentos. Este informe es idéntico al Informe Técnico ISO/TR 18128: 2014. *Information and documentation. Risk assessment for records processes and systems.*

documentos. Pese a ello, tal y como ya se ha comentado, se conocen escasas experiencias de aplicación en organizaciones del entorno cercano.

El segundo punto de partida se corresponde con la constatación de que sin evidencias documentales no es posible llevar a cabo los procesos de rendición de cuentas. Estos se basan en la existencia y la capacidad de recuperación de la información relativa a decisiones o actividades de las organizaciones. Por tanto, sin una adecuada gestión de estas evidencias, la rendición de cuentas no resultará en un proceso riguroso y completo. De esto se deduce que la gestión documental puede mejorar los procesos de rendición de cuentas.

Para esta investigación, se partió de estas dos constataciones: la primera afirma que la metodología de gestión del riesgo es aplicable a la gestión documental y la segunda, que la gestión documental puede mejorar los procesos de rendición de cuentas.

A partir de estas, se plantearon tres hipótesis para esta investigación: una general y dos específicas. La hipótesis general plantea que la integración de la metodología de gestión del riesgo en la gestión de documentos puede contribuir, de manera indirecta, a mejorar los procesos de rendición de cuentas pública. Se parte de tres ámbitos de estudio diferenciados, que pretenden relacionarse (ver Figura 1). En primer lugar, la gestión documental, en segundo lugar, la gestión de riesgos y, en tercer lugar, la rendición de cuentas pública. Interesa estudiar las relaciones entre estos ámbitos y, sobre todo, explorar los beneficios que aportan entre sí y en conjunto.

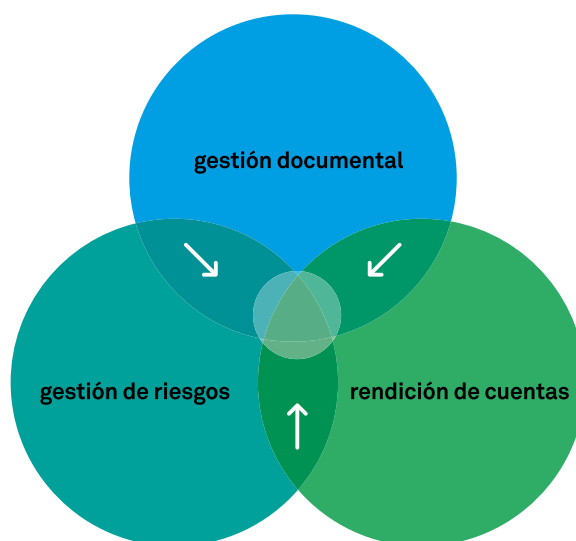


Figura 1 – Relaciones entre los ámbitos de estudio de la investigación (elaboración propia).

De esta primera hipótesis general se derivan las dos específicas. La primera hipótesis específica plantea que la gestión documental puede mejorar a través de la integración de la metodología de gestión del riesgo. La segunda hipótesis específica plantea que la gestión de riesgos puede mejorar a través de la metodología archivística y de gestión documental. Observando la reciprocidad entre estas dos metodologías, se puede profundizar sobre la hipótesis general de esta investigación.

Para trabajar en las hipótesis planteadas, se fijaron una serie de objetivos, que se presentan a continuación.

El primer objetivo general consistía en aplicar la metodología de gestión de riesgos a la gestión de documentos. Como paso previo, debía realizarse una aproximación teórica a los distintos ámbitos de estudio definidos y, en especial, a la gestión de riesgos. Se decidió partir del estudio de una metodología de gestión del riesgo normalizada y reconocida a nivel internacional, como es la recogida en los estándares internacionales de la organización ISO. Dentro de este objetivo general, se marcaron dos específicos. El primero de ellos fue identificar, analizar y evaluar los riesgos documentales de una organización real. El segundo fue proponer acciones de mejora y prevención a partir de los resultados obtenidos del primer objetivo.

No solo era importante estudiar si la metodología era aplicable, sino también tener en cuenta si realmente aportaba beneficios. De otro modo, se entendía que la investigación quedaba incompleta, al no contemplar una parte importante de la puesta en práctica de la metodología y olvidarse de la mejora continua de la gestión documental.

El segundo objetivo general se fijó en conocer la visión de los profesionales de la archivística y la gestión documental, así como de disciplinas afines, sobre la gestión de riesgos documentales. Era importante poder obtener información, de primera mano, sobre la madurez de esta metodología en la realidad archivística del entorno más cercano. También era fundamental obtener esta información desde una perspectiva multidisciplinar, incluyendo en el proceso de recopilación de información no solo expertos en gestión documental, sino expertos de otros campos de estudio que se relacionan en su día a día con la gestión de documentos, como pueden ser gestores de procesos, tecnólogos, juristas, entre otros.

El tercer objetivo general consistía en detectar mejoras de la gestión documental a partir de la integración de la metodología de gestión de riesgos. La transversalidad y adaptabilidad de la gestión documental a diferentes contextos y necesidades hace que, también, pueda beneficiarse de otras metodologías y técnicas afines, como es el caso de la gestión de riesgos. Incluir este proceso en el diseño, implantación y mantenimiento de sistemas de gestión documental podía contribuir a orientar los objetivos de manera más realista, así como a ampliar la perspectiva del gestor de documentos en relación a problemáticas que, de otro modo, probablemente no habría tenido presentes.

El cuarto objetivo general consistía en detectar mejoras para los procesos de rendición de cuentas a partir de la gestión documental. Uno de los pilares en los que se sustenta la rendición de cuentas es la existencia de información que, en las administraciones públicas, se fija en documentos (en papel o en formato electrónico). Partiendo de esta premisa, si se apuesta por incluir la gestión documental como un aspecto más de la rendición de cuentas, se puede conseguir la simplificación y optimización de este tipo de procesos.

Los objetivos 3 y 4 se relacionan entre sí, en la medida en que ambos profundizan sobre los puntos de encuentro de los ámbitos de estudio de esta investigación.

Para llevar a cabo los objetivos y trabajar las hipótesis se emplearon distintas metodologías que se explican a continuación.

El método de base empleado para la investigación fue el método archivístico, que sirvió como hilo conductor, y permitió enlazar los distintos apartados entre sí. La investigación archivística es el término usado comúnmente para referirse a la investigación que tiene como objetivo explorar cuestiones archivísticas. Algunas de estas investigaciones se centran en objetos, métodos y actividades que ya son reconocidos como parte del campo de la archivística, mientras otras investigaciones buscan incrementar el conocimiento archivístico a través de la investigación de ámbitos distintos o el uso de distintas metodologías (Duranti & Michetti, 2016, p. 80). La investigación que nos ocupa se enmarca dentro de este último grupo, y se centra en la integración de la gestión del riesgo en la metodología archivística, como un fenómeno que rodea la práctica de la gestión documental.

El conocimiento archivístico se alimenta del uso de los instrumentos de distintas disciplinas en un proceso que, de manera continua, amplía y mejora su base, sin alterarla. Esto significa que los archiveros deben estudiar conceptos, leyes y modelos de diferentes ámbitos para promover transferencias útiles a su propio ámbito, para incentivar el desarrollo de la teoría archivística en áreas emergentes de prueba e investigación, para eliminar la duplicación de esfuerzos teóricos en diferentes campos y para promover la consistencia del conocimiento científico (Duranti & Michetti, 2016, p. 83). En esta línea, el objetivo final de esta investigación es precisamente el de estudiar e integrar en la gestión documental una metodología, la gestión del riesgo, ya empleada con éxito en otros ámbitos de trabajo, como son el mercado financiero, la seguridad laboral o la seguridad de la información, entre otros.

Para ello, se debía realizar un estudio en profundidad de lo externo a la archivística y proponer una integración consistente y en línea con los principios archivísticos. Se necesitaba, no solo una propuesta individual, sino confrontar la nueva metodología con los profesionales y con la práctica real.

Para el objetivo 1 se decidió emplear la técnica del estudio de caso, que consiste en un análisis intensivo y detallado de un único caso, partiendo de una clara definición del alcance. En la selección de la organización para esta investigación se debían cumplir dos requisitos: por un lado, la existencia de un sistema de gestión documental y, por otro, el sometimiento obligatorio a la rendición de cuentas pública. Por ello, el estudio se realizó sobre un organismo público. Se definieron dos finalidades concretas. La primera era, propiamente, la de aplicar la metodología de gestión del riesgo a su gestión de documentos. La segunda consistía en analizar cómo puede afectar a los procesos de rendición de cuentas de la organización la inclusión de la gestión del riesgo en la gestión documental.

La recopilación de información para llevar a cabo este estudio siguió la metodología de triangulación. Se realizó a partir de entrevistas semi-estructuradas, el estudio de la documentación aportada y la observación directa sobre el funcionamiento de la organización.

Para el estudio de caso, se partió de la metodología explicada en los estándares ISO, concretamente en la norma UNE-ISO 31000: 2010² (en adelante, ISO 31000), el informe técnico UNE-ISO 18128: 2014 (en adelante ISO 18128) y la norma UNE-ISO 31010: 2011³ (en adelante, ISO 31010). La primera es la norma general de gestión del riesgo, que se complementa con la segunda, que es la específica de riesgos sobre procesos y aplicaciones informáti-

² – UNE-ISO 31000: 2010. Gestión del riesgo. Principios y directrices. Esta norma es idéntica a la Norma Internacional ISO 31000: 2009.

³ – UNE-EN 31010: 2011. Gestión del riesgo. Técnicas de apreciación del riesgo. Esta norma es la versión oficial, en español, de la Norma Euro pe a EN 31010: 2010 que a su vez adopta la Norma Internacional ISO/IEC 31010: 2009.

cas para la gestión de documentos. En estos dos estándares se da una explicación del proceso y las diferentes fases de la gestión del riesgo, que son las que se han seguido para el estudio de caso. Por último, la norma ISO 31010 consiste en un conjunto de técnicas para llevar a cabo el proceso de gestión del riesgo. Se realizó una selección de aquellas que se ajustaban mejor a la gestión de documentos y al contexto organizativo del organismo seleccionado, para aplicarse en el estudio de caso. Cabe mencionar que, durante la realización de esta investigación, la norma ISO 31000 sufrió un proceso de revisión, siendo publicada una nueva versión en el mes de febrero de 2018. No han podido incluirse los cambios realizados en la investigación, pero será necesario tenerlos en cuenta para posteriores estudios.

Este estudio de caso debe entenderse como un punto de partida para el desarrollo de posteriores aplicaciones. Cabe destacar que la organización solicitó de manera expresa la preservación de su anonimato en la realización del estudio y la publicación de resultados.

Para el objetivo 2, se decidió emplear la metodología del *Focus Group*, que consiste en una entrevista con varias personas sobre un tema o problema concreto. La finalidad era la de profundizar y debatir sobre la gestión de riesgos documentales desde una perspectiva multidisciplinar. Por este motivo, se realizaron dos debates, con profesionales de perfiles distintos. El primer grupo estuvo formado por una serie de expertos en gestión documental y archivos con trayectorias profesionales amplias, pero en tipos de archivo distintos. El segundo grupo estuvo formado por un grupo multidisciplinar de perfiles, con un amplio conocimiento de la gestión documental debido a su experiencia profesional en el diseño, implantación y mantenimiento de sistemas de gestión de documentos. Es necesario mencionar que, al igual que con el estudio de caso, los participantes de los debates prefirieron el anonimato para, de este modo, poder explicar experiencias personales de manera abierta y confidencial. La información se presenta de forma anonimizada, para evitar cualquier conflicto.

La finalidad de estos debates fue la de recopilar información sobre la visión y el conocimiento real que los participantes tenían de la gestión de riesgos documentales, así como su visión sobre si la integración de esta metodología en la gestión de documentos podría tener alguna afectación en los procesos de rendición de cuentas pública. Para ello, se plantearon las mismas preguntas en ambos grupos, se analizaron los resultados de manera individual, así como de manera comparada.

Resulta paradójico que en una investigación sobre rendición de cuentas pública, que se relaciona directamente con el acceso a la información y la transparencia, haya tenido tanta importancia el anonimato y la confidencialidad. En el estudio de caso, esto fue así porque el organismo público analizado creyó que exponer sus vulnerabilidades podría tener un impacto negativo en su imagen e incluso aumentar los riesgos a los que se podía ver expuesto. En los *Focus Groups*, en cambio, fue una cuestión de libertad de los participantes para poder exponer realidades y experiencias sin necesidad de obviar detalles en sus explicaciones. Esto permitió conocer situaciones de riesgo documental con consecuencias que iban más allá de la afectación a las propias organizaciones. En cualquiera de los dos casos, resulta destacable esta paradoja sobre la obtención de la información que sirve de base a la investigación. Esto no ha impedido realizar análisis pormenorizados de ambas experiencias prácticas, sino que, al contrario, ha favorecido los flujos de información y la recopilación de datos para el estudio.

Estas metodologías permitieron desarrollar los objetivos fijados para profundizar en las hipótesis planteadas, a partir del acercamiento desde diversas perspectivas y ámbitos de estudio.

La investigación se estructura a través de diferentes apartados teóricos, que dan paso a las experiencias prácticas mencionadas, para acabar presentando las conclusiones finales. En primer lugar, se realiza una aproximación al marco teórico de la gestión documental, que es la base sobre la que se realiza el análisis. En este primer capítulo, se analiza la definición de documento desde el punto de vista de la evidencia que puede servir a los procesos de rendición de cuentas pública. Se explican, también, los procesos de gestión documental, comparando el ciclo de vida con el *records continuum*, en la medida en que afectan a este objetivo probatorio, así como los instrumentos que son necesarios para llevarlos a cabo. En este primer apartado, se presenta la gestión documental como una metodología integradora y transversal, que beneficia y se ve beneficiada por otros métodos, como pueden ser la gestión del cambio, la gestión de procesos o la gestión de riesgos, entre otros.

El segundo capítulo se centra en el marco teórico de la rendición de cuentas y en su relación con la gestión de documentos. Se parte de la comprensión de las funciones de dicho proceso para pasar a explorar las casuísticas y los tipos que presentan diferentes autores. De este modo, se busca comprender la complejidad de la rendición de cuentas pública desde distintos enfoques, pero con la gestión documental como paso previo y necesario. En este capítulo se incluyen, además, apartados sobre transparencia, entendida como uno de los medios para facilitar la rendición de cuentas, en tanto que facilita el acceso a los documentos, que son la fuente original de la información.

El tercer capítulo explora la gestión de riesgos. Explica la teoría general de gestión del riesgo avanzando hacia su aplicación a la gestión documental. De este modo, se inicia el capítulo con una presentación de los diferentes estándares internacionales aplicables y la explicación en profundidad de las distintas fases del proceso. A partir de aquí, se analizan distintas metodologías y enfoques desarrollados desde el punto de vista documental, siendo estos el núcleo del capítulo.

El cuarto capítulo tiene como finalidad principal analizar el conocimiento que tienen los profesionales de los archivos y la gestión documental sobre la gestión de riesgos y su aplicación a su ámbito de trabajo. Es por ello que en este capítulo se presentan los *Focus Groups* realizados, así como la explicación en profundidad de la metodología seguida. Se incluye el desarrollo de los debates y su análisis individual y comparado. Este apartado es fundamental para conocer el grado de madurez de los profesionales en relación al tema estudiado, a través de una muestra.

El quinto capítulo desarrolla el objetivo 1, de la aplicación práctica de la metodología sobre gestión de riesgos documentales. Se desarrolla a través de un estudio de caso en el que se aplican distintas técnicas, seleccionadas en función de su adecuación al contexto de la organización y de su integración con la gestión documental. En este capítulo, se pone en práctica la metodología estudiada a nivel teórico, como un modo de evidenciar que es realmente aplicable en un entorno real. Permite, no solo demostrar las hipótesis relacionadas, sino disponer de un laboratorio de pruebas para analizar las técnicas y métodos seleccionados y su grado de idoneidad para la gestión de documentos. Además, los resultados obtenidos permiten proponer acciones de mejora y prevención, evidenciando los beneficios de la aplicación de la metodología.

El último capítulo incluye las conclusiones de la investigación tanto desde un punto de vista teórico y de análisis de las fuentes bibliográficas, como desde un punto de vista práctico, gracias a la aplicación de la teoría en un entorno real. Cabe mencionar que esta investigación pretende ser un punto de partida para desarrollos posteriores de la metodología trabajada. Debe entenderse como un primer paso de análisis desde el que poder mejorar la adaptación metodológica al entorno de la gestión de documentos, ya sea tanto en organismos públicos como privados. El hecho de que la presente investigación se centre en la administración pública no cierra las puertas a que la metodología estudiada pueda ser aplicada de igual modo en el sector privado. Cabrá tener en cuenta en ese caso, quizás, unos objetivos y unas aportaciones distintas.

Capítulo 1.

Marco teórico de la gestión documental

El presente capítulo reflexiona sobre la cuestión de la gestión documental y sobre la definición de documento, documento archivístico o de archivo⁴. También se profundiza en conceptos relacionados, como los procesos de gestión documental y los instrumentos que permiten su desarrollo.

El marco de referencia es la ciencia archivística, que se define como el cuerpo de conceptos y métodos dirigidos al estudio de los documentos en términos de sus relaciones documentales y funcionales y los modos en que se controlan y se comunican (Gilliland *et al.* 2016, p. 43). Sin embargo, cabe recordar que los archiveros no trabajan aislados, sino que a menudo se enfrentan con el trabajo, las suposiciones y los puntos de vista de diferentes profesionales en el amplio campo de las Ciencias de la Información, en el que entornos, objetivos, funciones e incluso la terminología pueden compartirse (Gilliland *et al.* 2016, p. 76). La aproximación teórica y terminológica a los conceptos de documento y de gestión documental se desarrolla, en este capítulo, desde este punto de vista multidisciplinar.

El capítulo se apoya en un conjunto de estándares internacionales, ampliamente reconocidos por la profesión, como son las normas ISO 15489⁵, ISO 30300⁶ e ISO 16175⁷. Son tres normas ISO centradas en los conceptos, procesos e instrumentos básicos de los sistemas de gestión documental y con aplicación a cualquier tipo de organización.

Se complementa, por tanto, la bibliografía teórica con las normas internacionales citadas, que tratan aspectos más operacionales. De este modo, se busca una aproximación a la gestión de documentos desde ambas perspectivas, sin olvidar la base científica, pero complementándola con definiciones más prácticas.

⁴ – En el texto se emplean “documento archivístico” y “documento de archivo” con idéntico significado. La decisión de emplear uno u otro término se relaciona con evitar reiteraciones y cacofonías a lo largo del texto.

⁵ – UNE-ISO 15489-1. Información y documentación. Gestión de documentos. Parte 1: Conceptos y principios.

⁶ – La familia de normas ISO 30300 consta de tres normas: UNE-ISO 30300 - Información y documentación. Sistemas de gestión para los documentos. Fundamentos y vocabulario; UNE-ISO 30301 - Información y documentación. Sistemas de gestión para los documentos. Requisitos; y UNE-ISO 30302 - Información y documentación. Sistemas de gestión para los documentos. Guía de implantación.

⁷ – La familia de normas ISO 16175 - Información y documentación. Principios y requisitos funcionales para documentos en entornos de oficina electrónica, consta de tres partes: Parte 1 – Generalidades y declaración de principios; Parte 2 – Directrices y requisitos funcionales para sistemas que gestionan documentos electrónicos; Parte 3 – Directrices y requisitos funcionales para los documentos en sistemas de la organización.

1.1 El concepto de documento

En sentido genérico, el documento se entiende como el testimonio de la actividad humana fijada sobre un soporte perdurable que contiene información (López Gómez & Gallego Domínguez 2007, p. 17). Según el *Manual de archivística y gestión de documentos* de la Asociación de Archiveros de Cataluña, el término documento, que semánticamente combina las voces y los conceptos de los verbos latinos *docere* (enseñar, instruir, informar) y *memorare* (recordar), abraza, en sentido amplio y genérico, cualquier registro de información con independencia de su soporte material (Capell i Garriga & Corominas i Noguera 2009, p. 74). Por su parte, el diccionario multilingüe del Consejo Internacional de Archivos⁸, define documento como la unidad indivisible de información constituida por un mensaje fijado a un medio de manera sintácticamente estable. Un documento tiene, por tanto, una forma fija y un contenido estable⁹.

En las definiciones anteriores se incluyen referencias a contenido y continente, como partes constituyentes de un documento. Cruz Mundet (Cruz Mundet 2005, p. 97) incluye el registro o la fijación de la información (contenido) en el soporte (continente), como un elemento más del documento. Con relación al contenido, lo importante es la existencia de información, que puede ser testimonio o evidencia de una actividad, así como también constituir un mensaje. En esta línea, el documento puede tener distintas funciones, como informativa, jurídica o testimonial, de las que se hablará más adelante.

Con relación al continente, el concepto de documento incluye todos los medios y formatos como, por ejemplo, fotografías, dibujos, grabaciones de sonido, vídeos, archivos de procesadores de texto, hojas de cálculo, páginas web o bases de datos (Pearce-Moses 2005, p. 126). También hay que tener presente que, en muchas ocasiones, los nuevos formatos no sustituyen a los viejos, sino que permanecen al mismo tiempo dando lugar a la elección entre unos y otros (Lappin 2010, p. 255). Esto tiene como consecuencia la existencia de entornos de trabajo híbridos, en los que se combinan los documentos en formato electrónico con los documentos en papel. Lo importante a tener en cuenta es que ambos pueden tener la misma función, independientemente de su soporte. La diferencia radica en su representación y visualización.

Las afirmaciones anteriores se aproximan al documento de una manera general. Desde la perspectiva archivística, además, se concretan otras características y cualidades de los documentos y se pueden encontrar diferenciaciones que se explican a continuación.

Cualquier conjunto de información, con independencia de su estructura o forma, puede ser gestionado como un documento. Esto incluye información en forma de documento, un conjunto de datos u otro tipo de información digital o analógica que sea creada, capturada y gestionada en el curso de una actividad (AENOR 2016, p. 10). Esta información es objeto de tratamiento de la archivística y tiene las siguientes características (Cruz Mundet 2012, p. 66):

- Es una información *interna*, producida por personas (físicas o jurídicas) en el desarrollo de sus actividades, de forma necesaria e inevitable.

⁸ – Diccionario Multilingüe del Consejo Internacional de Archivos: <http://www.ciscra.org/mat/> (consultado el 15/10/2017).

⁹ – Definición de documento del Diccionario Multilingüe del Consejo Internacional de Archivos: <http://www.ciscra.org/mat/mat/term/1676> (consultado el 15/10/2017).

- Es una información *previsible*, por cuanto es fruto de procesos establecidos, sean los procedimientos administrativos (caso de las administraciones públicas), sean los procesos de negocio (caso de las organizaciones privadas), sea la gestión de las actividades propias de las personas físicas en las que no interviene la voluntad creativa.
- Es una información *reglada*, en su creación, uso y conservación. La creación de todos estos documentos está recogida y regulada por normas legales y/o de procedimiento interno. Su utilización (tramitación, acceso, información, obtención de copias) también está sancionada por normas legales de carácter público y/o por normativa de las organizaciones privadas. Asimismo, su conservación, entendida en términos de eliminación o conservación, está regulada por normas.

Según Cruz Mundet, los documentos y la información propios de otras disciplinas no cumplen estas condiciones.

Tradicionalmente, el documento archivístico se ha definido como el vehículo estable mediante el cual el significado pretendido por el autor y el hecho real, documentado, sobre una transacción se comunican a lo largo del tiempo y del espacio (Lemieux 2001, p. 96). Para Lemieux, la definición archivística de documento se ha producido de manera mayoritaria en la era de los medios impresos (o el soporte papel) y sugiere que, en la actualidad, en la que se dispone de documentos electrónicos para la gestión del día a día de las organizaciones, la conceptualización del documento cambia. Pese a ello, las definiciones que existen de documento electrónico o documento digital mayoritariamente lo describen como un documento creado en forma digital (Duranti & Franks 2015, p. 163), sin mayor concreción.

Para Lemieux, la era electrónica ha trasladado la discusión epistemológica y ontológica sobre el documento desde una visión de objeto estable hacia una visión de documento como algo mutable e inestable (Lemieux 2001, p. 97). En el campo de la ciencia computacional, un documento es un objeto creado mediante *software*, como, por ejemplo, una aplicación de procesador de textos o un fichero informático no ejecutable, y que contiene datos para su uso por distintas aplicaciones. Esto adapta el concepto tradicional de documento a un objeto que contiene información (Duranti & Franks 2015, p. 185). En otras palabras, un documento digital¹⁰ es una entidad que presenta todos los atributos de un documento, pero que se ha generado como una serie de dígitos de ceros y unos y que requiere una combinación de *hardware* y *software* para representarlo de manera que las personas puedan leerlo y entenderlo (Duranti & Franks 2015, p. 163). Es decir, debe ser interpretado y mostrado al ojo humano mediante un reproductor (de vídeo, de cintas magnéticas de sonido o de un ordenador) (Soler i Jiménez 2009, p. 35). En cambio, los documentos analógicos, por otro lado, son aquellos que se representan mediante soportes como el papel, que suelen ser inteligibles al ojo humano y tienen un impacto visual directo.

Aunque los documentos archivísticos pueden manifestarse de distintas maneras, los mismos elementos formales que están presentes en los documentos archivísticos tradicionales¹¹ existen, explícita o implícitamente, en los documentos archivísticos electrónicos, y todos los documentos archivísticos electrónicos comparten los mismos elementos formales (Duranti 2008, p. 3).

¹⁰ –Documento digital y documento electrónico se emplean como sinónimos a lo largo del texto, en contraposición al documento analógico.

¹¹ – En referencia a los documentos en formato papel.

Duranti, al referirse al “documento archivístico¹² electrónico”, identifica seis características necesarias para su existencia (Duranti 2008, p. 2):

1. Una forma fija, como aquella forma que no pierde ninguno de sus elementos originales en el proceso de almacenaje y recuperación. Esta cuestión se refiere a la estabilidad del contenido binario, que debe permanecer completo e inalterado. Esto debe permitir que el mensaje se pueda transmitir de la misma manera en que se emitió por primera vez.
2. Un contenido inmodificable. Esto implica que su contenido intelectual debe permanecer igualmente estable e inalterado.
3. Enlaces explícitos a otros documentos archivísticos, dentro o fuera del sistema digital, mediante un código de clasificación u otro identificador único.
4. Un contexto administrativo identificable.
5. Un autor, un destinatario y un escritor. El autor es quien promulga el documento archivístico, el escritor es quien determina la articulación del discurso en el documento archivístico, y el destinatario es la persona a la que está dirigido el documento archivístico. Como un documento archivístico debe participar en una acción y cualquier acción debe recaer en alguien, el destinatario es necesario para la existencia del documento archivístico.
6. Una acción, en la que el documento archivístico participa o a la que el documento archivístico apoya, bien procedimentalmente o bien como parte de un proceso de toma de decisiones.

Estas características permitirán demostrar que el documento archivístico electrónico es fiable y auténtico a largo plazo (Soler i Jiménez 2009, p. 37).

El elemento de soporte¹³, sin embargo, no aparece en las definiciones de documento que se dan en los estándares internacionales. Por ejemplo, según la norma UNE-ISO 15489: 2016, el término “documento archivístico” se define como la información creada, recibida y conservada como evidencia y como activo por una organización o individuo, en el desarrollo de sus actividades o en virtud de sus obligaciones legales (AENOR 2016, p. 9). En cambio, sí aparecen en la definición los términos “evidencia” y “activo”.

Por una parte, la evidencia se define, en esta misma norma, como la documentación de una operación, y añade que se trata de una prueba de la realización de una actividad, que puede demostrar que ha sido creada en el curso normal de la misma y que está intacta y completa. Esta definición no se limita al sentido legal del término (AENOR 2016, p. 8). La evidencia puede emplearse para dar apoyo a una acción o a la toma de decisiones, así como para probar

¹² – En la traducción del artículo de Luciana Duranti se ha optado por traducir del inglés la palabra “document” por “documento” y la palabra “record” como “documento archivístico”, con el fin de expresar la diferencia conceptual entre los dos términos originales. Más adelante, en este mismo apartado, se comenta la problemática sobre la traducción de ambos términos.

¹³ – El soporte se refiere al medio en el cual se fija la información, por ejemplo, en papel, en cintas magnéticas o *software*. En los estándares internacionales, ya desde la publicación de la norma ISO 15489 en el año 2001, no se incluyen referencias a los soportes en la definición de documento. Esto implica que este elemento no cambia el concepto, sino que se trata como un atributo o característica más.

o refutar afirmaciones o hipótesis. Puede resultar útil para determinar la certeza de una proposición, justificando una creencia, explicando por qué es cierta o persuadiendo a la audiencia de su veracidad. Estos son propósitos para los que pueden emplearse los documentos de archivo (Yeo 2007, p. 322), aunque los documentos de archivo no son evidencias en sí mismos, sino que proporcionan evidencia. El documento archivístico enlazado al término evidencia se hace presente en numerosas definiciones de diferentes autores (Shepherd & Yeo 2003; Cruz Mundet 2005; Capell i Garriga & Corominas i Noguera 2009; Yeo 2007; Cox 2001; Soler i Jiménez 2009). Sin embargo, documento de archivo y evidencia no deben entenderse como sinónimos, sino que el documento es un instrumento que proporciona evidencia, que puede ayudar a demostrar un hecho o una actividad o, dicho de otra manera, que la evidencia puede obtenerse mediante su uso (Yeo 2007, p. 325).

Por otra parte, el término “activo” se define como cualquier bien que tiene valor para la organización (AENOR 2011, p. 14), incluyendo ejemplos como la información, las personas y su cualificación, *software* o aplicaciones informáticas, entre otros. La importancia de identificar la información y la documentación como activos de una organización radica en las medidas de preservación y prevención que se llevarán a cabo para evitar que se pueda acceder a ellos, utilizarlos, hacerlos públicos, manipularlos, destruirlos y/o robarlos de manera ilícita, dando como resultado una pérdida (Jones 2005, p. 5).

Como se puede apreciar hasta ahora, las definiciones de documento archivístico son interdependientes, ningún término puede definirse sin utilizar otros términos, que deberán definirse también (Yeo 2007, p. 315). Además, no existe tan solo una verdadera conceptualización de documento archivístico, sino muchas conceptualizaciones distintas que surgen de contextos sociales concretos (Lemieux 2001, p. 81). Partiendo de esta base, y leyendo las definiciones incluidas anteriormente, se deduce que encontrar una única definición no resulta sencillo. Eso sí, se puede afirmar que un documento de archivo no se define por su formato, su soporte o su edad, ni es simplemente un mecanismo para contener información, sino que la esencia del documento es que proporciona evidencia de una actividad específica (Shepherd & Yeo 2003, p. 2).

Es importante comentar en este apartado la distinción terminológica que existe en la tradición anglosajona¹⁴, donde se diferencia entre los términos de “*document*” y “*record*” para referirse a lo que en castellano se suele traducir como “documento” y “documento de archivo” o “documento archivístico”. La diferencia principal entre ambos términos es el valor de los documentos de archivo como evidencia de las actividades, transacciones, operaciones o acontecimientos generados o recibidos en el transcurso de una función (Duranti & Franks 2015, p. 315). En este escenario, los documentos o “*documents*” pueden cambiar a lo largo del tiempo mientras que los documentos de archivo o “*records*” son estables e invariables.

Hay autores de habla hispana que se muestran en desacuerdo con esta traducción, y afirman que ambos términos deben traducirse como “documento”. Para Cruz Mundet, por ejemplo, se trata de un fenómeno introducido como

¹⁴ – Países cuyo sistema legal y administrativo tiene orígenes ingleses.

resultado de la mala calidad de las traducciones de determinadas normas y referentes del inglés¹⁵ (Cruz Mundet 2012, p. 67). Si bien es cierto que el término “*record*” se traduce por la palabra “documento” sin necesidad de añadirle un adjetivo o un complemento, sí se considera necesario poder diferenciar la traducción del término “*document*”, puesto que las características y valores de ambos no son coincidentes. Es por ello que en esta investigación se opta por emplear la traducción mencionada pese a los argumentos de sus detractores.

En cualquier caso, cabe recordar que tanto el desarrollo de estándares y normas internacionales, como su traducción parten del consenso entre las personas de los distintos grupos de trabajo de los organismos de normalización. Esta traducción ha sido debatida a alto nivel por los miembros de los comités de desarrollo y traducción de normas, llegando al consenso antes mencionado para ambos términos. Pese a ello, sí se considera necesaria una revisión de la terminología para conseguir una mejor aproximación al lenguaje empleado por los profesionales de la archivística, así como también una simplificación en algunas traducciones que pueden llevar a confusión, como es el caso de documento y documento de archivo.

Los documentos de archivo se pueden definir como aquellos producidos y acumulados por una institución pública o privada, persona o familia en el uso de su gestión o actividad, para el cumplimiento de sus fines, y conservados como testimonio (a título de prueba), información y continuidad de la gestión (López Gómez & Gallego Domínguez 2007, p. 64). Tienen ciertos elementos diferenciadores, como son el carácter seriado, la génesis, la exclusividad y la interrelación (Cruz Mundet 2005, p. 97), que se explican a continuación:

- El carácter seriado: los documentos se producen uno a uno y con el paso del tiempo constituyen series¹⁶.
- La génesis: se producen dentro de un proceso natural de actividad, surgen como producto y reflejo de las tareas de su productor, no son algo ajeno a él.
- La exclusividad: la información que contienen rara vez se encuentra en otro documento con idéntica extensión e identidad, es exclusiva.
- La interrelación: como principio general, las piezas aisladas (documentos sueltos) no tienen sentido o tienen muy poco, su razón de ser viene dada por su pertenencia a un conjunto (la unidad archivística o expediente) y por las relaciones establecidas entre sí.

Cabe remarcar tres aspectos clave de los documentos de archivo. En primer lugar, las organizaciones los utilizan para llevar a cabo sus negocios, para permitir la toma de decisiones y para que puedan llevarse a cabo sus actividades. Los documentos de archivo proporcionan acceso a precedentes y a políticas, así como evidencian lo que se hizo o se decidió en un pasado. Permiten a las organizaciones protegerse frente al fraude y proteger sus derechos y activos.

¹⁵ – En este sentido cabe mencionar que en las normas internacionales que no son específicas de gestión documental (las más conocidas son la ISO 9001 o la ISO 14001), se ha venido traduciendo *record* por “registro”, dando lugar a confusiones importantes durante años. Para dar una solución a esta problemática, se ha establecido en las actualizaciones de normas desde el año 2015 el término *documented information* que se traduce fácilmente al castellano por “información documentada” clarificando y normalizando el concepto. Esta denominación va a estar presente en todas las normas ISO, ya sean de nueva creación o actualizaciones de normas ya existentes, puesto que es de obligatorio cumplimiento.

¹⁶ – Una “serie documental” se define como el conjunto de unidades documentales homogéneas organizadas de acuerdo con un sistema de clasificación, o conservadas como una unidad por el hecho de ser el resultado de un mismo proceso de formación o de clasificación, o de la misma actividad, porque tienen una misma tipología, o por cualquier otra relación derivada de su producción, recepción o uso (NODAC 2007, p. 27).

En segundo lugar, las organizaciones emplean los documentos de archivo para dar apoyo a la rendición de cuentas, cuando necesitan probar que han cumplido con sus obligaciones o que han cumplido con los requisitos de buenas prácticas o las políticas establecidas. En tercer lugar, los documentos de archivo también pueden emplearse para propósitos culturales o de investigación, para promover el conocimiento y comprender la historia corporativa (Shepherd 2006, p. 6).

1.1.1 Propiedades del documento de archivo

Los documentos archivísticos se generan a partir de funciones, actividades o procesos. Bien gestionados, estos proporcionan evidencia sobre cómo una política se ha desarrollado o ejecutado o sobre cómo se llevó a cabo un estudio, por ejemplo. (Thurston 2012, p. 4). Pero para que un documento archivístico pueda ser aceptado como una evidencia creíble, es necesario demostrar que dicho documento es auténtico y confiable, que no es fraudulento, y que su contenido es suficiente y preciso (Pearce-Moses 2005, p. 152). Lemieux va más allá, y afirma que un documento archivístico puede ser aceptado como una evidencia confiable de una transacción por los siguientes motivos (Lemieux 2001, p. 93):

- Su creación habría tenido que ser completada para dar efecto a la transacción de la organización para la cual el documento archivístico fue creado.
- La creación o producción normal de un documento archivístico exige precisión.
- El creador del documento de archivo no debe tener, por regla general, ningún motivo para manipular, sustituir, o falsificar el documento de archivo para algún propósito futuro que no se hubiese tenido en cuenta.
- La organización habría confiado en el documento de archivo para sus objetivos de negocio y, por tanto, se habría percatado si dicho documento no fuese confiable o auténtico, si este fuera el caso.
- El documento de archivo fue creado como el deber de un empresario y, por tanto, existe un riesgo de crítica o escándalo en caso de haberse producido errores.

Entran en juego, por tanto, otras propiedades de los documentos de archivo hasta ahora no definidas, como son la autenticidad, la fiabilidad o confiabilidad y la integridad. Los documentos, con independencia de su forma o estructura, deberían tener dichas características para ser considerados evidencia fidedigna de los eventos u operaciones (AENOR 2016, p. 10). Un documento no es solo información, es más que eso, se le supone fiabilidad: ser creíble y auténtico, capaz de servir como evidencia y de dar soporte a la rendición de cuentas (Öberg & Borglund 2006, p. 55).

Un documento auténtico es aquel del que se puede probar que es lo que afirma ser, que ha sido creado o enviado por el agente del cual se afirma que lo ha creado o enviado, y que ha sido creado o enviado en el momento en que se afirma (AENOR 2016, p. 10). La autenticidad se define como la cualidad de ser genuino, de no haber sido falsificado, y de estar libre de cualquier manipulación. Cabe mencionar que la autenticidad de un documento por sí sola no implica de manera automática que el contenido del documento sea fiable (Pearce-Moses 2005, p. 41).

Un documento es fiable porque su contenido es completo, exacto y es una fiel representación de las operaciones, actividades o hechos que evidencia, y de él se puede depender en el transcurso de las subsiguientes operaciones o

actividades (AENOR 2016, p. 11). La fiabilidad se define como la cualidad de ser confiable y merecedor de confianza (Pearce-Moses 2005, p. 340). Es un concepto relativo asociado con la autenticidad, la exactitud, la precisión, la completitud, la integridad o la consistencia. Se puede afirmar que es una de las propiedades requeridas en los documentos para la finalidad de rendir cuentas más comunes e importantes, y no importa cuál sea el contexto de la organización. Sin embargo, es una propiedad que normalmente se da por supuesta (Lemieux 2001, p. 92) cuando no siempre es real. Las administraciones pueden garantizar estas características de los documentos mediante la creación de un entorno de confianza para la gestión de la creación, organización, uso y preservación de los datos y documentos, mediante la combinación de leyes y políticas, estándares y prácticas, habilitando tecnologías, y con personas cualificadas y formadas. En este entorno, la integridad de los documentos y los datos se mantiene, y los metadatos (datos sobre datos), que proporcionan el contexto y la usabilidad, son preservados (Thurston 2012, p. 2). Si se pretende que los documentos puedan servir como evidencia a lo largo del tiempo, los usuarios futuros deben poder confiar en su autenticidad e integridad. La mera existencia de un sistema de gestión documental apoyará la credibilidad de los documentos de archivo (Shepherd & Yeo 2003, p. 103).

Un documento íntegro es aquel que está completo e inalterado (AENOR 2016, p. 11). La integridad se define como la cualidad de permanecer completo e inalterado frente a la pérdida, manipulación o la corrupción. Es un concepto relativo que evalúa si la naturaleza esencial del documento de archivo ha cambiado. En este contexto, la integridad se relaciona con la pérdida potencial de elementos físicos o intelectuales después de la creación del documento. Esto se distingue de la completitud, que se refiere a la presencia de todos los elementos, ya sean físicos o intelectuales, requeridos en el momento de la creación (Pearce-Moses 2005, p. 210).

A estas tres características esenciales del documento de archivo (autenticidad, fiabilidad, integridad), las normas ISO añaden la usabilidad. Un documento usable es aquel que puede ser localizado, recuperado, presentado e interpretado en un periodo de tiempo considerado razonable por las partes interesadas (AENOR 2016, p. 11) y, por tanto, legible al ojo humano. Por tanto, no solo es accesible, sino que puede utilizarse para realizar las actividades para las que fuese necesario. No hay que olvidar la rapidez de la obsolescencia tecnológica que, en muchos casos, deriva en la imposibilidad de leer e interpretar la información de los documentos.

1.2 El ciclo de vida y la teoría del *Records continuum*

El concepto de ciclo de vida de los documentos surgió en Estados Unidos como resultado del proceso de configuración del sistema archivístico federal. Su finalidad era, por un lado, recoger los fondos históricos de las administraciones federales, así como aquellos otros de interés nacional que pudieran rescatarse de manos de particulares; por otro lado, se trataba de poner en pie un sistema novedoso que resolviese las necesidades documentales de la Administración Federal para el desarrollo de sus actividades (Cruz Mundet 2012, p. 89).

El ciclo de vida de los documentos conlleva en su significado una progresión, una secuencia, un principio y un final (Duranti & Franks 2015, p. 343). Implica que los documentos no son algo estático, sino que desde el momento de su creación pasan por una serie de etapas que determinan algunas de sus características, hasta su disposición final

(conservación permanente o eliminación). Estas fases, por regla general, son tres: activa o de trámite, semiactiva o de vigencia, inactiva o de conservación, y se relacionan principalmente con la frecuencia de uso de los documentos y sus valores.

Este modelo implica que los documentos se conservan, en un primer momento, por motivos organizacionales y, también, que serán transferidos a la custodia del archivo cuando el paso del tiempo haya reducido su valor de negocio para la organización (Shepherd & Yeo 2003, p. 7). Los documentos deben ser producidos o agrupados para cumplir un objetivo específico y deben tener valores para otros objetivos que no sean los que los han generado o agrupado (Schefflenberg 1996, p. 16). Se entiende por valor archivístico el conjunto de valores administrativos, legales, probatorios y/o informativos que justifican la conservación permanente de los documentos para la administración productora, para otras administraciones y para la investigación (López Gómez & Gallego Domínguez 2007, p. 111). Los valores de un documento dependen del fin por el cual ha sido creado (valor primario) y de la utilidad que se pueda deducir con posterioridad (valor secundario). Por tanto, se entiende que los documentos pueden adquirir y perder valores con el paso del tiempo.

Este modelo de fases no implica que los profesionales de la archivística tan solo actúen en la etapa final de cambio de custodia, sino que el criterio archivístico está presente desde el momento inicial.

Las tres fases se definen de la siguiente manera (ver Figura 2):

1. Fase activa o de trámite: abarca desde el momento de la creación, incorporación o captura del documento o expediente al sistema de gestión documental, hasta su aprobación formal (cierre del expediente).
2. Fase semiactiva o de vigencia: aquella durante la cual la documentación todavía es necesaria para la gestión administrativa y como referencia legal, evidencia y testimonio de las actividades y decisiones de la organización.
3. Fase inactiva o de conservación: aquella en que se procede a la conservación y uso de los documentos con carácter informativo y que tienen un valor relevante para la investigación, convirtiéndose en patrimonio documental y memoria corporativa de la organización.

Estas fases se relacionaban, de manera general, con los espacios físicos que ocupaban los documentos en papel en cada una de ellas, y estos son los archivos de gestión, archivos intermedios y archivos históricos. En la administración electrónica esto no es así, puesto que las fases se entienden como una convención que permite distinguir las distintas etapas por las que pasan los documentos y que, en ningún caso, deben atribuirse necesariamente a los espacios físicos para una de estas fases.



Figura 2 - Ciclo de vida de los documentos (elaboración propia).

Este modelo de ciclo de vida ha sido criticado en los últimos años por su división artificial en tres etapas, que no siempre se corresponden con la realidad, y aún más en la actualidad, con el auge de los documentos en formato electrónico. Una de las críticas es que no contempla que el documento pueda regresar a la fase activa desde las etapas posteriores, puesto que se le presupone una secuencialidad. Otra de las críticas se refiere al concepto de la “muerte” o inactividad del documento, que tampoco se corresponde con la realidad, puesto que los documentos que se conservan de manera permanente no dejan de tener actividad, aunque esta se reduzca o cambie en relación a sus valores secundarios.

Para Cruz Mundet resulta inaceptable esta denominación de las distintas fases del ciclo de vida de los documentos, ya que presuponen una visión de la función de los documentos limitada a un rol meramente transaccional. Según este autor, el documento, en efecto, atraviesa por distintas fases: desde que se elabora y durante un periodo, habitualmente corto, es objeto de un uso intensivo para la resolución de los asuntos, de las actividades, que recoge y testimonia; con el paso del tiempo cada vez se utiliza menos, pierde su valor originario y es eliminado o bien adquiere un nuevo valor de futuro, que puede añadirse al valor inicial, sin sustituirlo, y se decide su conservación permanente. Esto quiere decir que los documentos pueden pasar de la actividad a la desaparición, pero que conservándose no quedan inactivos, lo que cambia es la perspectiva desde la que se les da utilidad (Cruz Mundet 2012, p. 91). Finalmente, en los últimos años se añadió una tercera crítica, la de estar demasiado enfocado a los documentos como entidades físicas y en las tareas operacionales, aspectos que resultan irrelevantes desde la perspectiva de los documentos electrónicos (Cruz Mundet 2012, p. 92).

Como evolución de este modelo, surgió el concepto del *records continuum*, en el que no hay etapas separadas, sino donde la gestión documental se ve como un proceso en el que un elemento puede ir de un estado a otro de manera continua, sin interrupciones o cambios de etapa. Este modelo encaja en la corriente postcustodialista de la archivística, un paradigma en el que las estrategias de custodia¹⁷ son, como mucho, una consideración menor de la implementación (Cunningham 2011, p. 179). Este enfoque pretendía, entre otras cosas, evitar que los archiveros y gestores de documentos quedasen relegados a una función meramente de conservación y custodia (finalista), sin ninguna implicación en las decisiones sobre la creación y gestión de los documentos. El paradigma postcustodialista es una “etiqueta” para un conjunto coherente de conceptos, modelos, teorías y métodos que proporcionan un enfoque integrado (Duranti & Franks 2015, p. 85) de la gestión documental.

¹⁷ – La custodia de los documentos se define como la salvaguarda de documentos en archivos para su cuidado. La custodia archivística tiene una dimensión física, que requiere la posesión física, propiedad y control de los documentos de archivo con el fin de que sean protegidos contra su alteración, destrucción o hurto. También tiene una dimensión legal en relación a que los archivos son los legítimos y legalmente designados guardianes de los documentos de archivo (Duranti y Franks 2015, p. 35).

El modelo del *records continuum* fue desarrollado entre los años 1980 y 1990 por Frank Upward para dar respuesta a las críticas mencionadas. Se trata de un modelo abstracto y conceptual, cuyo objetivo es entender y explorar las actividades de gestión de documentos en relación con múltiples contextos a lo largo del tiempo y del espacio. Se representa a partir de cuatro ejes que Upward denomina en inglés *evidential*, *transactional*, *recordkeeping*, *identity* y que para esta investigación se han traducido¹⁸ como probatorio, transaccional, archivístico e identitario. Estos ejes comprenden los conceptos clave en archivística, según Upward, y cada eje presenta cuatro coordenadas que pueden enlazarse dimensionalmente (Upward 1996, p. 8). Upward denomina las dimensiones del modelo en inglés como *create*, *capture*, *organise*, *pluralise*, que para esta investigación se han traducido como crear, capturar, organizar y pluralizar.

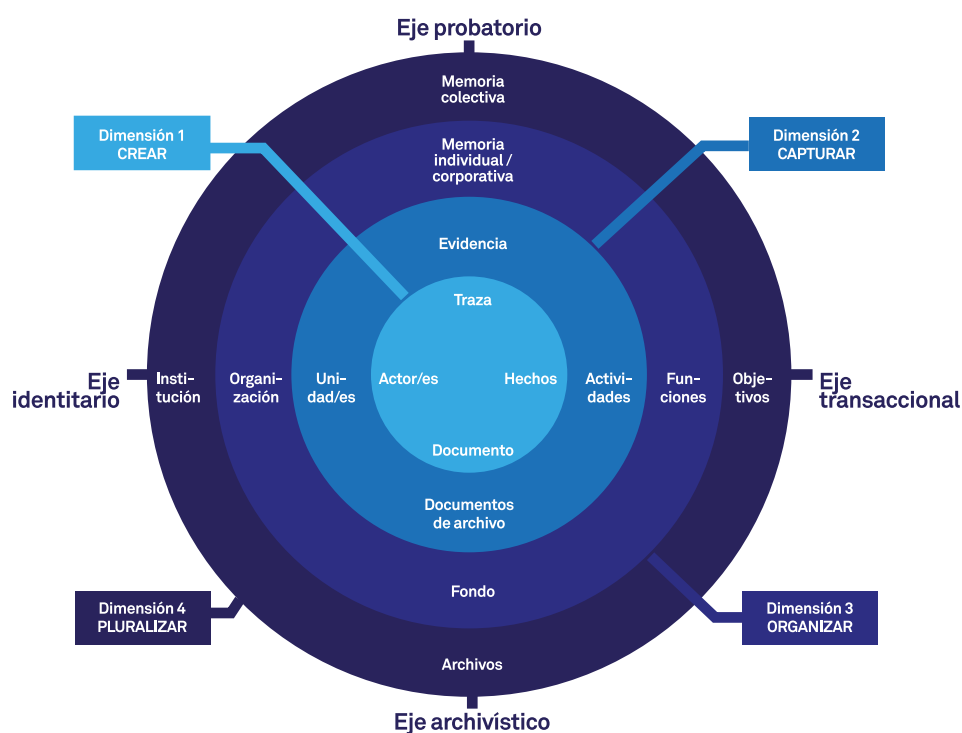


Figura 3 - Records Continuum (Frank Upward).

Este gráfico (ver Figura 3) es aplicable a cualquier entorno documental (Reed 2005, p. 1). En este modelo no hay etapas, sino perspectivas de la gestión documental. Puede interpretarse el gráfico concéntrico tanto del centro hacia el exterior como viceversa, en relación a las dimensiones. Lo mismo ocurre con los ejes, que pueden leerse de manera recíproca, tanto en vertical como en horizontal o de derecha a izquierda y viceversa. Todos estos procesos pueden darse de forma simultánea, iterativa y dinámica, como sucede muy a menudo, por lo cual los documentos pueden adquirir capas de metadatos contextuales cada vez más amplios. Se trata de procesos sincrónicos, no diacrónicos. Los documentos pueden ser tanto actuales como históricos desde el momento de su creación (Cunningham 2005, p. 109).

¹⁸ – Se han detectado distintas traducciones en castellano del modelo desarrollado por Upward. Finalmente, en esta investigación se ha optado por una traducción propia que intenta ajustarse lo máximo posible al significado de cada uno de los términos del modelo.

En la Figura 3 se pueden apreciar los cuatro ejes del modelo, que se explican a continuación:

- El eje archivístico enmarca los medios de almacenamiento de la información documentada sobre las actividades humanas. Sus coordenadas son el documento, el documento de archivo, el fondo y los archivos. El documento dentro del modelo se basa en un hecho o acción y es una pseudo representación de dicho hecho. En él hay contenido, estructura y un contexto de creación. El documento de archivo es una forma de evocación del documento, normalmente relacionada con otros documentos. Debe tener unas capas adicionales de contexto en relación a las que presenta un solo documento. Es precisamente esa información adicional la que permite separar al documento de su contexto de creación y mantenerse como documento de archivo a lo largo del tiempo y el espacio (Upward 1996, p. 9). El fondo se define por la agregación de los documentos de archivo relacionados con una organización. Finalmente, el archivo está constituido por una suma plural de fondos, conteniendo documentos de archivo de un número de organizaciones mayor.
- El eje probatorio consiste en la traza o huella de las acciones, la evidencia que los documentos de archivo pueden proporcionar, y su rol en la memoria individual, corporativa y colectiva.
- El eje transaccional presenta los hechos, las actividades, las funciones y los objetivos como coordenadas. Por objetivos se refiere a la función del organismo vista desde una perspectiva social más amplia. Este eje es el reflejo de las actividades y funciones de una organización.
- El eje identitario representa al actor, la unidad de trabajo a la que este está asociado (puede ser el actor solo), la organización de la que forma parte la unidad (puede ser también el actor o la unidad) y el modo como la identidad de esos elementos se institucionaliza a través del reconocimiento social. Este eje responde por dos temas que son principales en la ciencia archivística, como son la noción de que un archivo debe estar relacionado con el productor del documento de archivo, y la de que los documentos de archivo reflejan las autoridades y responsabilidades que sustentan un acto o un hecho (Upward 1996, p. 9). La identidad se relaciona directamente con el productor, entendido como persona física o jurídica, que genera documentos en el ejercicio de sus funciones (eje transaccional).

En la Figura 3 también se aprecian las dimensiones del modelo, que se explican a continuación:

- Dimensión 1 – Crear: creación de los documentos como reflejo de un acto o hecho del que forman parte (Cruz Mundet 2012, p. 94). Los documentos se crean como parte de una actividad o transacción (Cunningham 2005, p. 109).
- Dimensión 2 – Capturar: captura de los documentos como evidencia, vinculándolos con las actividades, transacciones, operaciones, decisiones o comunicaciones que documentan, así como con su contexto social e inmediato. Los documentos se capturan en un sistema, con contexto, contenido y estructura documentados en metadatos (Cunningham 2005, p. 110).
- Dimensión 3 – Organizar: agregación sobre las instancias individuales de las secuencias de las acciones, otorgando al documento los elementos explícitos que son necesarios para asegurar que este estará disponible a lo largo del tiempo. En esta dimensión el documento se une a otros documentos derivados de otras acciones con otras finalidades (Reed 2005, p. 2). Los documentos se organizan y se gestionan como memoria y pruebas empresariales o personales (Cunningham 2005, p. 110).
- Dimensión 4 – Pluralizar: pluralización de los documentos, facilitando el acceso y la conservación de la memoria. El documento puede satisfacer demandas externas de partes no involucradas con la organización en

la que fue creado. Esta dimensión conlleva garantizar que los documentos podrán ser revisados, accesibles y analizados más allá de la organización, para los múltiples propósitos externos de rendición de cuentas, fines históricos, y otros propósitos que sean requeridos, durante todo el tiempo que sea necesario (Reed 2005, p. 3).

Sobre la base de los cuatro ejes, los documentos se crean, se reúnen, se organizan y se hacen accesibles (Cruz Mundet 2012, p. 95). Es importante recalcar que las dimensiones no son barreras, que las coordenadas no están presentes de manera invariable y que pueden ocurrir distintos hechos de manera simultánea a lo largo de las dimensiones (Upward 1996, p. 10).

El concepto de continuidad del modelo es flexible e inclusivo y refleja un rango de cuestiones en relación al rol de los documentos en las organizaciones y sociedades contemporáneas. Enfatiza que los mismos principios aplican a la gestión de documentos, ya sean estos de nueva creación o heredados del pasado (Shepherd & Yeo 2003, p. 10).

1.3 La gestión de documentos

La gestión de documentos se define en los estándares internacionales como el área de gestión responsable de un control eficaz y sistemático de la creación, la recepción, el mantenimiento, el uso y la disposición de los documentos, incluidos los procesos para capturar y mantener, en forma de documentos, la información y evidencia de las actividades y operaciones de la organización (AENOR 2016, p. 9). Engloba, por tanto, toda la documentación de una organización, incluyendo tanto a los responsables de su gestión como a cualquier empleado que cree o gestione documentos en el ejercicio de las funciones que tenga asignadas.

La organización ARMA Internacional¹⁹ establece unos principios de gestión documental, que son generalmente aceptados por los profesionales. Son ocho: rendición de cuentas, integridad, protección, conformidad, disponibilidad, retención, disposición y transparencia. Se basan en la experiencia práctica, así como en la consideración y el análisis extensivo de la doctrina legal y la teoría de la información (ARMA Internacional 2014, p. 2). Se explican a continuación:

- Principio de rendición de cuentas: un alto ejecutivo (o una persona con autoridad similar) debe supervisar el programa de gobernanza de la información²⁰ y delegar la responsabilidad sobre la gestión de documentos de

¹⁹ – ARMA Internacional es una organización profesional sin ánimo de lucro para gestores de información y documentos, así como otros profesionales relacionados. Proporciona oportunidades de formación y realiza publicaciones de manera periódica sobre las principales cuestiones de la gestión de documentos. Entre estas publicaciones se encuentran guías y estándares. Más información en: <https://www.arma.org/> (consultado el 21/01/2018).

²⁰ – ARMA define estos principios como de gestión documental, pese a que en la explicación de cada uno de ellos hace referencia a la gobernanza de la información. En el texto explicativo que acompaña estos principios se mezclan ambos términos y se define la gobernanza de la información como “un marco de rendición de cuentas que incluye los procesos, roles, estándares y métricas que aseguran el uso efectivo y eficiente de la información permitiendo a una organización alcanzar sus objetivos”. Puede apreciarse la gran similitud con la definición de gestión documental.

archivo y la información a las personas apropiadas. La organización adopta políticas y procedimientos para guiar al personal y asegurar que el programa puede auditarse.

- Principio de integridad: debe construirse un programa de gobernanza de la información para que la información que se genera y se gestiona por la organización tenga unas garantías razonables y adecuadas de autenticidad y fiabilidad.
- Principio de protección: debe construirse un programa de gobernanza de la información para asegurar un nivel razonable de protección para los documentos de archivo y la información que son privados, confidenciales, secretos, clasificados o esenciales para la continuidad del negocio, así como para los que requieran cualquier otro tipo de protección.
- Principio de conformidad: debe construirse un programa de gobernanza de la información para cumplir con las leyes aplicables y otras obligaciones, así como también con las políticas de la organización.
- Principio de disponibilidad: la organización debe mantener documentos de archivo e información de modo que se asegure su recuperación oportuna, eficiente y precisa cuando sea necesario.
- Principio de retención: la organización debe mantener documentos de archivo e información durante un tiempo apropiado, teniendo en cuenta los requisitos legales, fiscales, operacionales e históricos.
- Principio de disposición: la organización debe proporcionar seguridad y una adecuada disposición de los documentos de archivo y la información que no deban conservarse, mediante la aplicación de la legislación y de las políticas de dicha organización.
- Principio de transparencia: las actividades y procesos de una organización, incluyendo el programa de gobernanza, deben documentarse de manera abierta y verificable. Dicha documentación debe estar disponible para todo el personal y para las partes interesadas que corresponda.

Estos principios no están dirigidos a ninguna situación, industria, país u organización específicos ni tampoco tienen la intención de describir un conjunto de normas legales de obligado cumplimiento, sino que lo que pretenden es establecer un conjunto de características de un programa efectivo para la gobernanza de la información, permitiendo la flexibilidad (ARMA International 2014, p. 3).

Por su parte, según los estándares internacionales, la gestión de documentos se basa en los siguientes principios (AENOR 2016, p. 9):

- La creación, captura y gestión de los documentos es parte integral de la gestión de la organización en cualquier contexto.
- Los documentos, con independencia de su forma o estructura, son evidencia fidedigna de la actividad de la organización cuando tienen las características de autenticidad, fiabilidad, integridad y usabilidad.
- Los documentos constan de contenido y metadatos que describen el contexto, el contenido y la estructura de dichos documentos, así como de su gestión a través del tiempo.
- Las decisiones relativas a la creación, captura y gestión de los documentos están basadas en la apreciación del riesgo de las actividades de la organización, en su contexto legal, y social.
- Los sistemas para gestionar documentos, con independencia de su grado de informatización, permiten la

aplicación de los instrumentos de gestión de documentos y la ejecución de los procesos para la creación, identificación y gestión de dichos documentos. Estos dependen de las políticas y las responsabilidades que se hayan definido, y de la supervisión y la formación establecida para poder cumplir con los requisitos de gestión de documentos.

Los principios de la organización ARMA se consideran más generalistas que los consignados en los estándares internacionales, que detallan aspectos concretos de la gestión de documentos. Puede, por tanto, darse una complementariedad entre ambos grupos de principios, siendo los primeros considerados un marco general de actuación, y los segundos, requisitos más concretos sobre la documentación, información y aplicaciones informáticas de las organizaciones. De hecho, ARMA afirma que las organizaciones deberán implementar estándares para poder cumplir con sus principios, puesto que, sin la adhesión a estos estándares y principios, no pueden llevar a cabo sus operaciones de la manera más eficiente y efectiva posible, ni tampoco pueden asegurar o demostrar que han cumplido con los requisitos legales o normativos, así como con sus deberes y responsabilidades (ARMA International 2014, p. 2) y esto tiene unas consecuencias.

Se destacan dos principios, uno de cada modelo. Por una parte, ARMA incluye la documentación y transparencia de los sistemas de gestión documentales como un principio más. No se limita a la transparencia clásica, sobre la actividad y las funciones de las organizaciones, sino que incorpora esta obligación moral para los gestores de información, teniendo el deber de hacer pública la información sobre procesos, aplicaciones y sobre el sistema de gestión documental en general, cuando así se requiera. Por otro lado, ISO afirma que las decisiones en relación a la gestión de documentos e información debe basarse necesariamente en la apreciación del riesgo²¹, integrando esta práctica en la gestión documental.

En las organizaciones en que la gestión documental no se realiza de manera adecuada, los documentos archivísticos a menudo resultan inadecuados para los propósitos para los que se necesitan, se pierden con frecuencia y existe la posibilidad de que algunos puedan destruirse de manera prematura y/o se conserven cuando ya no son necesarios. Esto puede ocasionar una serie de consecuencias, como por ejemplo (Shepherd & Yeo 2003, p. XIII):

- Incapacidad de la organización para demostrar que realizó aquello que se requería, o que las políticas y procedimientos se han seguido de manera correcta.
- Incapacidad para defenderse en caso de quejas contra sus productos o servicios, o contra las acciones de sus empleados.
- Incapacidad de probar sus derechos o proteger sus activos.
- Las actividades de la organización pueden verse comprometidas si no se dispone de información crítica cuando se necesite.
- Los derechos de los clientes, ciudadanos y la comunidad en general, pueden quedar perjudicados.

²¹ – La apreciación del riesgo se define como el proceso global que comprende la identificación del riesgo, el análisis del riesgo y la evaluación del riesgo (AENOR 2010, p. 10).

Estos son algunos ejemplos²² de las consecuencias derivadas de una mala gestión documental en cualquier organización. Una adecuada gestión aumentará la capacidad para garantizar que los documentos de archivo estén disponibles cuando se necesiten, que la privacidad y la confidencialidad se mantengan y que los documentos duplicados e innecesarios se eliminen (Shepherd & Yeo 2003, p. XIII) siguiendo el marco legal y normativo establecido.

1.3.1 Procesos de gestión documental

Dentro de esta gestión se engloban distintos procesos que abarcan el ciclo de vida de los documentos. Para esta investigación se parte de los procesos identificados y definidos en los estándares internacionales, como son las normas de la familia ISO 30300 y la norma ISO 15489. Estos son: creación, captura, clasificación e indización, acceso, almacenamiento, uso y reutilización, migración o conversión, y disposición.

Creación y captura

Los documentos se crean, o se reciben y se capturan, con el fin de llevar a cabo las actividades de la organización. De hecho, la creación de documentos es la primera actividad que captura, de una manera formal, las decisiones tomadas por individuos, que llevan a cabo transacciones y toman decisiones como parte del día a día de su organización, de las que son responsables y sujetos de la rendición de cuentas (Duranti & Franks 2015, p. 305).

Para analizar las necesidades sobre qué documentos deben crearse y capturarse²³, lo principal debe ser la identificación y el análisis de (Shepherd & Yeo 2003, p. 102):

- Los requisitos de la organización, o de las unidades de negocio específicas, para los documentos archivísticos que proporcionan evidencia e información para su uso operacional.
- Los requisitos de la organización, de unidades de negocio específicas o de accionistas externos para las evidencias que dan soporte a la rendición de cuentas.
- Los costes de crear, capturar y mantener los documentos de archivo que se requieran, así como el riesgo de la organización de no contar con esos documentos.

²² – Algunos casos concretos son los casos de: *Arthur Andersen*, *Enron Account*, en relación con fraude y corrupción; la Comisión del 11 de septiembre, en relación al terrorismo; el caso *Bichard*, en relación a abusos sexuales y asesinato de menores; entre otros. En todos ellos se aludió a una mala praxis en la gestión de los documentos, ya fuese por ocultación, eliminación, manipulación, entre otras. Con una buena gestión de la información y los documentos se podría haber contribuido a la prevención de estos hechos.

²³ – En la captura se incluyen tanto los documentos creados por la organización, como los recibidos en el ejercicio de sus funciones.

Los gestores de documentos necesitan alejarse de la idea del documento de archivo como un instrumento tan solo con funciones administrativas o históricas para entenderlo como un activo crítico, tanto de la organización como de la sociedad (Cox 2001, p. 44). Estos proporcionarán servicio a las actividades de la organización, pero también evidencia a lo largo del tiempo. Asimismo, podrán servir como fuente primaria en los procesos de rendición de cuentas, internos y externos, para una sociedad más informada y participativa. Para que esto sea posible, la creación de documentos debería implicar tanto la creación de contenido como de metadatos que documenten las circunstancias de su creación (AENOR 2016, p. 24). Estos metadatos deben fijarse y mantenerse como evidencia de la actividad que refleja el documento, para que este pueda traspasar el ámbito funcional que lo originó y adquirir nuevos valores en contextos distintos.

El término “creación” aplicado a los documentos de archivo requiere de la comprensión del quién, del qué, del cuándo, del dónde, del por qué y del cómo un documento se crea, puesto que la creación no ocurre sin más. La creación de un documento depende de, interactúa con, y también impacta en otras acciones de gestión documental, incluyendo la captura, la gestión, el uso, la preservación y la disposición (Duranti & Franks 2015, p. 305).

Clasificación

La clasificación se define como la identificación y estructuración sistemática de las actividades y/o documentos de las organizaciones en categorías, de acuerdo con convenciones, métodos y normas de procedimiento lógicamente estructurados (AENOR 2016, p. 8). La clasificación es básica para una gestión efectiva de los documentos. El resto de desarrollos en un programa diseñado para controlar documentos estará supeditado a la clasificación (Schellenberg 1996, p. 52).

Existen distintos tipos de clasificación, según si el criterio es funcional u orgánico. En el pasado, los documentos se veían normalmente como productos de un departamento o unidad de negocio específicos y por ello se realizaba una clasificación orgánica. Sin embargo, con el tiempo, se vio claramente que las actividades que se llevan a cabo en cada unidad contribuyen al propósito y las funciones de la organización como un todo, y los sistemas empleados para gestionar los documentos de dichas actividades deben reflejar una perspectiva amplia de la organización (Shepherd & Yeo 2003, p. 74). Se pasó entonces a una clasificación funcional.

Si los documentos se clasifican para reflejar la organización y la función, pueden ser eliminados o conservados en relación a la organización o a la función, y la evidencia que contienen sobre ellas es la primera cuestión a tener en cuenta en la valoración de documentos públicos. Tanto los archiveros como los trabajadores públicos tienen en cuenta el valor probatorio de los documentos de archivo para documentar la organización y la función. Si estos documentos se clasifican para reflejar la organización, pueden eliminarse cuando una unidad administrativa haya quedado obsoleta. Y si además están clasificados por función, si se separa aquello significativo de aquello útil, la política de lo operacional y, generalmente, lo importante de lo que no lo es, entonces el método de clasificación proporciona la base para conservar o destruir los documentos de archivo de manera selectiva tras haber servido a los propósitos actuales del negocio (Schellenberg 1996, p. 52).

La clasificación de documentos incluye (AENOR 2016, p. 25):

- Vincular el documento con la actividad que está siendo documentada, en un nivel adecuado (por ejemplo, con una función, actividad o proceso de trabajo).
- Establecer vínculos entre documentos individuales y grupos de documentos, para documentar en todo momento las actividades de la organización.

El proceso de clasificación es el acto de vincular un documento a su contexto. Además de lo mencionado anteriormente, permite la aplicación de reglas de acceso y permisos, la ejecución de reglas de disposición adecuadas y la migración de documentos de una función o actividad concreta a un nuevo entorno como resultado de la reestructuración administrativa (AENOR 2016, p. 22).

Acceso

Los documentos se conservan para poder ser accesibles por usuarios autorizados cuando así sea requerido (Shepherd & Yeo 2003, p. 216). El acceso se define como el derecho, modo y medios de localizar, usar o recuperar información (AENOR 2016, p. 7). Varía a lo largo del ciclo de vida y se ve influenciado por cómo se usa el documento, por políticas corporativas y por leyes aplicables sobre acceso y publicación (Duranti & Franks 2015, p. 1).

La finalidad del acceso sobrepasa los límites de la organización, y se hace partícipe también a la ciudadanía y a otras organizaciones, sobre todo para la información gestionada por los organismos públicos, puesto que la legislación obliga a permitir el acceso a dicha información, así como a publicaciones periódicas sobre cuestiones concretas y que deben ser de acceso público. El derecho de los ciudadanos a acceder a la información y documentación pública es un aspecto esencial de la relación entre estos ciudadanos y los poderes públicos en una sociedad democrática. Los derechos propios de una sociedad democrática necesitan, para su materialización, una práctica efectiva del acceso a la información pública (Capell i Garriga & Corominas i Noguera 2009, p. 437). Sin embargo, una ley de transparencia no puede ser efectiva si los documentos son incompletos o no existen (Roberts 2006, p. 111). Es básico, además, ser capaz de recuperar la información y los documentos. La posibilidad de éxito de la accesibilidad debe vincularse de manera ineludible a la existencia de unos documentos organizados, descritos de manera estandarizada, preservados en su autenticidad, fiabilidad e integridad (Alberch i Fugueras 2013, p. 24).

Almacenamiento

Los documentos, con independencia de su formato o soporte, deberían almacenarse de modo que estén protegidos contra el acceso no autorizado, las alteraciones, la pérdida o la destrucción, incluyendo el robo y las catástrofes (AENOR 2016, p. 25). Esto se relaciona directamente con la adecuada conservación y preservación de los documentos, así como con la gestión de riesgos. No se trata tan solo de ordenar y mantener los documentos en un espacio (físico o virtual), sino de mantener sus características inalterables a lo largo del tiempo. Esto implica que deberían implementarse ciertas medidas para garantizar los siguientes aspectos (AENOR 2016, p. 25):

- Entorno/s y soportes de almacenamiento adecuados.
- Uso de materiales para la protección física y procedimientos especiales de manipulación cuando sea necesario.
- Protección y supervisión rutinarias de la seguridad física y de la información.
- Desarrollo y verificación de procedimientos definidos para la planificación y recuperación ante catástrofes y la formación pertinente del personal en estos aspectos.

Uso y reutilización

Los sistemas de gestión documental deberían diseñarse para permitir un uso fácil de los documentos (AENOR 2016, p. 26). Los documentos deben ser usables durante todo el tiempo en que son conservados.

La reutilización de la información reconoce el derecho de los particulares y organizaciones a reutilizar la información del sector público para finalidades comerciales, reconocimiento que pretende favorecer iniciativas económicas por parte del sector privado a partir de la información, los datos y los documentos de los que dispone el sector público (Capell i Garriga & Corominas i Noguera 2009, p. 440). La reutilización del contenido de un documento como parte de una operación de negocio (en otros procesos de trabajo internos o externos) crea un nuevo documento en un nuevo contexto, con metadatos independientes en el momento de la captura y en los procesos de gestión (AENOR 2016, p. 26).

Migración y conversión

La conversión se define como el proceso de transformación de los documentos de un formato a otro. La migración, por su parte, es el proceso de transferencia de los documentos de un sistema de *hardware* o *software* a otro sin modificar su formato (AENOR 2016, p. 8).

Durante la migración o la conversión, todo el contenido del documento y sus metadatos asociados en la aplicación o formato de origen deberían conservarse hasta que el proceso se termine y la integridad y fiabilidad de la aplicación o formato de destino haya sido controlada y asegurada (AENOR 2016, p. 26).

Disposición

La disposición se define como la serie de procesos asociados con la aplicación de decisiones de transferencia, destrucción o conservación de los documentos, que se documentan en los calendarios de conservación y otros instrumentos (AENOR 2016, p. 8) como, por ejemplo, las tablas de valoración documental o de retención documental.

Se parte de la premisa de que no todos los documentos deben conservarse de manera permanente. Los sistemas de gestión documental se basan en el tratamiento eficiente de los documentos y, para alcanzar esta finalidad, uno de sus principios es determinar el periodo de conservación de los documentos, distinguiendo aquellos que serán de conservación permanente de los que deben ser destruidos en un plazo concreto (Capell i Garriga & Corominas i Noguera 2009, p. 190). Se conserva para informar, y en este proceso se trata de evaluar la cantidad y la calidad informativa de los documentos, para decidir uno u otro destino (Cruz Mundet 2012, p. 276). Para ello deben conocerse los valores de los documentos, puesto que, en caso de decidir su eliminación, se debe tener en cuenta que la destrucción es un proceso que no permite la reconstrucción de la información.

La valoración documental debe llevarse a cabo por un grupo de expertos multidisciplinar, no debe ser nunca una decisión individual del gestor de documentos de la organización. Se trata de un proceso analítico donde se distinguen los distintos valores que poseen los documentos para decidir, de manera fundamentada, qué documentos de un conjunto serán los que se deberán conservar de manera permanente. Se debe tener presente que el resultado final de la valoración es el de conservar una determinada documentación que contendrá una información que en el futuro deberá permitir la interpretación de nuestra sociedad (Capell i Garriga & Corominas i Noguera 2009, p. 190), por lo que no es una tarea fácil ni debe caer en la subjetividad.

Los últimos estándares publicados explican que la valoración no solo se refiere a la decisión final sobre la conservación o eliminación de los documentos, sino que se trata del proceso de evaluar las actividades de la organización para determinar qué documentos necesitan crearse y capturarse, y por cuánto tiempo es necesario conservarlos (AENOR 2016, p. 17). De esta manera, se amplían los usos tradicionales del término (explicados anteriormente) para incluir el análisis del contexto de la organización, sus actividades y los riesgos, con el fin de permitir la toma de decisiones sobre qué documentos crear y capturar, y cómo se asegurará su gestión adecuada a lo largo del tiempo (AENOR 2016, p. 18). Esta visión no contradice la tradicional, sino que la complementa. Si bien es cierto que en los procesos de valoración ya se incluía el estudio del contexto, no se aplicaba este análisis a la decisión sobre la creación y captura de documentos, sino que se aplicaba tan solo a la disposición entendida como la decisión de conservar o eliminar al final del proceso.

Dentro del proceso de disposición, los estándares internacionales también incluyen los subprocesos de transferencia de documentación. Esto se refiere al cambio de la custodia o propiedad de los documentos, incluyendo los metadatos. También puede incluir el traslado de los documentos desde una localización a otra (AENOR 2011, p. 16).

Descripción

Se entiende por descripción archivística la elaboración de una representación esmerada de una unidad de descripción y, en su caso, de las partes que la componen, mediante la recopilación, el análisis, la organización y el registro de cualquier información que sirva para identificar, gestionar, localizar y explicar los documentos de archivo, proporcionando también información sobre su contexto de creación y el sistema a partir del cual han sido organizados (NODAC 2007, p. 15).

Este proceso no se incluye en la norma ISO 15489 del año 2016. Sin embargo, sí se incluye la posibilidad de utilizar metadatos de indización para hacer que los documentos sean más fácilmente recuperables. Los metadatos de indización, como lugares geográficos, materias o nombres de personas, pueden vincularse a los documentos en el momento de la captura, o pueden añadirse cuando sea necesario a lo largo de su existencia (AENOR 2016, p. 25).

La descripción resulta clave para otros procesos como el acceso o la disposición. Mientras el documento de archivo (en oposición a la mera información) tenga un rol dentro de la actividad humana, la recopilación y preservación de los datos que establecen su identidad e integridad (y la presentación clara de estos datos) permanece una parte esencial de la responsabilidad archivística (Duranti & Franks 2015, p. 39). Estos datos son los que describen los documentos, los metadatos.

La descripción es una de las tareas básicas de la organización archivística de los documentos, puesto que se trata de la acción que hace de puente entre el documento y las personas interesadas en su contenido. Mantiene la vinculación con el contexto y asegura la autenticidad de los documentos. Por ello, la descripción se convierte en una de las herramientas fundamentales para facilitar el acceso y la consulta de la documentación y, en este sentido, permite cumplir con una de las funciones esenciales de la archivística: comunicar, hacer posible la obtención de la información contenida en documentos (Capell i Garriga & Corominas i Noguera 2009, p. 154). Es una herramienta que se aplica en todas las etapas del ciclo de vida de los documentos, desde que se inician con la gestión administrativa en adelante, de manera que la descripción realizada al comienzo puede ser utilizada y transferida con los documentos en las siguientes etapas, añadiendo, modificando, mejorando cuanto sea necesario (Cruz Mundet 2012, p. 232). Cuando se describe, los archiveros están capturando, recopilando, analizando y organizando información sobre todo el sistema de gestión documental (Duranti & Franks 2015, p. 39).

1.3.2 Instrumentos de gestión documental

En la implantación y gestión de los procesos mencionados es fundamental disponer de una serie de instrumentos de gestión documental, para facilitar el cumplimiento de los requisitos de gestión de documentos. Estos instrumentos se pueden diseñar e implementar de distintas formas, dependiendo del entorno tecnológico y de negocio. Su diseño e implementación debería tener en cuenta las características de las aplicaciones de gestión documental con las que deberían interactuar (AENOR 2016, p. 20).

Del mismo modo que con los procesos, para la definición de los instrumentos se parte de aquellos identificados en los estándares internacionales, como son las normas de la familia ISO 30300 y la norma ISO 15489. Estos son: política de gestión documental, esquema de metadatos, cuadro de clasificación, cuadro de seguridad y acceso, calendario de conservación, catálogo de tipologías documentales, catálogo de formatos y registro de eliminaciones. Los instrumentos enumerados, pese a provenir de estándares internacionales ampliamente aceptados, no son los únicos que pueden emplearse para la gestión documental en una organización. A este listado pueden añadirse, por ejemplo, el modelo de gestión documental y la tabla de documentos esenciales, entre otros. El desarrollo de unos instrumentos u otros depende de las necesidades de cada organismo.

El modelo de gestión documental, pese a no recogerse en la bibliografía, es una herramienta clave de cualquier sistema de gestión documental, que tiene como objetivos principales unificar criterios y normalizar la gestión de documentos mediante el establecimiento de unas directrices claras. El modelo de gestión documental parte de la comprensión del contexto y se adapta a cada organización. Necesita del compromiso de todos los actores implicados, principalmente de los ámbitos de organización, tecnológico, jurídico y de gestión documental.

El modelo suele depender de la existencia de una política de gestión documental definida en la organización. Este instrumento marca las bases y estructura el sistema para poder desarrollar tanto instrumentos de gestión documental como herramientas tecnológicas que permitirán a la organización trabajar de manera eficaz y eficiente en relación a su información y documentación.

Política de gestión documental

El primer instrumento es la política de gestión documental, que es la base sobre la que se sustenta el sistema. Esta no se relaciona directamente con ningún proceso, aunque es el marco dentro del que se desarrollarán los instrumentos necesarios. Se trata de un documento en el que consta la declaración de intenciones de la organización en relación con la gestión de los documentos. En algunos casos, también puede incluirse el plan de actuación e incluso procedimientos sobre cómo cumplir con los requisitos aplicables. Existen múltiples formas de este tipo de documento, desde las más sencillas que constan de una o dos páginas, únicamente con la declaración de intenciones²⁴ (son las que siguen el modelo MSS²⁵ de ISO) hasta las más complejas, incluso con más de 300 páginas, que incluyen los roles y responsabilidades de los trabajadores, los procesos, la formación, algunos procedimientos, entre otras cuestiones²⁶. La política debe adaptarse a las necesidades de la organización que la desarrolla.

²⁴ – Un ejemplo de este tipo de políticas es la Política de Gestión Documental y Archivo de la Universidad del País Vasco: <https://www.ehu.eus/es/web/idazkaritza-nagusia/dokumentuak-gestionatu-eta-artxibatzeko-politika> (consultado el 11/02/2018). Otro ejemplo es la Política de Gestión de Documentos de la Universidad de Lleida: http://www.udl.cat/export/sites/universitat-lleida/ca/serveis/arxiu/galleries/docs/Servei_Arxiu_Documents/Politica_gestio_cast.pdf (consultado el 11/02/2018).

²⁵ – MSS se corresponde con *Management System Standards* según la organización ISO. Según esta organización, un sistema de gestión se define como un conjunto de elementos interrelacionados o que interactúan en una organización con el fin de establecer políticas y objetivos, y los procesos para alcanzarlos (AENOR 2011, p. 16).

²⁶ – Un ejemplo de este tipo de políticas es la Política de gestión de documentos electrónicos del Ministerio de Hacienda y Administraciones Públicas del Gobierno de España: http://www.minhfp.gob.es/Documentacion/Publico/SGT/POLITICA%20DE%20GESTION%20D_E%20DOCUMENTOS%20MINHAP/politica%20de%20gestion%20de%20documentos%20elect_ronicos%20MIN-HAP.pdf (consultado el 11/02/2018). Otro ejemplo es la Política de Gestión Documental de la Diputación de Barcelona: https://seu-electronica.diba.cat/serveis-de-la-seu/gestio-documental/fitxers/D6459_14_Politica_GDocumental.pdf (consultado el 11/02/2018).

Esquema de metadatos

Es el instrumento que identifica los metadatos, obligatorios y opcionales, que deben informarse en el momento de la captura y durante la gestión de los documentos. Debe desarrollarse para definir qué metadatos se usan para identificar, describir y gestionar procesos de gestión de documentos. Los esquemas de metadatos pueden relacionarse con diferentes entidades. Las entidades clave para gestionar documentos son las siguientes (AENOR 2016, p. 20):

- Documentos, incluyendo todos los niveles de agrupación.
- Agentes, incluyendo personas, unidades de negocio, tecnologías o aplicaciones de gestión documental y corporativas.
- Actividades de la organización, como funciones de negocio, actividades y operaciones o procesos de trabajo.
- Regulaciones, como leyes u otros requisitos que regulan las actividades de la organización y la creación o gestión de los documentos.
- Relaciones, entre entidades y niveles de agrupación.

La importancia de los metadatos radica en la mejora de la identificación y recuperación de los documentos, así como en la posibilidad de relacionar políticas, reglas de acceso, permisos o derechos con los documentos. También contribuyen a mantener información sobre la trazabilidad de las acciones y procesos llevados a cabo sobre los documentos, aumentando la fiabilidad de la información en los procesos de rendición de cuentas.

Cuadro de clasificación

Es el instrumento que permite identificar todos los documentos con los asuntos para los que han sido creados, así como agruparlos físicamente o intelectualmente en los expedientes. Debe tener en cuenta los siguientes aspectos (Capell i Garriga & Corominas i Noguera 2009, p. 140):

- Debe ser capaz de englobar toda la documentación independientemente de la fecha de generación y de su soporte.
- La construcción de un cuadro de clasificación debe estar precedida por la identificación de las series, el estudio de la historia y la estructura de la institución.
- La recuperación de la información referente al ordenamiento jurídico: leyes y normas, tanto internas como externas.
- La recuperación de los documentos relativos a manuales de procedimiento administrativo y las normas de organización interna (circulares, directrices, entre otros), memorias administrativas o inventarios.
- La selección de los niveles jerárquicos necesarios atendiendo a las necesidades de organización del fondo.
- Toda agrupación documental debe tener una entrada concreta y única en el cuadro de clasificación.

Los documentos se generan en el curso de las actividades de una organización y estos proporcionan evidencia de dichas actividades, que a su vez forman parte de una instancia mayor, como es la función de la que la actividad forma parte. Por ello, los cuadros de clasificación basados en funciones, procesos y actividades conectan firmemente los documentos con el contexto de su creación (Shepherd & Yeo 2003, p. 74).

Los cuadros de clasificación se basan en el análisis de las funciones, procesos y actividades. Documentan las relaciones entre los documentos y las actividades que los han generado. Proporcionan una base esencial para el control intelectual de los documentos y para facilitar su gestión a lo largo del tiempo. Las funcionalidades primarias de un cuadro de clasificación son (Shepherd & Yeo 2003, p. 73):

- Proporcionar relaciones entre documentos que derivan de una misma actividad o de actividades relacionadas.
- Determinar cuándo un documento debe incluirse en una agregación mayor de documentos.
- Ayudar a los usuarios a recuperar documentos.
- Ayudar a los usuarios a interpretar los documentos.

También resultan útiles para proporcionar el marco en el que determinar, evaluar y documentar las responsabilidades de custodia, los derechos de acceso, las precauciones de seguridad y los periodos de retención. Es por ello que la clasificación es un proceso esencial en la gestión de documentos, que mantiene la influencia a lo largo de la existencia del documento. Por todo lo anterior, el cuadro de clasificación debe ser lo más estable posible, de modo de la clasificación dada al fondo perdure en el tiempo. También debe ser objetivo, es decir, que no dependa tanto de la percepción que el archivero pueda tener en cuanto a aspectos inequívocos. Por último, debe sustentarse en un criterio que emane de la propia naturaleza de los documentos, del proceso administrativo del cual son resultado (Cruz Mundet 2012, p. 216).

Cuadro de seguridad y acceso

Para regular los accesos se desarrolla un instrumento llamado “cuadro de roles y permisos” o “cuadro de seguridad y acceso”. Se trata de un conjunto de reglas que identifican derechos de acceso y el régimen de permisos y restricciones aplicables a los documentos (AENOR 2016, p. 22). Cuanto más compleja, o de mayor volumen, sea la organización, mayor será la necesidad de disponer de este instrumento para garantizar los accesos controlados y la seguridad adecuada de la información. Esta puede describirse como el nivel de seguridad que, según el sentido común, se necesitaría para proteger la información de cualquier acceso, recopilación, utilización, divulgación, supresión, modificación o destrucción no autorizados (AENOR 2006, p. 19).

La seguridad se vincula directamente con la clasificación, puesto que en el momento de la captura de un documento, mediante la vinculación establecida por la clasificación, este debe incorporar las restricciones en relación a su acceso, la posibilidad de realizar agregaciones, las vinculaciones con los procesos de negocio de la organización o con los diferentes agentes implicados (Capell i Garriga & Corominas i Noguera 2009, p. 342).

Calendario de conservación

Es el instrumento que permite difundir las reglas de conservación y que establece los plazos de retención de los documentos en las sucesivas fases del ciclo de vida, así como su disposición final. Las reglas de conservación son normas establecidas a partir de la determinación de los valores primario y secundario que presentan los documentos (Capell i Garriga & Corominas i Noguera 2009, p. 257).

El calendario de conservación también puede contener instrucciones acerca del momento en que los documentos se deberían transferir de un entorno de almacenamiento a otro o para la conservación continuada de documentos por parte de la organización responsable (AENOR 2016, p. 23).

Este instrumento se construye sobre una base de investigación que combinará las necesidades y requisitos de la valoración documental junto con los procedimientos administrativos y los recursos de la organización capaces de dirigir los requisitos de transferir, almacenar, eliminar y/o preservar los documentos (Duranti & Franks 2015, p. 182).

Catálogo de tipologías documentales

Es el instrumento que categoriza todas las clases de documentos que gestiona una organización. Permite identificar los tipos documentales, contribuyendo a la identificación homogénea de los documentos y a normalizar su nomenclatura. Se entiende por tipos o tipologías documentales la expresión tipificada de unidades documentales con unas características estructurales, en general, homogéneas, de actuaciones únicas o secuenciales, normalmente reguladas por una norma de procedimiento, derivadas del ejercicio de una misma función y realizadas por un determinado órgano, unidad o persona con competencia para ello (Duplá del Moral 2005, p. 84).

La importancia de este instrumento radica en el uso de una misma terminología para referirse a los documentos, lo que puede contribuir a que todos los actores implicados en proyectos de gestión documental (incluidos los usuarios finales) hablen un mismo lenguaje (Departament de Cultura 2015, p. 9). Además, permite el desarrollo de formatos normalizados (plantillas) de los documentos, lo que facilita la gestión.

Catálogo de formatos

Es el instrumento donde se indican los formatos aceptados o normalizados de los documentos para una organización. Para conseguir un tratamiento integral de los documentos y expedientes electrónicos de una organización, es necesario sistematizar los formatos aceptados o normalizados con base en estándares internacionales y en las convenciones normativas aplicables.

El catálogo de formatos permite, además, establecer medidas de preservación de documentos electrónicos a largo plazo. También facilita los procesos de conversión, cuando es necesario.

Registro de eliminaciones

Es el instrumento donde se guarda evidencia de la documentación eliminada por una organización. Es una herramienta básica de todo el sistema de gestión documental. El registro recopila la información relativa a las diferentes destrucciones documentales que se han ido ejecutando (Capellades *et al.* 2016, p. 13). Los documentos que se van a eliminar deben identificarse y consignarse en un registro para autorizar su destrucción. De esta manera, se deja evidencia documental del proceso llevado a cabo.

Este instrumento se relaciona directamente con el proceso de disposición y con el calendario de conservación. Sin un trabajo previo de valoración documental y toma de decisiones sobre qué debe conservarse y qué puede eliminarse, no puede llevarse a cabo la destrucción y, por tanto, el registro de eliminaciones carece de sentido.

Tabla de documentos esenciales

Es el instrumento en el que se identifican los documentos imprescindibles de un organismo y los que se deben proteger de manera especial frente a un eventual siniestro. Los documentos esenciales se definen como aquellos documentos de emergencia y operacionales que serán necesarios, de manera inmediata, para iniciar la recuperación de las operaciones tras un desastre, y como los documentos de derechos e intereses necesarios para proteger los activos, las obligaciones y los recursos de la organización, así como también a los empleados y a los clientes o los ciudadanos (Pearce-Moses 2005, p. 151). Disponer de un listado de este tipo de documentos para favorecer un mejor control es un aspecto crítico para cualquier organización.

1.4 Transversalidad de la gestión documental

Para el diseño e implantación de un sistema de gestión documental adecuado (que incluye los procesos e instrumentos anteriormente explicados), las organizaciones necesitan tener en cuenta una serie de cuestiones como: el desarrollo de políticas, el análisis de procesos, la gestión de proyectos, la gestión del cambio, la gestión de riesgos, la continuidad del negocio, la capacitación de las personas, la gestión de la calidad, la configuración de las herramientas informáticas, así como una cultura organizativa preparada para trabajar la gestión documental desde el plano estratégico. No se trata tan solo de comprar tecnología y ponerla en funcionamiento, sino que hay otras cuestiones, también transversales, que son de vital importancia para alcanzar el éxito.

El desarrollo de políticas parte de las necesidades de la organización, en relación con los requisitos normativos y legales que esta debe cumplir sobre la gestión de la información que genera y gestiona. Esto incluye las políticas relativas a las responsabilidades de gestión documental, así como también una política de gestión documental estratégica. Se puede desarrollar una única política generalista o varias en relación con distintos aspectos, como pueden ser la

preservación, la firma electrónica, la eliminación de documentos, entre otros. La decisión depende de la estrategia de implantación de la organización.

El análisis de procesos se emplea para recopilar información sobre las operaciones, procesos y funciones de una organización con el fin de identificar los requisitos para la creación, incorporación y control de los documentos (AENOR 2008, p. 7). Este análisis describe y analiza qué ocurre en una función, en un contexto específico de negocio. No puede realizarse en abstracto, sino que depende de la detallada recopilación de información y la comprensión bien fundamentada del contexto y la misión de la organización (AENOR 2008, p. 5).

El análisis de procesos ayuda al desarrollo y mejora del cuadro de clasificación corporativo mediante el conocimiento en profundidad de sus funciones, actividades y sus vínculos con los documentos. Según el nivel de detalle con que se realice, se pueden especificar los documentos necesarios para cada proceso de trabajo, minimizando las posibles desviaciones a la hora de desempeñar las actividades del día a día. Integrar los procesos de gestión de documentos en protocolos automatizados, que se integran en los procesos de trabajo, garantizará que los documentos de la organización sean creados, incorporados y controlados sistemáticamente en sus sistemas de negocio (AENOR 2008, p. 5).

La gestión de proyectos implica llevar un control exhaustivo sobre la implantación y el mantenimiento del sistema de gestión documental en la organización, incluyendo la definición de roles y responsabilidades, y los calendarios de actuación. Se incluye aquí también la gestión del cambio, puesto que en la implantación de los sistemas de gestión se realiza una modificación de metodologías y procedimientos a nivel organizativo, que es necesario gestionar de manera que se minimice al máximo la resistencia al cambio de las personas.

También relacionado con la gestión del proyecto, se puede incluir el análisis de su continuidad y viabilidad. No hay que olvidar que, una vez la implantación se ha llevado a cabo, es necesario dedicar recursos y esfuerzos al mantenimiento del sistema. Es aquí donde cobran una especial importancia la valoración y el análisis del proyecto de futuro que se quiere para la organización.

En relación con la gestión del cambio, no debe olvidarse el factor humano en el desarrollo, implantación y mantenimiento de los sistemas de gestión documentales. Se deben planificar acciones informativas, formativas y de concienciación de manera continua y dirigidas a los profesionales, según sus perfiles y sus responsabilidades dentro del sistema. Estas acciones formativas deben incluir formación sobre requisitos, políticas, prácticas, roles y responsabilidades para la gestión de documentos, y deben dirigirse a todos los miembros de la dirección y del personal, así como a cualquier otra persona responsable de cualquier parte de la actividad de la organización que implique la creación, captura y gestión de los documentos (AENOR 2016, p. 17). Esto ayuda a minimizar riesgos de fallos, ya sea por desconocimiento, incompetencia u otro tipo de causas.

La capacitación de las personas debe ser continuada y no debe dejar al margen a nadie. Es fundamental que se exija a las organizaciones desarrollar y potenciar la capacitación técnica del personal afectado por la implantación y por el funcionamiento del sistema de gestión documental, puesto que son estas personas las que deben ser capaces y competentes, a lo largo del tiempo, de trabajar dentro del sistema sin que se produzcan fallos e incidencias graves. La formación puede entenderse también como una estrategia de prevención de riesgos del sistema.

Cabe recordar que la gestión de riesgos opera como un pilar central de la práctica de la gestión documental, y que es parte de los marcos de conformidad, gobernanza y riesgo que cada vez más dominan el pensamiento de la gestión de documentos (Duranti & Franks 2015, p. 369). Se incluye aquí, como un elemento más de la implantación, que no solo se lleva a cabo con esta finalidad, sino que se debe incorporar una valoración de riesgos continua posterior a la implantación en el marco general de gestión de riesgos de la organización (Associació d'Arxivers - Gestors de Documents de Catalunya 2012, p. 30).

La gestión del riesgo se puede aplicar a la totalidad de una organización, a todas sus áreas y niveles principales, en todo momento, así como a las funciones, los proyectos y las actividades específicas (AENOR 2010, p. 5). Es responsabilidad de cada organización decidir el alcance de la gestión de riesgos en relación con la gestión documental, sin olvidar los beneficios indirectos que puede aportar esta integración a la mejora global del organismo.

En este sentido, se incorporan la gestión del cambio y la gestión de riesgos como dos aspectos de suma importancia, tanto para el diseño y la implantación del sistema, como para su posterior mantenimiento. De este modo, la gestión documental deja de entenderse como una práctica aislada, o autónoma, dentro de las organizaciones para trabajarse en consonancia con otros procesos y proyectos, que le sirven como apoyo y a los que da apoyo.

La gestión de la calidad se relaciona con el control del proceso de implantación y del rendimiento de las aplicaciones informáticas a partir de una serie de criterios definidos previamente. Del mismo modo que la gestión de riesgos, no es un aspecto que deba olvidarse una vez implantado el sistema, sino que debe permanecer en el tiempo para asegurar la calidad y para alcanzar la mejora continua. Además, puede aprovecharse la gestión de la calidad mediante la integración del sistema de gestión documental, como un sistema integrado de gestión para la organización.

En relación con la tecnología, es necesario garantizar que las aplicaciones informáticas no solo tengan las capacidades de gestión de documentos necesarias, sino que, además, estas capacidades se configuren correctamente para adecuarlas al funcionamiento de la infraestructura informática de la organización (Associació d'Arxivers - Gestors de Documents de Catalunya 2012, p. 31). Las aplicaciones de gestión documental pueden estar diseñadas específicamente para gestionar documentos, o pueden ser aplicaciones diseñadas para gestionar otros procesos de negocio y estar adaptadas también para soportar la creación, captura y gestión de los documentos (AENOR 2016, p. 13).

Por último, es vital que la cultura organizativa refuerce el valor y la importancia de una adecuada gestión de documentos y que genere expectativas por parte de todos los trabajadores de la organización. Estas expectativas deben reforzarse periódicamente también a través de los responsables de los departamentos, y canalizarse a través de la dirección ejecutiva (Associació d'Arxivers - Gestors de Documents de Catalunya 2012, p. 31). Al fin y al cabo, en muchos casos se trata de un proceso de cambio de la cultura organizativa y, por este motivo, es muy necesario concienciar y acompañar a los trabajadores en este proceso de cambio cultural.

1.5 Normalización y certificación de la gestión de documentos

La normalización tiene como objetivo la elaboración de una serie de especificaciones técnicas (conocidas como “normas” o “estándares”) que son utilizadas por las organizaciones, de manera voluntaria, como referencia para probar la calidad y la seguridad de sus actividades y productos. Lo interesante de seguir estas normas o estándares es poder demostrar y garantizar, frente al cliente o usuario final, que el producto o servicio que se ofrece responde a unos requisitos mínimos de calidad, diferenciándolo de otros. Un sistema normalizado es siempre un sistema de mayor rigor, calidad y exigencia que otro que no esté normalizado, si bien es cierto que esto exige, por parte de la organización, un mayor esfuerzo de su personal y de medios con los que poder afrontar la puesta en marcha y el mantenimiento del sistema. Solo un compromiso firme de la organización y de sus directivos puede permitir esto (Núñez Fernández 2007, p. 31).

Una norma es fundamentalmente un consenso, que pretende resolver un problema o facilitar la actividad industrial o económica, alcanzado con garantía de participación de todas las partes interesadas y accesible al público (Brito Marquina 2015, p. 34). Proporciona un punto de partida equitativo, y promueve la competencia y la innovación.

En los últimos años, la gestión documental ha estado inmersa en un proceso de sistematización y normalización como respuesta al aumento exponencial de los documentos generados en las organizaciones, y por la generalización del uso de documentos electrónicos. El comercio y la administración electrónica, junto a la legislación asociada a estas actividades, han evidenciado la necesidad de estándares, normas y recomendaciones para una correcta y eficiente gestión de la documentación. Esta eficiencia en la gestión permite mantener las características de los documentos: autenticidad, fiabilidad, integridad y disponibilidad (Grupo de Difusión del CTN 50-SC1 2012, p. 175) garantizando así su funcionalidad a lo largo del tiempo.

La normalización en gestión documental no se centra exclusivamente en el diseño de sistemas de gestión, sino que va mucho más allá. Existen normas ISO sobre prácticamente todos los aspectos de la gestión documental, desde la captura o la digitalización pasando por la descripción, las evidencias electrónicas, los repositorios virtuales, la preservación digital, o la destrucción. Se puede afirmar que existe una o varias normas para cada fase del ciclo de vida de los documentos. Si bien es cierto que no es necesario trabajar con todas ellas para disponer de un sistema de gestión documental funcional, práctico y eficiente, sí resultan de gran utilidad como instrumentos de trabajo, y así es como deben entenderse.

No todas estas normas son certificables, sino que hasta el año 2011, con la publicación de la familia de normas ISO 30300, no se dispone de un estándar internacional certificable en gestión documental. La norma más importante de esta familia es la *UNE-ISO 30301 – Información y documentación. Sistemas de gestión para los documentos*, que se enmarca dentro de la tipología de normas ISO de Sistemas de Gestión (*Management System Standards, MSS*) certificables, diseñadas para asistir a organizaciones de todo tipo y tamaño en la implementación, operación y mejora de un sistema de gestión efectivo. Esta norma internacional especifica los requisitos que debe cumplir un sistema de gestión para los documentos, con el objetivo de apoyar a la organización en la consecución de sus fines, misión, estrategia y metas. Sitúa la gestión documental como un aspecto a tener en cuenta en las estrategias orientadas a la mejora continua de la gestión empresarial, junto a la calidad, medioambiente, seguridad y prevención de riesgos laborales o seguridad de la información (Grupo de Difusión del CTN 50-SC1 2012, p. 176).

El propósito de implementar un sistema de gestión documental es realizar la gestión sistemática y verificable de los documentos como información acerca de las actividades de la organización (Bustelo Ruesta 2011, p. 11). La importancia de la auditoría, y posible certificación, de estos sistemas radica en que, de esta manera, se proporciona una garantía sobre la transparencia y la trazabilidad de las decisiones tomadas por la dirección y los altos cargos, así como también el reconocimiento de su responsabilidad (AENOR 2011, p. 5). En este contexto, se publican en el año 2001 los dos primeros estándares de sistemas de gestión documentales, las normas ISO 15489, partes 1 y 2. Esta publicación coincide con un acontecimiento de repercusión internacional en el que la gestión de la información y documentación tiene un papel relevante, como son los escándalos de ENRON y Arthur Andersen²⁷ (Bustelo Ruesta 2011, p. 4).

Estas normas se conciben como una guía de buenas prácticas, por tanto, sin la posibilidad de certificarse. Años más tarde, ya en 2011, y como respuesta a la necesidad de certificación solicitada por los profesionales del sector, nace la serie de normas ISO 30300 con una vocación integradora con otros sistemas de gestión o MSS. En la implantación de cualquier MSS existe, de hecho, un fuerte componente de gestión de documentos. Los propios sistemas de gestión se basan en la existencia de una política y objetivos documentales y de unos procedimientos que describen los distintos procesos incluidos en el sistema. Al mismo tiempo, los procesos de trabajo deben generar evidencias que permitan comprobar que se han realizado según lo que se había definido. El sistema de gestión para los documentos propuesto en la norma ISO 30301 puede, por lo tanto, implementarse, auditarse y certificarse integrado con otros sistemas de gestión (por ejemplo, sistemas ISO 9001, ISO 27001, ISO 14001, ISO 18001, entre otros) permitiendo, con poco esfuerzo, ampliar la eficacia de los mismos (Bustelo Ruesta 2011, p. 4).

Con la publicación de la norma ISO 30301 se consigue, además, incluir el objetivo de la certificación para la gestión documental por entidades de acreditación reconocidas. Las auditorías de certificación deben llevarse a cabo por organismos de evaluación de la conformidad, que deben cumplir una serie de requisitos y seguir unos principios como son la imparcialidad, la competencia, la responsabilidad, la transparencia o la confidencialidad, entre otros. El valor de la certificación reside en el grado de confianza y fe pública que se establece con una evaluación imparcial y competente por una tercera parte (AENOR 2015, p. 14). En cualquier caso, lo más interesante de trabajar de acuerdo a este estándar internacional no es tanto la obtención de un certificado, sino el poder garantizar la conformidad con un modelo de gestión normalizado y de reconocimiento internacional (Moro Cabero 2011, p. 456) que permite mantener las características que las evidencias documentales deben cumplir y permite la trazabilidad de la información hasta la fuente original.

La norma ISO 30301 se compone de diez apartados y tres anexos. De estos, se deben tener en cuenta para la certificación los apartados del 4 al 10, más el Anexo A, que es normativo y, por tanto, de obligado cumplimiento. El resto de apartados y anexos no influyen en los procesos de auditoría y certificación. La norma sigue el modelo de estructura de alto nivel desarrollado por la organización ISO el año 2011 y que, a partir de 2012

²⁷ – El final de Arthur Andersen ocurrió cuando la empresa, auditora de Enron Corporation, fue sentenciada por los tribunales federales de Houston en 2002 por delitos de obstrucción a la justicia, y de destrucción y alteración de documentos relacionados con la quiebra de Enron y las irregularidades cometidas por dicha corporación. Ver noticias relacionadas: «Arthur Andersen Admits It Destroyed Documents Related to Enron Account» en <https://www.wsj.com/articles/SB1010695966620300040> (consultado el 18/02/2017) y «Enron's Collapse: The Auditor; Enron's Auditor Says It Destroyed Documents» en: <http://www.nytimes.com/2002/01/11/business/enron-s-collapse-the-auditor-enron-s-auditor-says-it-destroyed-documents.html> (consultado el 18/02/2017).

todas las normas de sistemas de gestión deben seguir. Tiene como objetivo la consistencia y el alineamiento de todos los MSS a través de la unificación y el consenso sobre su estructura, así como de un texto principal idéntico y de unos términos y definiciones comunes. A este esqueleto común pueden añadirse apartados concretos y propios en función de la especificidad de cada norma, siguiendo una serie de instrucciones.

En la estructura de la norma se encuentran los siguientes apartados: objeto y campo de aplicación, referencias normativas, términos y definiciones, contexto, liderazgo, planificación, soporte, operación, evaluación del desempeño del sistema y mejora, Anexo A, Anexo B y Anexo C. De estos, los tres primeros y los dos últimos no son normativos y, por tanto, no se auditan ni certifican.

La norma ISO 30301 dispone de un anexo normativo y de obligado cumplimiento en el que se especifican procesos y controles de gestión documental, el Anexo A. De hecho, se puede afirmar que la mayor concentración de requisitos se encuentra en dicho anexo. Mientras que, en el resto de la norma, los requisitos tienen un carácter más generalista y son fácilmente integrables con otras normas ISO. El anexo A es específico de esta norma y se divide en dos grandes bloques: creación y control. El primero, de creación, engloba todos aquellos procesos y controles que se relacionan con la generación y captura de evidencias documentales, como la definición de metadatos, la determinación de tipologías de documentos, formatos y soportes normalizados, entre otros. En el bloque de control se engloban todos aquellos procesos y controles en relación con la gestión de los documentos, una vez han sido capturados en el sistema de gestión documental. Se incluyen aspectos relacionados con el registro, la clasificación, el acceso, la transferencia, los traslados, la destrucción, entre otras cuestiones.

El anexo A, además de un listado de requisitos muy exhaustivo, resulta un instrumento tremendamente útil para el diseño e implantación de sistemas de gestión documental, puesto que cuenta con un listado de procesos, y controles para dichos procesos, que abarcan la gestión del ciclo de vida documental. Además, en el anexo se incluyen aspectos relacionados con la tecnología que se emplea para esta gestión, y dedica uno de los subapartados a las condiciones de administración y mantenimiento de las aplicaciones informáticas para la gestión de documentos.

Disponer de esta norma ISO, además de servir para la mejora de la gestión documental en las organizaciones, la posiciona a nivel estratégico, dotándola de mayor fuerza y protagonismo. Esto debe verse como una oportunidad para los profesionales de la archivística y la gestión de documentos, que no debe dejarse pasar. La gestión documental ayuda a las organizaciones a obtener mejores resultados, a ser más transparentes y facilita los procesos de rendición de cuentas, tal y como se explicará en próximos capítulos.

Capítulo 2.

Marco teórico y metodológico de la gestión de riesgos documentales

Según la Real Academia Española de la lengua el término “riesgo” se define como la contingencia o proximidad de un daño²⁸. Proviene del italiano *risico* o *rischio* y este del árabe clásico *rizq* (lo que depara la providencia). También puede definirse como la posibilidad de que algo desagradable ocurra.

Organizaciones de cualquier tipo y tamaño se enfrentan a factores e influencias internas y externas por las que resulta incierto saber si se conseguirán sus objetivos. La incidencia que esta incertidumbre tiene sobre la consecución de los objetivos de una organización constituye el riesgo (AENOR 2010, p. 8).

Se trata de un concepto que puede aplicarse a muchas disciplinas, como, por ejemplo: tecnologías de la información, gestión de negocios, ingeniería industrial, mercado financiero o seguridad laboral. En cada una de estas áreas, el riesgo puede definirse de maneras distintas y desde perspectivas epistemológicas diferentes, aunque una definición de aplicación general podría ser la probabilidad de frecuencia y la probabilidad de magnitud de una futura pérdida (Jones 2005, p. 5). En otras palabras, con qué frecuencia es probable que algo negativo suceda, y qué tipo de pérdidas podrían derivarse.

De esta definición se extraen tres premisas básicas para entender el riesgo. La primera es que se trata de una cuestión de probabilidades. La segunda es que los riesgos incluyen dos componentes: frecuencia y magnitud o severidad. La tercera es que el riesgo aplica a cualquier campo de acción. Por tanto, la naturaleza fundamental del riesgo es universal, independientemente del contexto (Jones 2005, p. 8) o del ámbito de trabajo.

La gestión de los riesgos es nuclear al gobierno de las organizaciones (Amutio Gómez, Candau, & Mañas 2012, p. 6) y, especialmente, los riesgos relacionados con las evidencias documentales que se generan, y con las que se trabaja, deben trasladarse a los órganos de gobierno y directivos para la toma de decisiones fundamentada. En el campo de la gestión documental, la gestión del riesgo es un proceso poco estudiado por el momento, pero va cogiendo fuerza y apareciendo cada vez más en la implantación de sistemas de gestión documental normalizados. Precisamente, es en los estándares internacionales donde encontramos mayor trabajo en esta dirección, partiendo de la norma *UNE-ISO 31000: 2010 – Gestión del riesgo. Principios y directrices*, que ha dado lugar al posterior desarrollo de un informe técnico²⁹ específico de riesgos de gestión documental, la norma *UNE-ISO/TR 18128: 2014 – Información y documentación. Apreciación del riesgo en procesos y sistemas de gestión documental*. En ambas normas se encuentra una definición del término riesgo prácticamente igual, que lo define como el efecto de la incertidumbre sobre la consecución de los objetivos y añade las siguientes aclaraciones al respecto (AENOR 2010, p. 8):

²⁸ – Definición de riesgo según el Diccionario de la Real Academia Española: <http://dle.rae.es/?id=WT8rAMI> (consultado el 04/03/2018).

²⁹ – Un informe técnico ISO contiene información distinta a un estándar internacional. Puede incluir, por ejemplo, datos obtenidos de una encuesta, de un informe o un “estado del arte” de alguna cuestión. No se trata de una norma de requisitos y se identifica porque aparecen las iniciales “TR” en el título del documento, que se corresponden con las siglas de Informe Técnico en inglés (*Technical Report*). Pese a no ser consideradas normas como tales, se suele hacer referencia a los informes técnicos como normas. Se puede consultar más información sobre los diferentes productos ISO en el siguiente enlace: <https://www.iso.org/deliverables-all.html> (consultado el 01/01/2018).

- Nota 1: Un efecto es una desviación, positiva y/o negativa, respecto a lo previsto.
- Nota 2: Los objetivos pueden tener diferentes aspectos (tales como financieros, de salud y seguridad, o ambientales) y se pueden aplicar a diferentes niveles (tales como nivel estratégico, nivel de un proyecto, de un producto, de un proceso o de una organización completa).
- Nota 3: Con frecuencia, el riesgo se caracteriza por referencia a sucesos potenciales y a sus consecuencias, o a una combinación de ambos.
- Nota 4: Con frecuencia, el riesgo se expresa en términos de combinación de las consecuencias de un suceso (incluyendo los cambios en las circunstancias) y de su probabilidad.
- Nota 5: La incertidumbre es el estado, incluso parcial, de deficiencia en la información relativa a la comprensión o al conocimiento de un suceso, de sus consecuencias o de su probabilidad.

En la conceptualización y la definición del riesgo se necesita, por tanto, añadir algunos factores o elementos que deben tenerse en cuenta a la hora de poder llevar a cabo con pertinencia el proceso de gestión del riesgo. Estos elementos son: amenazas, vulnerabilidad y activos (Jones 2005, p. 5). Según Jones, el riesgo es un valor derivado de la combinación de estos tres elementos:

- Amenaza: es todo aquello capaz de actuar contra un activo de modo que el resultado sea un daño. Algunos ejemplos pueden ser un tornado, una inundación o un *hacker*. El aspecto clave de la amenaza es la fuerza que se aplica (viento, agua, código) contra el activo y que puede causar una pérdida (Jones 2005, p. 13).
- Vulnerabilidad: comúnmente definida como una debilidad que puede ser explotada. Se puede definir como la condición en que la capacidad de la amenaza (fuerza) es mayor que la capacidad de resistencia a dicha amenaza. La vulnerabilidad siempre depende del tipo y nivel de fuerza que se aplique sobre el activo (Jones 2005, p. 5). Para cada vulnerabilidad identificada pueden asociarse varios riesgos.
- Activo: en el contexto de la gestión del riesgo de la información y los documentos, un activo puede definirse como cualquier dato, aplicación, dispositivo u otro componente, dentro de dicho contexto, que dé soporte a actividades que necesiten de información o documentos para llevarse a cabo y puedan ser ilícitamente usados, desclasificados, publicados, destruidos, accedidos, robados, etc., dando como resultado una pérdida (Jones 2005, p. 15).

A partir de estos tres elementos puede definirse el riesgo como la frecuencia con la que algo negativo ocurre y la magnitud o resultado que se deriva de ello. Estas probabilidades resultan, como se ha descrito, de una combinación entre la amenaza, la vulnerabilidad y las características del activo. Aplicando estos conceptos a la gestión de documentos y archivos, el riesgo puede definirse a partir de aquellas amenazas que afectan a la integridad, disponibilidad y confidencialidad de la información y los documentos de una organización (Pullen & Maguire 2007, p. 5).

Lemieux fue una de las primeras en relacionar los riesgos y su gestión con el ámbito de la gestión documental, la información y los documentos. Según Lemieux, los riesgos de la información y los documentos (en adelante riesgos documentales³⁰) abarcan cualquier amenaza que provenga de alguna insuficiencia de la información y los documentos (Lemieux 2004a, p. 2) y que puede suponer el incumplimiento de los objetivos de la organización.

³⁰ – Se realizan diferentes traducciones del inglés *records risks* al castellano, según la publicación. Por un lado se traduce como riesgos de la información y de los documentos, por otro, se traduce como riesgos de gestión documental y, por otro, como riesgos documentales. En esta investigación se emplea la última de las opciones como traducción amplia y de consenso.

Los documentos y la información contenida en ellos afectan a las entradas, procesos, salidas y resultados de cualquier organización. Por ello, necesitan ser gestionados de manera adecuada dentro de cualquier estrategia de gestión del riesgo (Pullen & Maguire 2007, p. 4). Una política de gestión documental definida y controlada asegura que una organización esté más protegida frente a este tipo de riesgos, y que las prácticas de gestión documental cumplen con los requisitos legales y normativos aplicables. Cuanto mejor sea la gestión de documentos en una organización, menor riesgo existirá.

El objetivo de la gestión de riesgos documentales es proteger la misión de la organización, asegurando la creación y el mantenimiento de los documentos y sus características de fiabilidad, autenticidad, integridad y usabilidad durante el tiempo que sea necesario.

Estas características, y su mantenimiento a lo largo del tiempo, se logran con la implantación de aplicaciones de gestión documental o de sistemas de captura y control de documentos que sean fiables, seguros, conformes, exhaustivos y sistemáticos. La norma ISO 30300 define estas características de la siguiente manera (AENOR 2011b, p. 9):

- Fiables: permiten la continuidad del negocio y apoyan la gestión de riesgos. Estas deben:
 - Capturar de forma rutinaria todos los documentos dentro del alcance de las actividades de la organización que cubren.
 - Organizar los documentos de forma que reflejen los procesos de negocio.
 - Proteger los documentos de alteraciones o disposiciones no autorizadas.
 - Funcionar de forma habitual como la fuente primaria de información de las acciones documentadas en los documentos.
 - Proporcionar acceso rápido a todos los documentos cuando se necesitan.
 - Capturar información acerca de la recuperación, uso y disposición de los documentos que gestionan.
 - Ser capaces de un funcionamiento continuo y regular.
- Seguras: emplean un control adecuado de las medidas para prevenir las acciones no autorizadas (acceso, destrucción, alteración o eliminación). Los sistemas seguros facilitan la rendición de cuentas y la gestión de riesgos.
- Conformes: cumplen con los requisitos derivados de las actividades habituales, las expectativas de las partes interesadas y el entorno reglamentario en los que opera la organización. Las aplicaciones pueden evaluarse con estos requisitos, como parte de sus procesos de mantenimiento y mejora del sistema de gestión documental (SGD). Los sistemas conformes aseguran la rendición de cuentas, el buen gobierno y la gestión de riesgos.
- Exhaustivas: gestionan documentos derivados de un rango completo de actividades de la organización, grupo de organizaciones o secciones de la organización que los usan. Los sistemas exhaustivos facilitan la eficiencia y la eficacia organizativas.
- Sistemáticas: los procesos de creación y gestión de documentos se sistematizan a través del diseño y funcionamiento de las aplicaciones de gestión según las políticas documentadas, la asignación de responsabilidades y las metodologías formales. Esto ayuda a dirigir eficientemente la organización y a gestionar los riesgos.

Las organizaciones que trabajan con aplicaciones informáticas que mantienen estas características, están expuestas a una menor probabilidad de que ocurran los riesgos.

Dentro de la conceptualización del riesgo, también hay que tener en cuenta que la mayoría de las actividades, procesos o proyectos tiene un ciclo de vida, como, por ejemplo, el ciclo de vida documental explicado en el capítulo anterior. En la mayoría de casos, también, los riesgos pasan por distintas fases y su nivel o clasificación varían en función de la etapa en la que se encuentre dentro del proceso de apreciación o en función de la evolución de la actividad o proyecto con el que se relacionen. En cualquiera de los casos, el riesgo cambia y evoluciona a lo largo del tiempo. Es probable percibir cambios en las amenazas y prioridades de la organización a lo largo del tiempo que pueden afectar en gran medida un nivel de riesgo previamente evaluado (Wheeler 2011b, p. 43). Puede realizarse la evaluación, dando como resultado un nivel de riesgo alto en el día de hoy, pero reduciéndose en seis meses, como resultado de los esfuerzos y estrategias para mitigarlo (Wheeler 2011b, p. 43). El riesgo es, por tanto, un elemento en “evolución” o en cambio constante.

En línea con la idea del ciclo de vida documental, Bearman hace una reflexión sobre los puntos críticos en que se acentúan los riesgos sobre los procesos de gestión documental, identificando seis “momentos” de riesgo que se dan en situaciones de transición a lo largo de la vida de los documentos: captura, mantenimiento, ingreso, acceso, disposición y preservación. Bearman aplica esta teoría a los documentos electrónicos ya que, según este autor, es ampliamente reconocido que los documentos electrónicos se someten a un riesgo máximo de perder sus características como documentos de archivo en los momentos en que pasan de un estado a otro, por ejemplo, cuando se pasa el control sobre los mismos de una aplicación informática a otra (Bearman 2006, p. 24). Se considera necesario añadir a estos seis momentos definidos por Bearman, el riesgo que supone la no creación de un documento como evidencia de aquello que se ha decidido y se ha llevado a cabo.

Pese a que el autor no lo incluye de manera explícita, sí hace referencia a que la literatura está de acuerdo en que existe un mayor riesgo en los momentos previos a la captura de un documento en un SGD, o a la transferencia hacia un entorno archivístico controlado, puesto que podría alterarse, perder su identidad original, o separarse de los metadatos requeridos para establecer su autenticidad (Bearman 2006, p. 31).

Siguiendo esta idea, Bearman afirma que el consenso en la naturaleza del riesgo documental significa que estados y tipos específicos de riesgos, así como los criterios para evaluar si la transición ha ocurrido con éxito, podrían ser acordados de manera general. Un modelo adecuado expondría los momentos del riesgo, independientemente de las soluciones que se ofreciesen para gestionarlos (Bearman 2006, p. 25). Esta teoría se construye sobre el modelo del ciclo de vida de los documentos, sin el cual dejaría de tener sentido. Se propone un modelo normalizado de gestión del riesgo documental, adaptable a cualquier tipo de organización con tan solo unos pequeños ajustes.

2.1 Estándares de gestión del riesgo

Existen diferentes estándares y normas internacionales que tratan del proceso de gestión del riesgo de manera genérica, así como también con relación a la información y los documentos. Las organizaciones que han trabajado en esta normalización son, principalmente, el *UK Institute of Risk Management (IRM)*, la *International Standardization Organization (ISO)*, *Standards Australia (SA)* y *Association of Records Managers and Administrators (ARMA International)*. Se

aprecia una preponderancia de países anglosajones en el desarrollo de esta metodología, si bien el objetivo principal es la normalización, lo que implica que su aplicación puede extrapolarse a cualquier contexto.

Se introducen a continuación aquellos que se han tenido en cuenta a la hora de desarrollar este capítulo.

Norma **UNE-ISO 31000: 2010 – Gestión del riesgo. Principios y directrices** (en adelante ISO 31000). Esta norma establece una serie de principios que se deben satisfacer para que la gestión del riesgo sea eficaz. Recomienda que las organizaciones desarrollen, implementen y mejoren de manera continuada un marco de trabajo, cuyo objetivo sea integrar el proceso de gestión del riesgo en los procesos de gobierno, de estrategia y de planificación, de gestión, y de elaboración de informes, así como en las políticas, los valores y en la cultura de toda la organización (AENOR 2010, p. 5).

La adopción de procesos coherentes dentro de un marco de trabajo exhaustivo puede contribuir a asegurar que el riesgo se gestiona de manera eficaz, eficiente y pertinente dentro de la organización. El enfoque genérico que se describe en este estándar internacional proporciona los principios y las directrices para gestionar cualquier forma de riesgo de una manera sistemática, transparente y fiable, dentro de cualquier alcance y de cualquier contexto (AENOR 2010, p. 5).

Durante la realización de esta investigación, la norma ISO 31000 sufrió un proceso de revisión, siendo publicada una nueva versión en el mes de febrero de 2018. No han podido incluirse los cambios realizados en la investigación, pero será necesario tenerlos en cuenta para posteriores estudios.

ISO/IEC³¹ Guía 73: 2009 – Gestión del riesgo. Vocabulario. Se trata de una guía que proporciona definiciones estándar de la terminología genérica en relación con la gestión del riesgo. Pretende alcanzar una aproximación coherente a la descripción de las actividades relacionadas con dicha gestión, así como el uso de una terminología uniforme para la gestión del riesgo en procesos y ámbitos muy distintos entre sí, pero que deben enfrentarse al mismo proceso.

La norma **ISO/IEC 31010: 2011 – Gestión del riesgo. Técnicas para la apreciación del riesgo** (en adelante, ISO/IEC 31010). Este estándar sirve de apoyo a la norma ISO 31000, proporcionando directrices sobre la selección y aplicación de técnicas sistemáticas para la apreciación del riesgo, aunque sin referir la totalidad de técnicas existentes. Se introduce un abanico de técnicas, incluyendo referencias específicas a otros estándares internacionales donde los conceptos y aplicación de las mismas se describen con mayor detalle.

El propósito de la apreciación del riesgo es el de proporcionar información basada en evidencias para tomar decisiones informadas sobre cómo tratar los riesgos y cómo elegir entre diferentes opciones de tratamiento. Este estándar parte de la base de que la apreciación del riesgo se realiza siempre dentro del marco y el proceso de gestión del riesgo descrito en la norma ISO 31000.

El informe técnico **UNE-ISO/TR 18128: 2014 IN – Información y documentación – Apreciación del riesgo en procesos y sistemas de gestión documental** (en adelante, ISO/TR 18128). Está dirigido a ayudar a los profesionales de la gestión de documentos y a las personas que tienen responsabilidad sobre los documentos en sus organizaciones a apreciar (identificar, analizar y evaluar) los riesgos relacionados con los procesos y sistemas de gestión documental. Parte de la premisa de que la organización ha creado documentos de sus actividades para cumplir con los requisitos

³¹ – IEC (Comisión Electrotécnica Internacional) es una organización mundial para la normalización, que comprende todos los comités electrotécnicos nacionales (Comités Nacionales de IEC). El objetivo de IEC es promover la cooperación internacional, sobre todas aquellas cuestiones relativas a la normalización en los campos eléctrico y electrónico. Para este fin y también para otras actividades, IEC publica Normas Internacionales, Especificaciones Técnicas, Informes Técnicos, Especificaciones Disponibles al Público (PAS) y Guías. Los documentos producidos tienen la forma de recomendaciones para uso internacional.

operacionales u otros propósitos, y que ha establecido un mecanismo mínimo para la gestión y control sistemáticos de los mismos. Este punto de partida implica que la gestión de riesgos documentales, tal y como la entiende ISO, no es posible sin la existencia de un SGD que ya esté funcionando de manera adecuada. Esta idea refuerza la necesidad de disponer de sistemas que permitan a las organizaciones la gestión y el control de la información que generan a lo largo del tiempo.

El informe técnico ISO/TR 18128 proporciona, además, directrices y ejemplos basados en el proceso general de gestión del riesgo establecido en la norma ISO 31000, aplicados a los riesgos relacionados con los procesos y sistemas de gestión documental.

Por último, se incluye como estándar, aunque no publicado por la organización ISO, el modelo de evaluación de riesgos de la información y los documentos desarrollado y publicado por la organización ARMA en 2009: *“Evaluating and Mitigating Records and Information Risks. An ARMA International Guideline”*. Se considera necesario incluir esta publicación, ya que ha sido desarrollada desde el punto de vista de la profesión archivística en el seno de una asociación de archiveros y gestores de documentos, con el objetivo de fijar unas directrices básicas para la realización de la identificación, análisis y evaluación de riesgos propiamente de la información y los documentos. En el momento de realizar la búsqueda de metodologías específicas no se encontró ningún referente a nivel europeo o español y es por este motivo que se seleccionó esta metodología.

Este modelo proporciona un marco de trabajo con cuatro áreas (Administrativa, Control de documentos, Legal y normativa, Tecnológica) para entender y evaluar los riesgos de una organización con relación a la gestión de documentos y de la información. Cualquier organización puede usar estas directrices y herramientas de evaluación para identificar las áreas más críticas, así como las estrategias de mitigación de riesgos que mayor garantía le aportan. Sirve, por tanto, como un estándar en la materia.

2.2 El proceso de gestión del riesgo

Según la norma ISO/IEC 31010, la gestión del riesgo incluye la aplicación de métodos lógicos y sistemáticos para (AENOR 2011 a, p. 9):

- La comunicación y consulta a lo largo del proceso de gestión del riesgo.
- El establecimiento del contexto para identificar, analizar, evaluar y tratar los riesgos asociados a una actividad, proceso, función o producto.
- La monitorización y revisión de los riesgos.
- La realización de informes y la documentación de los resultados de manera apropiada.

La gestión del riesgo no es una política más que debe crearse, sino que es la política sobre la cual construir todos

³² – IEC (Comisión Electrotécnica Internacional) es una organización mundial para la normalización, que comprende todos los comités electrotécnicos nacionales (Comités Nacionales de IEC). El objetivo de IEC es promover la cooperación internacional, sobre todas aquellas cuestiones relativas a la normalización en los campos eléctrico y electrónico. Para este fin y también para otras actividades, IEC publica Normas Internacionales, Especificaciones Técnicas, Informes Técnicos, Especificaciones Disponibles al Público (PAS) y Guías (de aquí en adelante “Publicaciones IEC”). Los documentos producidos tienen la forma de recomendaciones para uso internacional.

los demás procesos de negocio y políticas de la organización (ARMA International 2009, p. 21). La gestión del riesgo debe estar integrada en las prácticas y procesos de la organización, de manera que sea relevante, eficaz y eficiente (AENOR 2010, p. 17). Por tanto, no es solo control de calidad, sino que también implica la mejora del proceso (Shimell 2002, p. 188).

Actualmente, las organizaciones admiten la necesidad de reconocer, en su modelo interno de gestión del riesgo, las interrelaciones existentes entre los diferentes riesgos inherentes a las actividades del negocio, lo que genera un alejamiento del tradicional modelo de gestión del riesgo “por silos” y contribuye a configurar un Sistema de Gestión Integral del Riesgo (SGIR) como “una buena práctica” a nivel internacional (Martínez García 2009, p. 1). Este modelo de gestión integral, por un parte, reconoce las interrelaciones existentes entre todos los riesgos inherentes a las actividades del negocio y, por otra, configura una filosofía de gestión que permite trasladar la estrategia y los objetivos definidos en la gestión del riesgo a todos los niveles de la estructura, a través de los valores implícitos en la cultura corporativa (Martínez García 2009, p. 5).

Dentro de este proceso de gestión integral del riesgo existen diferentes etapas que analizan, evalúan, tratan los riesgos. Estas deben llevarse a cabo de manera periódica a medida que el riesgo evoluciona (Wheeler 2011b, p. 43).

Según la norma ISO 31000, el proceso de gestión del riesgo comprende las siguientes actividades o etapas (AENOR 2010, p. 20) (ver Figura 4):

- Comunicación y consulta
- Establecimiento del contexto
 - Externo
 - Interno
 - Del proceso de gestión del riesgo
 - Definición de los criterios del riesgo
- Apreciación del riesgo o Identificación
 - Análisis
 - Evaluación
- Tratamiento del riesgo
- Seguimiento y revisión
- Registro o documentación del proceso de gestión del riesgo

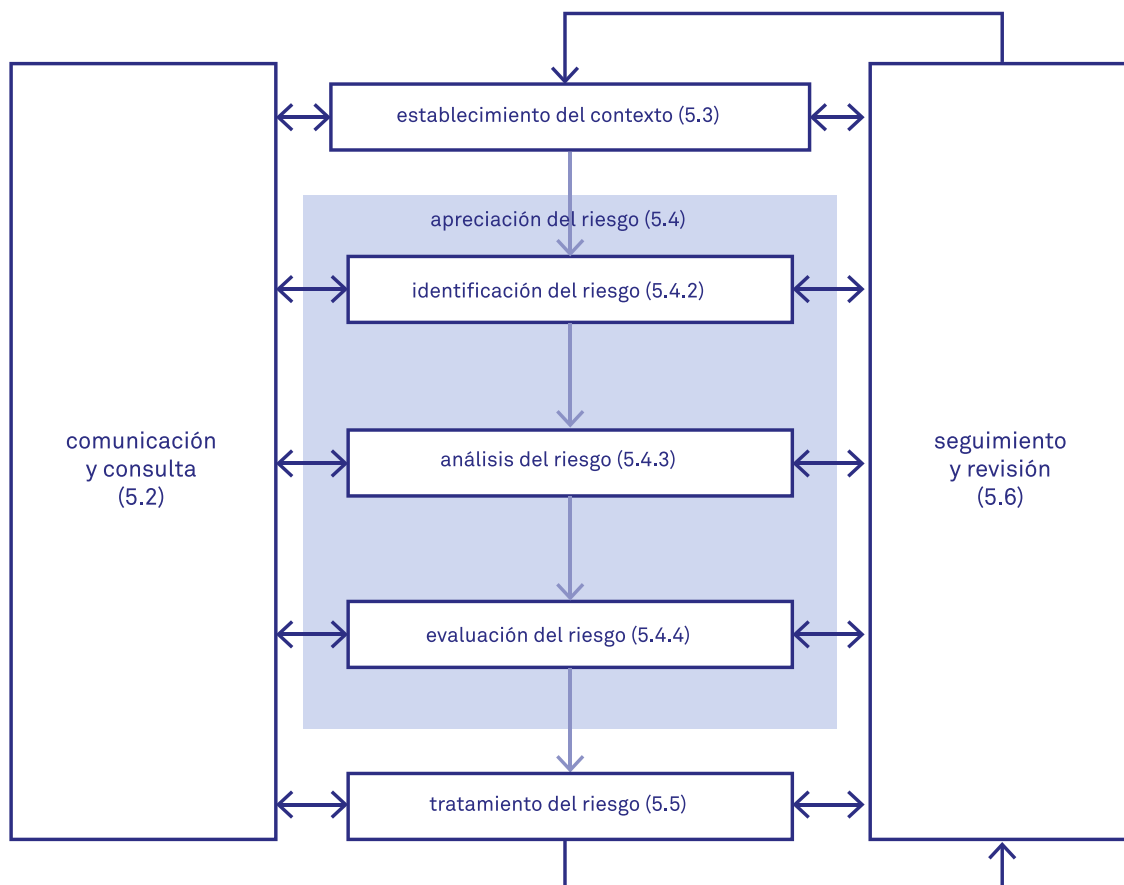


Figura 4 - Proceso de gestión del riesgo (ISO 31000).

Dentro de este proceso hay apartados generales, como el establecimiento del contexto, la comunicación y consulta, y el seguimiento y revisión, de los cuales se establece un procedimiento o metodología que puede compartirse con cualquier campo de trabajo. También aparecen otros apartados, que son específicos y se relacionan con la actividad de la cual se realiza la gestión del riesgo, en este caso, la gestión de documentos. Estos son fundamentalmente los procesos de apreciación y tratamiento que están directamente relacionados con la parte operacional de la gestión de los documentos y de la información.

Cada uno de estos pasos puede ser más o menos complejo en función del contexto y la realidad de la organización, el alcance y cómo de detallado se quiera desarrollar el proceso general (Wheeler 2011b, p. 44). Disponer de un alcance para la apreciación claramente definido es crucial para el buen desarrollo del proceso de gestión del riesgo.

Dentro de este esquema, faltar añadir la definición de roles y responsabilidades para llevar a cabo el proceso. Lemieux afirma que los roles y responsabilidades para la gestión de los riesgos documentales deben ser claramente identificados y deben extenderse a todos los niveles y ubicaciones de la organización (Lemieux 2004a, p. 41). Cabe mencionar que las normas ISO normalmente incluyen este aspecto como un apartado más en su estructura. En el caso de la norma ISO 31000, si bien no se ha desarrollado de esta manera, sí se incluye el mandato de asignar la obligación de rendir cuentas y las responsabilidades que corresponden a los diferentes niveles de la organización (AENOR 2010, p. 16) en varios de sus apartados. Se considera insuficiente la dispersión de un aspecto tan importante por distintas secciones de la norma, lo que podría conllevar a una definición de responsabilidades difusa y secundaria.

La distribución de responsabilidades refleja la concienciación y la gestión de riesgos documentales en las estructuras corporativas, los procesos y la tecnología existentes. Además, los roles y responsabilidades para las áreas funcionales que tradicionalmente se han centrado en la gestión de documentos e información o que se han enfrentado anteriormente a riesgos documentales (como pueden ser el departamento de gestión documental o el de sistemas de información) necesitan redefinirse en cuanto a la manera de encajar la gestión de este tipo de riesgos en el programa de gestión del riesgo general de la organización (Lemieux 2004a, p. 44).

2.2.1 Comunicación y consulta

Las comunicaciones y las consultas con las partes interesadas externas e internas se deberían realizar en todas las etapas del proceso de gestión del riesgo (AENOR 2010, p. 20). El objetivo principal en esta fase es identificar e imponer prioridades, y tomar las decisiones adecuadas (AENOR 2014, p. 25).

La comunicación es parte de una gestión eficaz del riesgo para garantizar a toda la organización el reconocimiento de los mismos (AENOR 2014, p. 25). Por este motivo es fundamental, desde el inicio, desarrollar planes de comunicación y consulta en la organización, con el fin de asegurar que las personas responsables de la implementación del proceso de gestión del riesgo, y las partes interesadas, son informadas y comprenden la información para la toma de decisiones y las razones por las que son necesarias determinadas acciones. Según la norma ISO 31000, un enfoque consultivo en equipo puede (AENOR 2010, p. 21):

- Ayudar a establecer adecuadamente el contexto.
- Asegurar que los intereses de las partes interesadas se comprenden y se tienen en consideración.
- Ayudar a asegurar que los riesgos se identifican adecuadamente.
- Reunir diferentes áreas de experiencia para analizar los riesgos (equipos multidisciplinares).
- Asegurar que las diferentes opiniones se tienen en cuenta de forma adecuada, al definir los criterios de riesgo y en la evaluación de ellos.
- Conseguir la aprobación y el apoyo para un plan de tratamiento.
- Favorecer una gestión del cambio adecuada durante el proceso de gestión del riesgo.
- Desarrollar un plan adecuado de comunicación y consultas externas e internas. Estos planes deben tratar temas relativos al riesgo en sí mismo, a sus causas, a sus consecuencias, y a las medidas a tomar para tratarlo.

Las comunicaciones y las consultas deben facilitar el intercambio de información veraz, pertinente, exacta y entendible, así como tener en cuenta los aspectos de confidencialidad y de integridad personal (AENOR 2010, p. 21) del marco legal aplicable. También es fundamental plantear el cambio hacia la gestión de riesgos con un enfoque positivo, enfatizando la percepción del riesgo como una oportunidad cuando está bien gestionado y no como una amenaza, es decir, como una fuente de desventaja competitiva (Martínez García 2009, p. 78).

2.2.2 Establecimiento del contexto

Establecer el contexto de la organización permite definir los objetivos, así como los parámetros a tener en cuenta para la gestión del riesgo, establecer el alcance y los criterios de riesgo (AENOR 2010, p. 21) para llevar a cabo el resto del proceso. Dentro de este apartado se deben analizar el contexto externo, interno y del proceso de gestión del riesgo, así como identificar los criterios de riesgo.

Además de recopilar información sobre el contexto social, político, medioambiental, financiero o ético, debe incluirse también la información sobre la infraestructura tecnológica, los sistemas de información, los aspectos legales que afectan al desempeño de la organización, entre otras cuestiones. Algunas de las razones para recopilar este tipo de información contextual son (Lemieux 2004a, p. 25):

- Para dar apoyo al proceso de identificación de riesgos y sus fuentes, puesto que sin una buena comprensión del entorno en el que opera la organización, los gestores del riesgo tendrán dificultades para conocer los tipos de riesgo a los que puede exponerse dicha organización, así como sus causas potenciales.
- Para ayudar a determinar la probabilidad y el impacto de los riesgos identificados, cosa que resultará imposible sin un conocimiento en profundidad del contexto.
- Para dar apoyo al proceso de definición de la “pérdida aceptable”, o lo que se conoce como el nivel de tolerancia al riesgo³² que está dispuesto a aceptar una organización.
- Para identificar qué estrategias de tratamiento del riesgo funcionarán, puesto que sin la comprensión del contexto resultará tremendamente difícil diferenciar entre los riesgos que pueden controlarse y los que no.
- Para ayudar a establecer prioridades para el tratamiento de los riesgos, dando preferencia a la actuación sobre aquellos que pueden derivar en un incumplimiento de los objetivos estratégicos o aquellos que pueden tener un impacto mayor en la organización.

Puede parecer que estas actuaciones son muy lejanas al estudio del contexto, pero resulta fundamental incluirlas para, llegado el momento, hacer una toma de decisiones informada.

El contexto externo

Se refiere al entorno externo en el que la organización lleva a cabo sus actividades y dentro del cual busca conseguir sus objetivos. Incluye aspectos como la comprensión de los requisitos legales y normativos aplicables, el entorno social y cultural, político, tecnológico, económico, así como las relaciones con las partes externas interesadas, sus percepciones y valores, entre otros.

³² – Algunos casos concretos son los casos de: Arthur Andersen, Enron Account, en relación con fraude y corrupción; la Comisión del 11 de septiembre, en relación al terrorismo; el caso Bichard, en relación a abusos sexuales y asesinato de menores; entre otros. En todos ellos se aludió a una mala praxis en la gestión de los documentos, ya fuese por ocultación, eliminación, manipulación, entre otras. Con una buena gestión de la información y los documentos se podría haber contribuido a la prevención de estos hechos.

El contexto interno

Está formado por todo aquello que, dentro de la organización, puede influir en el modo en que se gestiona el riesgo. Incluye aspectos como, por ejemplo, la estructura de la organización, las funciones y responsabilidades, las políticas, objetivos y estrategias que se establecen, la cultura de la organización o las normas, directrices y modelos que sigue la organización en su día a día.

El contexto del proceso de gestión del riesgo

Este varía de acuerdo con las necesidades de la organización, aunque deben establecerse, como mínimo, los objetivos, las estrategias, el alcance del proceso y los parámetros de las actividades de la organización, o partes de la organización, donde se aplica dicho proceso. Incluye, entre otros, aspectos como la definición de responsabilidades relativas al proceso de gestión del riesgo, la definición de las metodologías de apreciación del riesgo o la definición de la metodología para la evaluación del desempeño y eficacia en la gestión del riesgo. Sin la comprensión del contexto resulta imposible clasificar el impacto de los riesgos sobre la organización en términos de pérdida de productividad, pérdida de ingresos, sanciones normativas u otros (Wheeler 2011a, p. 91).

Es importante destacar la definición del alcance, puesto que se puede aplicar tanto a una organización como a una función concreta, un área o incluso varias organizaciones. Es necesaria una determinación muy clara para la aplicación del proceso, para evitar incidencias en la identificación de riesgos.

La definición de los criterios de riesgo

Los criterios de riesgo son aquellos que se aplican para evaluar la importancia del riesgo. Los criterios deben reflejar los valores, objetivos y recursos de la organización y pueden derivarse de los requisitos legales o normativos aplicables. Deben incluir (AENOR 2010, p. 23):

- La naturaleza y los tipos de consecuencias que se pueden producir, y cómo se medirán.
- La forma en que se expresa la probabilidad.
- Cómo se determinará el nivel de riesgo.
- El criterio por el cual se decide cuándo un riesgo necesita tratamiento.
- El criterio por el que se decide cuándo un riesgo es aceptable o tolerable.
- Cuándo y cómo se tendrán en cuenta combinaciones de riesgos.

Los criterios para evaluar los riesgos documentales deben incluir, además, el tamaño y alcance de los sistemas de gestión documental de la organización, el número de usuarios y el uso que se hace del sistema en las operaciones de la organización.

Los criterios para evaluar los riesgos que afectan a los procesos de gestión documental deben incluir la frecuencia del proceso, cuántos sistemas se usan en el mismo, y su importancia relativa en la creación o gestión de los documentos, el seguimiento de los procesos y el potencial para revertir o remediar los posibles efectos adversos (AENOR 2014, p. 9).

2.2.3 Apreciación del riesgo (*Risk assessment*)

La apreciación del riesgo es el subproceso que comprende la identificación, el análisis y la evaluación del riesgo. Se incluye dentro del proceso global de gestión del riesgo y debe proporcionar una mejora en la comprensión de los riesgos que pueden afectar a la consecución de los objetivos, y la adecuación y efectividad necesaria de los controles ya existentes. Las salidas (*outputs*) de la apreciación del riesgo son entradas (*inputs*) para el proceso de toma de decisiones de la organización.

La apreciación de riesgos documentales se debe incluir, cuando exista, en el proceso general de gestión del riesgo de la organización. Los profesionales de la gestión de documentos deben tener en cuenta, según el informe técnico ISO/TR 18128, el contexto interno y externo de la organización, así como el contexto propio de gestión del riesgo, incluyendo (AENOR 2014, p. 8):

- Roles y responsabilidades: se debe especificar el rol de los profesionales de la gestión de documentos en la apreciación de los riesgos relacionados con los procesos y sistemas de gestión documental.
- Alcance y amplitud de las actividades de apreciación del riesgo: para evitar redundancia y conflictos, así como para facilitar un enfoque integral de la gestión del riesgo que incluya la gestión de documentos, se deben hacer explícitas las relaciones con otras áreas de apreciación del riesgo, como la seguridad de la información.
- Metodología: se debe aplicar la metodología normalizada de apreciación del riesgo utilizando las herramientas de apreciación del riesgo y reportando a la persona o área designada.
- Criterios de riesgo: cuando se han establecido criterios de riesgo generales para la organización, se deben usar para el proceso de apreciación de los riesgos relacionados con los procesos y sistemas de gestión documental.

Cuando la organización no ha establecido un proceso general de gestión del riesgo, los profesionales de gestión de documentos necesitan establecer, al iniciar el proceso, los criterios de riesgo que se aplicarán para los procesos y sistemas de gestión documental (AENOR 2014, p. 8). Los responsables de la gestión de documentos necesitan convertirse en activos clave de la gestión de riesgos documentales y de riesgos de la información, junto a otros responsables de otras áreas funcionales. Los gestores de documentos están capacitados de manera única para este tipo de gestión, puesto que poseen el conocimiento sobre los documentos y la información de la organización, así como la comprensión de las herramientas y las técnicas de gestión documental que pueden ayudar a mitigar los riesgos documentales en ella (Lemieux 2004a, p. 3).

La apreciación del riesgo debe supervisarse y revisarse a intervalos regulares con el fin de asegurar que los controles seleccionados para el tratamiento de los riesgos permanecen efectivos (AENOR 2014, p. 25), así como asegurar que el contexto no ha experimentado cambios significativos. Existen diferentes momentos en los que es necesario llevar a cabo una nueva apreciación del riesgo, como, por ejemplo:

- Un cambio en el contexto de la organización (sea interno o externo).
- Un cambio significativo en las amenazas identificadas.
- Un cambio en los requisitos legales o normativos.

- Un cambio en las políticas de gestión de documentos.

A continuación, se explican las tres fases que se enmarcan en la apreciación del riesgo: identificación, análisis y evaluación.

Identificación de riesgos documentales

Todas las organizaciones identifican, analizan y controlan los riesgos relacionados con el éxito de su funcionamiento, pero en la mayoría no se tienen en cuenta los riesgos documentales. Sin embargo, cualquier organización crea, recibe, gestiona y conserva documentos e información dentro del desarrollo de sus actividades de negocio. Dicha información debe ser, y debe poder demostrarse que es auténtica, fiable, íntegra y usable.

La identificación de riesgos en cualquier organización debe, por tanto, incluir aquellos relacionados con la información y los documentos, así como con los procesos y las aplicaciones de gestión documental, con el objetivo de detectar qué situaciones pueden darse que puedan afectar a la capacidad de los documentos para satisfacer las necesidades y los objetivos de la organización. El conocimiento de los riesgos permite aumentar la confianza en los sistemas que desempeñan su función.

Dentro del contexto de la gestión de documentos, el riesgo es impulsado o generado por hechos que impactan en la usabilidad, la integridad, la confianza y la fiabilidad de la información y los documentos (ARMA International 2009, p. 2). El proceso de identificación del riesgo incluye la detección de las causas y el origen del riesgo, las acciones, situaciones o circunstancias que pueden tener un impacto material sobre los objetivos de la organización, así como la naturaleza de ese impacto (AENOR 2014, p. 10). Para llevar a cabo la identificación de riesgos con éxito, Lemieux (Lemieux 2004b) propone dos enfoques distintos, que además pueden ser complementarios: el enfoque basado en hechos y el enfoque basado en requisitos, que se explicarán con detalle más adelante. Ambas técnicas son válidas y tienen sus ventajas e inconvenientes.

Enfoques y técnicas para la identificación de riesgos documentales

Para la identificación de riesgos, cualquier organización debe aplicar los instrumentos y las técnicas que mejor se adapten a sus objetivos y aptitudes, así como a los riesgos a los que está expuesta (AENOR 2010, p. 24). Para ello, es esencial disponer de información pertinente y actualizada sobre el desempeño de los procesos. La identificación global de riesgos es un componente crítico incuestionable de cualquier ejercicio de gestión del riesgo, puesto que los riesgos pueden darse en muchos niveles dentro de una organización, como por ejemplo (Lemieux 2004a, p. 25):

- Nivel estratégico
- Nivel organizacional
- Nivel de proyecto
- Nivel operativo

A nivel estratégico, los gestores de riesgos necesitan centrarse en la identificación de los riesgos clave para alcanzar con éxito los objetivos de la organización. En los niveles inferiores, el foco está en los riesgos que afecten a programas, proyectos y en los niveles de servicio operacional (Lemieux 2004a, p. 26).

Además, hay que tener en cuenta la existencia de dos visiones a la hora de identificar riesgos. La primera enfatiza la identificación en los riesgos de la organización, en cuanto a que no estén disponibles, o lo estén, pero no con las características adecuadas, los documentos y la información que se requieren para las transacciones y el control de las operaciones y los procesos. La segunda se centra en la identificación y gestión de los riesgos documentales y de la información a partir de las amenazas que les afectan directamente. En el primer caso, el foco está en las debilidades de los documentos respecto a los objetivos estratégicos de la organización. Las causas pueden derivar de múltiples fuentes, incluyendo desastres, fallos en los ordenadores o brechas de seguridad. La ventaja de este enfoque es que no se pierde la visión estratégica. Se hace explícita la relación entre los documentos y el logro de los objetivos estratégicos de la organización (Lemieux 2004a, p. 5). Por su parte, la segunda visión se centra de manera explícita en las amenazas operacionales que pueden afectar a los documentos de manera directa. La ventaja de este enfoque es el análisis de las fuentes de información que proporcionan evidencias en las organizaciones, sin las cuales no podrían desarrollarse los procesos de trabajo.

Para poder llevar a cabo la identificación de riesgos existen, por tanto, diferentes enfoques y perspectivas. En esta investigación se incluyen dos enfoques presentados por Victoria Lemieux, que resultan útiles para las dos visiones explicadas. El primero de ellos parte de los hechos desencadenantes de un riesgo y el segundo, del análisis de los requisitos de gestión documental. Se explican a continuación.

El primer enfoque se basa en hechos o amenazas. Tradicionalmente, las organizaciones han identificado y gestionado los riesgos asociados a la información y los documentos que les afectan a partir de un hecho, acontecimiento, o amenaza desencadenante. Las amenazas son “cosas que ocurren” (Amutio Gómez *et al.* 2012, p. 27) o más en detalle, situaciones que pueden provocar un suceso o un hecho, que pueden afectar de manera negativa a una organización.

Según el modelo MAGERIT 3.0, las amenazas típicas pueden ser de origen natural, del entorno, defectos de las aplicaciones, causadas por las personas de forma accidental o causadas por las personas de forma deliberada. No todos los tipos de amenaza afectan por igual a las características de los documentos. Las amenazas necesitan ser más que solamente posibles, necesitan ser probables para que valga la pena continuar con la fase de análisis (Wheeler 2011a, p. 96). En cualquier caso, es importante entender que las amenazas no son riesgos *per se*. Este enfoque contiene las siguientes etapas:

1. Identificación de amenazas.
2. Identificación de los riesgos a partir de estas amenazas.
3. Relación de los riesgos con el cumplimiento o no de los requisitos aplicables.

El segundo enfoque se basa en requisitos. Consiste en la identificación de los riesgos asociados a la información y los documentos, a partir del análisis de los requisitos que la organización aplica a la documentación y la información con la que trabaja. Estos pueden derivar de la legislación y de normativas. El riesgo, a través de este enfoque, aparece en el momento en que la organización se desvía del cumplimiento de dichos requisitos. Para poder trabajar de acuerdo a este enfoque, Lemieux identifica tres etapas. En una primera etapa, las organizaciones necesitan determinar las características de los documentos que mejor se adapten a sus requisitos de negocio, definir estas características y determinar la importancia de cada una. En la segunda etapa, la organización debe evaluar el impacto que podría tener en sus objetivos de negocio el hecho de que los documentos no cumplieran con los requisitos establecidos. En la tercera etapa, se deben incluir las posibles amenazas que pueden provocar el incumplimiento con los requisitos definidos, la probabilidad de que esto ocurra y las causas que pueden ocasionarlo. Este enfoque contiene las siguientes etapas:

1. Identificación de los requisitos aplicables.
2. Identificación de los riesgos a partir del cumplimiento o no con los requisitos.
3. Identificación de amenazas, que complementa la determinación de los riesgos.

En la siguiente figura se pueden ver ambos enfoques y su relación con la identificación de riesgos documentales (ver Figura 5).



Figura 5 - Enfoques para la identificación y gestión de riesgos de información y documentos (Lemieux 2004b).

El enfoque basado en requisitos es muy similar al que propone la normativa internacional ISO, en concreto el informe técnico ISO/TR 18128, en su apartado 4.2, que afirma que los riesgos se identifican basándose en su potencial para socavar las características generales de los documentos (AENOR 2014, p. 9) (autenticidad, integridad, fiabilidad y usabilidad), haciendo que no satisfagan los propósitos para los que fueran creados.

Ambos enfoques, según Lemieux, tienen ventajas e inconvenientes. Por ejemplo, el enfoque basado en hechos puede conllevar la rápida identificación de estrategias de prevención o mitigación de los riesgos, ya que se basa en la determinación directa de un acontecimiento desencadenante o amenaza. En cambio, a la hora de detectar fallos del sistema o de procedimiento puede resultar más eficaz el enfoque basado en requisitos, ya que analiza los procesos de negocio y detecta fallos en los flujos de información.

El enfoque basado en requisitos tiene otras ventajas, ya que empieza por analizar los requisitos documentales con los que necesita cumplir la organización para alcanzar sus objetivos y, por tanto, puede ser un mejor método cuando se use la gestión de riesgos como un proceso estratégico.

El enfoque basado en amenazas, dado que se basa en un método usado frecuentemente en las organizaciones para

la gestión del riesgo (Lemieux 2004b, p. 48) será más fácilmente integrado en cualquier taxonomía ya existente o en el sistema de gestión del riesgo que la organización esté utilizando.

A continuación, se presentan las fortalezas y debilidades de cada uno de los enfoques explicados, según Victoria Lemieux (ver Figura 6).

En conclusión, trabajar en función de uno u otro método depende de las necesidades y objetivos de la organización. Probablemente, lo más recomendable es emplear ambos enfoques de forma complementaria.

ENFOQUE	FORTALEZAS	DEBILIDADES
<i>basado en hechos</i>	Identificación de estrategias de mitigación del riesgo de manera más sencilla	Menos útil para lograr un enfoque estratégico
	Puede requerir menos tiempo y menos recursos	Puede perpetuar un acercamiento parcial en el tratamiento del riesgo
<i>basado en requisitos</i>	Más útil a la hora de definir una estrategia de defensa frente a una amenaza conocida	Puede pasar por alto causas sistémicas de los riesgos
	Mantiene un enfoque estratégico	Puede conllevar la inversión de más tiempo y recursos
	Promueve un acercamiento a la gestión del riesgo más creativo y multidisciplinario	Puede resultar menos útil a la hora de centrarse en analizar una amenaza conocida
	Más útil a la hora de identificar tipos sistémicos de riesgos de la información y la gestión de documentos	Puede resultar difícil su integración en una práctica de gestión del riesgo ya existente en una organización

Figura 6 - Fortalezas y debilidades de los enfoques de identificación de riesgos según Lemieux.

Análisis de riesgos documentales

Los riesgos se analizan para poder determinar sus consecuencias potenciales y la probabilidad de que ocurran (AENOR 2014, p. 9). El análisis de riesgos siempre tiene en cuenta, por tanto, una combinación de causas o fuentes, probabilidad y consecuencias (ver Figura 7).



Figura 7 - Factores para el análisis de riesgos (elaboración propia).

Los métodos de análisis propuestos por las normas ISO (AENOR 2011a; 2014) son tres: cualitativos, semi-cuantitativos y cuantitativos. Se explican brevemente a continuación:

- Los métodos cualitativos pueden combinar consecuencias, probabilidad y nivel del riesgo mediante niveles significativos como “alto”, “medio” y “bajo”.
- Los métodos semi-cuantitativos utilizan escalas numéricas para las consecuencias y probabilidades, y las combinan utilizando una fórmula para determinar el nivel de riesgo. Las escalas pueden ser lineales o logarítmicas, o tener cualquier otra relación; la fórmula utilizada puede variar.
- Los métodos puramente cuantitativos son los que utilizan valores numéricos para las consecuencias y sus probabilidades, se pueden utilizar (estadísticamente) donde haya datos disponibles sobre el desempeño de los procesos y sistemas de gestión documental durante un periodo significativo, para ello es necesario el desarrollo de indicadores y controles que permitan estas mediciones a lo largo del tiempo.

Con relación a las consecuencias, su análisis determina la naturaleza y el impacto que podría tener un evento, situación o circunstancia en particular si ocurriese. Dicho evento puede tener un rango de impacto de magnitudes diferentes, así como afectar a diferentes objetivos y partes interesadas. Los tipos de consecuencias a analizar y las partes interesadas afectadas pueden ser determinadas a partir del análisis del contexto de la organización. Las consecuencias, con relación a la gestión documental, se identifican con la inexistencia, la pérdida, el uso indebido o el daño a los documentos (entre otros), hechos que afectan a su usabilidad, autenticidad, completitud e inalterabilidad a lo largo del tiempo y, por consiguiente, podrían fallar a la hora de dar soporte a las actividades de la organización (como son el cumplimiento de objetivos, la eficiencia y la eficacia, los flujos de información, la rendición de cuentas, entre otras).

El análisis de las consecuencias puede centrarse en dos aspectos diversos. Por un lado, analizando la severidad del riesgo y su afectación dentro de la organización, proceso o procedimiento; y, por otro lado, apuntando las posibles consecuencias que podrían ocurrir si se da el riesgo, como, por ejemplo, la pérdida de credibilidad o fiabilidad de la organización, la pérdida de clientes, los despidos o las pérdidas económicas. Las consecuencias pueden valorarse junto con la severidad, aunque analizadas por separado, pueden proporcionar mucha más información para una toma de decisiones informada. Los factores a tener en cuenta son, entre otros (AENOR 2014, p. 23):

- El número de usuarios y otras partes interesadas afectadas.
- El efecto del daño o la pérdida de los documentos en las operaciones en curso de la organización.
- Las medidas ya existentes para responder a la interrupción en el acceso a los documentos.
- El tiempo y el esfuerzo para recobrar o reemplazar los documentos afectados.
- El impacto de la pérdida para recobrar o reemplazar los documentos afectados.
- El impacto de la pérdida o el daño de los documentos en los derechos o propiedad de la organización.
- El impacto de la pérdida o el daño de los documentos en la capacidad de la organización para cumplir con sus obligaciones con todas las partes interesadas.
- Los requisitos legales y regulatorios de informar sobre los daños, pérdida o acceso no autorizado a los documentos.
- El impacto en la imagen pública de la organización.

Existen diferentes momentos en los que se necesitará un nuevo análisis del riesgo (básicamente, un ciclo completo de apreciación), incluyendo los siguientes motivos (Wheeler 2011, p. 44):

- Un cambio en la sensibilidad del activo, que es objeto del análisis.
- Un cambio significativo en el entorno de amenazas.
- Un cambio en los requisitos legales o normativos.
- Un cambio en la política de seguridad.
- Según los plazos previstos, en función de la sensibilidad al riesgo de los activos.

También se pueden incluir cambios en el diseño o la implantación del sistema de gestión, como posibles desencadenantes de un nuevo análisis de riesgos.

Tal y como se ha apuntado anteriormente, normalmente las consecuencias se asocian con pérdidas o con resultados negativos. Sin embargo, tal y como se menciona en las normas ISO, también puede relacionarse con beneficios u oportunidades de mejora. Las oportunidades se explican por los beneficios potenciales que pueden obtenerse al asimilar un riesgo, un aspecto más relacionado con los negocios o el mundo financiero que con la gestión documental.

Lo que interesa destacar en este capítulo, sin embargo, es otro tipo de relación positiva entre el análisis y el tratamiento de los riesgos y las oportunidades de mejora o beneficios que resultan de ello. A la hora de prevenir o tratar un riesgo, indirectamente se beneficia todo el sistema, ya que se está trabajando en un aspecto sobre el que quizás no se realizaría ninguna acción si no fuese porque se ha identificado ese riesgo relacionado. Por tanto, al mismo tiempo que se previene un riesgo se obtiene un beneficio o una mejora.

Mediante la normalización de la gestión de riesgos documentales pueden, por tanto, alcanzarse mejoras en el desempeño de la gestión documental en las organizaciones. Algunos ejemplos de ello son (Lemieux 2004b, p. 56):

- Planificación más efectiva de las estrategias y programas de gestión documental para asegurar su alineación con los objetivos estratégicos del negocio.
- Mejor control de los costes de la gestión de documentos e información.
- Mejora de la evaluación y medición de las funciones de la gestión de documentos e información.
- Mejora de la toma de decisiones sobre la gestión de documentos e información.
- Aumento del valor compartido, resultado de unas estrategias creíbles para mitigar los riesgos relacionados con la gestión de información y documentación.
- Mejora de la conformidad con relación a los requisitos legales y normativos relacionados con la gestión de documentos e información.

Evaluación de riesgos documentales

La evaluación del riesgo es aquella fase de la apreciación de riesgos que proporciona un proceso estructurado para identificar cómo los riesgos pueden afectar a los objetivos. El propósito de la evaluación del riesgo es ayudar a tomar decisiones sobre qué riesgos necesitan tratamiento y con qué prioridad, partiendo de los resultados del análisis de los riesgos (AENOR 2014, p. 22).

Se parte del resultado del análisis para una toma de decisiones adecuada sobre las acciones a implantar. Las decisiones pueden incluir, entre otras cuestiones, cuándo un riesgo necesita tratamiento, la prioridad de tratamiento o cuándo una actividad debe llevarse a cabo. La decisión sobre si tratar el riesgo, y cómo hacerlo, dependerá de los costes y beneficios asociados a correr el riesgo y los costes y beneficios asociados a implementar acciones de control y de mejora. Para las decisiones se debe tener en cuenta el contexto más amplio del riesgo e incluir la consideración de la tolerancia del riesgo por otras partes diferentes de la organización, que se benefician del riesgo. Las decisiones se deben tomar de acuerdo con los requisitos legales, reglamentarios y requisitos de otro tipo (AENOR 2010, p. 25).

Además, la evaluación debe considerar los siguientes principios (Lemieux 2004a, p. 27):

- Objetividad: los métodos de medición se basan en criterios normalizados.
- Consistencia: los riesgos que se evalúan son aquellos que aparecen en la documentación relacionada con su gestión.
- Relevancia: los riesgos documentados se pueden gestionar.
- Transparencia: todo aquello relacionado con la gestión de los riesgos se informa y se documenta.
- Aplicación a toda la organización: los riesgos engloban toda la organización.
- Completitud: todo lo que puede conllevar riesgos ha sido identificado.

Lo ideal es que los sistemas no fallen, pero lo cierto es que se acepta convivir con sistemas que fallan. El asunto no es tanto la ausencia de incidentes, sino la confianza en que están bajo control: se sabe qué puede pasar y se sabe qué hacer cuando pasa (Amutio Gómez *et al.* 2012, p. 7). En este sentido, determinar el nivel de tolerancia de los riesgos es

uno de los aspectos fundamentales. El nivel de tolerancia es la máxima exposición posible al riesgo que es aceptable, basándose en los beneficios y costes asociados (ARMA International 2009, p. 20). Debe revisarse de manera periódica, teniendo en cuenta los cambios en procedimientos o políticas de la organización, así como otros aspectos del contexto interno y externo.

Cabe mencionar que la evaluación del riesgo, en relación con la probabilidad y las consecuencias adversas, debe dar el suficiente peso a los incidentes excepcionales o sin precedentes cuando tienen un impacto generalizado y grave hasta el punto de catastrófico. Asimismo, el impacto de una acumulación de incumplimientos leves puede ser muy superior a un incidente individual, si el resultado es el deterioro de la integridad y fiabilidad de los documentos o del sistema de gestión documental (AENOR 2014, p. 22). Se deben valorar ambas situaciones para la toma de decisiones sobre el mejor tratamiento posible.

2.2.4 Tratamiento del riesgo

Una vez completado el proceso de apreciación del riesgo, deben llevarse a cabo las acciones necesarias para el tratamiento del mismo. Esto conlleva seleccionar y acordar una o más opciones para cambiar la probabilidad del incidente, el efecto de los riesgos, o ambos, así como la implementación de dichas opciones. Se trata de un proceso cíclico en el que se dan las siguientes etapas (AENOR 2010, p. 25):

- Evaluar el tratamiento del riesgo.
- Decidir si los niveles del riesgo residual son tolerables.
- Si no lo son, decidir un nuevo tratamiento del riesgo.
- Evaluar la eficacia del nuevo tratamiento.

Las opciones de tratamiento del riesgo no se excluyen unas a otras, ni todas son apropiadas en cualquier circunstancia. Existen múltiples formas de tratar un riesgo y el simple hecho de ignorarlas, o ignorar el riesgo, implica la aceptación a su exposición. La selección de la opción más apropiada implica una compensación de los costes y esfuerzos de la implementación, en función de los beneficios o ventajas que se puedan obtener (AENOR 2010, p. 25). Existen varias opciones para tratar riesgos, por ejemplo:

- Aceptación: una decisión puede ser aceptar que el riesgo pueda suceder. Cuando se acepta un riesgo, la organización debe reservar fondos para el caso de que el riesgo se concrete y haya que responder a sus consecuencias (Amutio Gómez *et al.* 2012, p. 54).
- Eliminación: eliminar la actividad que puede causar el riesgo o la fuente.
- Transferencia o compartición: debido a que la transferencia puede ser parcial o total, es más general referirse a “compartir el riesgo”. Hay dos formas básicas de hacerlo: repartir responsabilidades o contratación de seguros, de manera que el asegurador corre con las consecuencias (Amutio Gómez *et al.* 2012, p. 54).
- Mitigación: incluye dos opciones, como son reducir la degradación causada por una amenaza o reducir la probabilidad de que una amenaza se materialice (Amutio Gómez *et al.* 2012, p. 53).

Algunas opciones de tratamiento pueden aplicarse individualmente o bien en combinación, siempre que sea beneficioso para la organización. Al seleccionar las opciones de tratamiento del riesgo, la organización debería tener en

cuenta los valores y percepciones de las partes interesadas. Cuando las opciones de tratamiento impacten o puedan impactar sobre el riesgo en cualquier otra parte de la organización o en las partes interesadas, estas deberían involucrarse en el proceso de toma de decisión (AENOR 2010, p. 26).

Además, el fallo o la ineficacia de las medidas de tratamiento del riesgo pueden constituir un riesgo mayor, por ello es fundamental realizar el seguimiento de las acciones para controlar y tratar los riesgos a lo largo del tiempo. A la hora de decidir las acciones para el tratamiento es fundamental considerar, no solo el impacto económico³³ sobre la organización, sino otros aspectos relacionados (Wheeler 2011b, p. 54), como son:

- Implementación del tratamiento.
- Recursos adicionales que serán necesarios.
- Formación y concienciación del personal.
- Reducción de la capacidad operativa debido a la complejidad del tratamiento.

Hay que tener presente que el tratamiento de un riesgo puede comportar, a su vez, la aparición de nuevos riesgos. También, que el tratamiento del riesgo puede introducir o ser causante de riesgos secundarios que necesiten pasar nuevamente por el proceso de gestión: comunicación, apreciación, tratamiento, seguimiento y revisión. Estos riesgos secundarios deben incorporarse al mismo plan de tratamiento que el riesgo original. La relación entre los dos riesgos debe identificarse y mantenerse. El plan de tratamiento debe, además, identificar con claridad el orden de prioridad en que deben implantarse los tratamientos de riesgo individuales. La norma ISO 31000 añade algunas opciones de tratamiento, complementando las anteriormente vistas (AENOR 2010, p. 25):

- Evitar el riesgo decidiendo no iniciar o continuar con la actividad que causa el riesgo.
- Aceptar o aumentar el riesgo a fin de perseguir una oportunidad.
- Eliminar la fuente del riesgo.
- Modificar la probabilidad.
- Modificar las consecuencias.
- Compartir el riesgo con otras partes (incluyendo los contratos y la financiación del riesgo).
- Retener el riesgo, basándose en una decisión informada.

Una vez se ha seleccionado el tratamiento adecuado para cada riesgo, es recomendable asignar un propietario para cada estrategia de control del riesgo, así como fijar plazos límite y metas concretas. Este enfoque debe incluir una estimación de los recursos necesarios para implementar cada estrategia de tratamiento (Lemieux 2004a, p. 28).

³³ – El coste total del control o tratamiento del riesgo no debería nunca exceder el coste del valor del activo o del potencial impacto del riesgo.

2.2.5 Seguimiento y revisión

El seguimiento y la revisión del proceso de gestión del riesgo deben planificarse y someterse a verificación o supervisión de manera regular. La gestión de riesgos documentales es un proceso sistemático que incluye la evaluación y el control de los riesgos identificados sobre el SGD en una organización. Para la implantación y el refuerzo de dicha gestión, no solo deben existir políticas, sino también procesos y procedimientos que den respuesta a las necesidades de la organización (ARMA International 2009, p. 20).

La revisión debería abarcar todo el proceso de gestión del riesgo con la finalidad de (AENOR 2010, p. 26):

- Asegurar que los controles son eficaces y eficientes.
- Obtener información adicional para mejorar el proceso de apreciación del riesgo.
- Analizar y sacar conclusiones de los sucesos, cambios, tendencias, éxitos y fallos.
- Detectar los cambios en el contexto interno y externo, incluidos los cambios en los criterios de riesgo y en el propio riesgo, que puedan requerir la revisión de los tratamientos, así como de la prioridad de actuación.
- Identificar riesgos emergentes.

Lemieux añade a esta lista (Lemieux, 2004a, p. 28):

- Supervisar los riesgos a lo largo del tiempo para detectar aumentos o disminuciones en su categorización.
- Supervisar que los procedimientos y la información obtenida en las fases de apreciación y tratamiento del riesgo es precisa y completa.
- Identificar cuándo un mejor conocimiento hubiese ayudado a tomar mejores decisiones.
- Identificar las lecciones aprendidas durante el proceso de gestión del riesgo.

La supervisión puede ser periódica o eventual. Las responsabilidades del seguimiento y la revisión deben estar claramente definidas y alineadas con las responsabilidades asignadas para las estrategias de tratamiento.

El avance en la implantación de planes de tratamiento del riesgo proporciona una medida de funcionamiento. Los resultados pueden incorporarse en la gestión global de la organización, en su medición y en las actividades internas y externas.

Los resultados del seguimiento y de la revisión deben documentarse e incluirse en informes internos y externos, según convenga. También se deberían utilizar como elementos de entrada para la revisión del marco de trabajo de la gestión del riesgo general (AENOR 2010, p. 27) y su mejora continua. Cabe recordar que no existe un único modo correcto de gestionar el riesgo (Lemieux 2004a, p. 29), por lo que la adaptación debe ser continua.

2.2.6 Documentación del proceso de gestión del riesgo

Las actividades de gestión del riesgo deberían ser trazables (AENOR 2010, p. 27). En este proceso la documentación proporciona la base para la mejora de los métodos y de las herramientas, así como del proceso en su conjunto. La

documentación y las evidencias son cruciales para poder llevar a cabo el seguimiento y la evaluación del proceso de gestión, así como para demostrar el nivel de mitigación y de control de los riesgos.

Las decisiones relativas a la creación de documentos y evidencias con relación al proceso de gestión del riesgo deben tener en cuenta, según la norma ISO 31000, (AENOR 2010, p. 27):

- Las necesidades de la organización en materia de aprendizaje continuo.
- Los beneficios de reutilizar la información para fines de gestión.
- Los costes y los esfuerzos que suponen la creación y el mantenimiento de los documentos y evidencias.
- Las necesidades legales, reglamentarias y operacionales para efectuar o generar los documentos.
- El método de acceso, la facilidad de recuperación y los medios de almacenaje.
- El periodo de conservación.
- El carácter sensible de la información.

Todos estos aspectos, relacionados directamente con la creación y el control de los documentos, ya se contemplan dentro de cualquier sistema de gestión documental, con lo que incluir la gestión del riesgo en un SGD supone tener, automáticamente, estas variables controladas y gestionadas de manera adecuada, ahorrando el desarrollo de herramientas y procedimientos específicos para la gestión de las evidencias documentales sobre la gestión del riesgo.

Además de la documentación mencionada, el informe ISO/TR 18128 recomienda documentar la identificación de los riesgos, ya sea en un registro específico para documentos o en el registro de riesgos de la organización (AENOR 2014, p. 10). Según esta norma, deben informarse los siguientes campos de información relativos a cada riesgo identificado:

- ID del riesgo: asignación de un número o código unívoco que identifica a cada riesgo de manera individual.
- Nombre del riesgo.
- Tipo o agrupación del riesgo.
- Propietario del riesgo, o responsable.
- Fecha de identificación: fecha en que se detectó el riesgo.
- Fecha de la última actualización: fecha en que se actualizó el registro del riesgo por última vez.
- Descripción: breve explicación sobre en qué consiste el riesgo.
- Manifestación del riesgo: circunstancias en las que el riesgo puede darse.
- Coste, si se materializa: monetario u otro.
- Probabilidad.
- Impacto.
- Estrategia para evitarlo: aquellas acciones que prevengan el riesgo.
- Estrategia para el tratamiento: aquellas acciones que mitiguen el riesgo.

- Fecha límite: en función de la implementación de las estrategias para evitar o mitigar el riesgo.
- Propietario de la acción/custodia: persona o área responsable del tratamiento o prevención del riesgo.
- Fecha de revisión: es el momento de actualizar la información relativa a la probabilidad y el impacto a partir del análisis de la efectividad de las acciones para el tratamiento o prevención del riesgo.
- Referencias cruzadas con riesgos relacionados: campo de información para indicar si el riesgo que se documenta está relacionado con otros riesgos identificados y registrados.
- Estado del riesgo y estado de la acción.
- Fecha de la última evaluación.

Para entender mejor a qué hace referencia cada uno de los campos de información, en la Figura 8 se puede ver un ejemplo de una entrada de un registro de riesgos, según el informe ISO/TR 18128.

DESCRIPCIÓN DEL RIESGO	
campos del registro	contenido
ID del riesgo	4
nombre del riesgo	incapacidad para determinar el creador de un documento
tipo o agrupación del riesgo	documento
propietario del riesgo	administrador de la aplicación de gestión de documentos (EDRMS)
fecha de identificación	12 / 10 / 2013
fecha de la última actualización	15 / 10 / 2013
descripción	incapacidad para descubrir quién es el creador de un documento registrado
manifestación del riesgo	incertidumbre acerca de la unidad de negocio creadora de los documentos
coste, si se materializa	bajo
probabilidad	media
impacto	alto
estrategia para evitarlo	revisar y fijar las plantillas de documentos dentro de la EDRMS
estrategia para el tratamiento	revisar y fijar las plantillas de documentos dentro de la EDRMS
fecha límite	31 / 12 / 2013
propietario de la acción / custodia	administrador de la EDRMS
fecha de revisión	31 / 01 / 2014
referencias cruzadas con riesgos relacionados	3; 12
estado del riesgo y estado de la acción	empezó la acción de mitigación del riesgo
fecha de la última evaluación	15 / 10 / 2013

Figura 8 - Ejemplo de una entrada de un registro de riesgos (ISO/TR 18128, Anexo A).

La documentación y las evidencias son un aspecto crucial. La documentación del riesgo es inherente al proceso de gestión del riesgo y no debe dejarse para el último momento, sino que debe implementarse desde la fase de identificación. Esto resultará de suma importancia para organizaciones que deben auditar sus sistemas de gestión, puesto que necesitarán evidencias documentales del proceso llevado a cabo para poder demostrar la mejora continua del sistema de gestión.

2.3 Enfoques para la identificación de riesgos documentales

La identificación del riesgo es el proceso que comprende la búsqueda, el reconocimiento y la descripción de los riesgos. Incluye la identificación de las fuentes del riesgo³⁴, los sucesos³⁵, sus causas y sus consecuencias potenciales. Puede incluir datos históricos, análisis teóricos, opiniones informadas de expertos, así como las necesidades de las partes interesadas (AENOR 2010, p. 11).

El objetivo consiste en generar una lista exhaustiva de riesgos, basada en aquellos sucesos que podrían crear, mejorar, prevenir, degradar, acelerar o retrasar el logro de los objetivos (AENOR 2010, p. 23). Es fundamental realizar una identificación exhaustiva, ya que un riesgo que no se identifica en esta etapa no se incluirá en las fases posteriores (análisis, evaluación y tratamiento).

Un factor a considerar es el hecho de que un riesgo puede tener más de una causa o, en otras palabras, varias causas pueden resultar en el mismo riesgo. Por ejemplo, en una organización, el riesgo de pérdida de información corporativa valiosa puede ser resultado de una inundación, un incendio, o de una eliminación intencionada por un empleado. De aquí se deduce que la relación entre el riesgo y la causa puede ser de uno a uno o de uno a muchos (Lemieux 2004a, p. 13).

En el ámbito de la gestión documental, actualmente, encontramos dos métodos principales existentes a la hora de llevar a cabo la identificación de riesgos en una organización. Por un lado, disponemos de la metodología desarrollada por la organización ARMA en su publicación "*Evaluating and Mitigating Records and Information Risks. An ARMA International Guideline*" y, por otro, de la metodología desarrollada por la organización ISO, en el informe técnico específico ISO/TR 18128, basado en la metodología de gestión del riesgo de la norma ISO 31000.

ARMA se aproxima al riesgo a través de la delimitación de cuatro grandes áreas relacionadas con la gestión de documentos en una organización. Estas son: área administrativa, área de control de documentos, área legal y área tecnológica. Su metodología propuesta pasa por la identificación de riesgos para cada una de estas áreas, como base para una gestión global del riesgo de la información y los documentos. Por su parte, ISO se aproxima a la identificación de riesgos a través de la delimitación de tres categorías relacionadas con la creación y el control de documentos

³⁴ – Se define la fuente del riesgo como cualquier elemento que por sí solo o en combinación con otros, tiene el potencial intrínseco de provocar un riesgo. Nota 1: no existe riesgo cuando otro objeto, persona u organización no interactúa con la fuente del riesgo; Nota 2: una fuente de riesgo puede ser tangible o intangible (AENOR 2010, p. 11).

³⁵ – Un suceso es la ocurrencia o cambio de un conjunto particular de circunstancias (AENOR 2010, p. 11).

en una organización: contexto, sistemas y procesos. Su propuesta pasa por la enumeración de diferentes áreas de incertidumbre enmarcadas en estas categorías, dentro de las cuales se identifican los riesgos con el objetivo de una gestión global del riesgo documental.

A continuación, se explican estas dos metodologías con detalle y se realiza una comparación entre ambas.

2.3.1 Metodología de identificación de riesgos propuesta por la organización ARMA

La organización ARMA propone un cuadrante (ver Figura 9) en el que incluye cuatro dimensiones del riesgo documental. Pretende ser un marco de referencia para el establecimiento de sistemas y metodologías para la evaluación de las amenazas que pueden afectar a la gestión del riesgo, tanto en organizaciones públicas como privadas.

En dicha publicación se describe un proceso estructurado para el desarrollo de un sistema de gestión de riesgos, que se sustenta en este cuadrante.



Figura 9: Cuadrante de riesgos según la metodología de ARMA.

En él se especifican cuatro categorías o dimensiones: riesgos administrativos, riesgos en el control de los documentos, riesgos legales o normativos y riesgos tecnológicos. Cada una de ellas se divide en diferentes áreas que se relacionan entre sí, jerárquicamente, con una categoría superior y el resto de categorías del cuadrante, con lo que el análisis resultante se presume completo y sólido.

La metodología ARMA describe cada una de las categorías y sus ámbitos relacionados con el objetivo de que el análisis de la situación de la organización, a partir de lo descrito, permita identificar debilidades y riesgos potenciales. Se acerca más a un listado de requisitos a considerar para una correcta gestión documental.

Riesgos administrativos

Son aquellos referidos a las amenazas relacionadas con la gestión del SGD de la organización. Se incluyen dentro de esta categoría tres grandes áreas: Gobernanza de la Información, Gestión del Cambio y Gestión de Emergencias. Cada una de estas tiene distintas cuestiones asociadas, a tener en cuenta para la identificación de los riesgos. Se explican a continuación.

- Gobernanza de la Información: ARMA la define como el establecimiento de políticas y procedimientos, así como la ejecución y mejora de ambos para el control y la gestión de la información dentro de la organización. Se debe definir un marco, dentro del cual poder gestionar, controlar, hacer accesible y usable la información, así como desarrollar los mecanismos para ello. En concreto, ARMA explica que, al identificar los riesgos dentro de esta categoría, deben tenerse en cuenta (ARMA International 2009, p. 6):
 - El compromiso constante por parte de todos los niveles de la organización: es crítico para el éxito de la gestión del SGD, ya que no se está gestionando un proyecto con principio y final, sino un proceso continuo.
 - La capacitación y formación adecuadas del personal encargado de la gestión de documentos: las cuestiones legales, normativas, tecnológicas y de aplicaciones informáticas son complejas dentro de un SGD y es por ello que los riesgos asociados a ellas deben ser gestionados por personal altamente cualificado y capacitado.
 - La creación de comités consultivos para la toma de decisiones en materia de gestión documental: los gestores de documentos no pueden llevar a cabo una gestión integral del riesgo en sus organizaciones sin la implicación y cooperación de otros profesionales cualificados, como administradores de sistemas o auditores, entre otros. Los comités pueden proporcionar retroalimentación y aconsejar sobre prioridades y estrategias. En algunas organizaciones, además, el comité consultivo tiene autoridad sobre la supervisión y es responsable sobre la toma de decisiones acerca de los aspectos relacionados con el SGD.
 - El desarrollo de políticas y procedimientos de gestión documental: las políticas y los procedimientos de gestión documental son componentes esenciales de cualquier SGD, ya que establecen directrices sobre la gestión de los activos de información. Para proteger a la organización, dichas directrices deben seguir la normativa legal y los requisitos de gestión de documentos asociados. Algunas organizaciones disponen de una sola política de gestión documental mientras que otras complementan dicha política con otras más específicas en materias como la captura, la retención, el acceso, la preservación u otros aspectos. Independientemente del enfoque sobre la política de la organización, este tipo de instrumentos normalmente incluyen, según ARMA:
 - Propósito, alcance y objetivos del SGD.
 - Definición de los documentos corporativos.
 - Responsabilidad sobre la información documentada que se relaciona con las operaciones del negocio de la organización.
 - Responsabilidades sobre las funciones de gestión documental.

- La formación continua en todos los niveles de la organización: las políticas y procedimientos de gestión documental no pueden llevarse a cabo sin una adecuada formación de la dirección, el personal, los proveedores y otras partes interesadas, ya que ellos son quienes generan, gestionan y conservan los documentos en nombre de la organización. La formación no debe darse una sola vez, sino que deben establecerse acciones formativas de manera periódica para garantizar que el personal conoce y está concienciado de sus responsabilidades y cuenta, además, con la información necesaria para desempeñar su trabajo conforme a los requisitos documentales establecidos.
 - La asignación de responsabilidades en materia de gestión documental en todos los niveles de la organización, además de la comunicación, información y formación sobre qué implican dichas responsabilidades. Estas deben incluirse en las descripciones de los puestos de trabajo y la organización debe asegurarse de que todos los trabajadores las conocen, las entienden y las aplican.
 - El seguimiento y evaluación del cumplimiento con lo anteriormente establecido: las políticas y procedimientos de gestión documental son diseñados y desarrollados para dar cumplimiento a los requisitos legales y normativos. Su supervisión por parte de los trabajadores ayuda a mitigar riesgos y permite identificar áreas de mejora dentro del SGD. Todo ello debe ser documentado. Pueden llevarse a cabo, también, auditorías internas o externas para comprobar que se cumplen los requisitos, políticas y procedimientos.
- Gestión del cambio: en este contexto se relaciona con los posibles cambios en la organización que podrían afectar al SGD, ya sean tecnológicos, de contexto, legales u otros. Cualquier modificación en los instrumentos de gestión documental solo puede tener éxito si en la organización existe una adecuada gestión del cambio, por lo que es un aspecto fundamental a tener en cuenta a la hora de identificar los riesgos. Dentro de esta área se incluyen cuestiones de comunicación, formación, así como de la progresión en la implementación de los cambios.
- Un plan de comunicación es un componente esencial en cualquier estrategia de gestión del cambio. La información sobre los cambios necesita ser difundida de manera regular, así como ser efectiva y honesta durante el tiempo que dure el proyecto. Los trabajadores necesitan conocer de qué forma cambiará su trabajo y qué se espera de ellos durante el proceso de cambio, además de poder dar su opinión y proporcionar sus conocimientos al respecto.
 - La formación también es un aspecto clave de cualquier estrategia de gestión del cambio. Deben considerarse tres principios básicos a la hora de planificar un programa de formación (ARMA International 2009, p. 9):
 - Se deben enmarcar las necesidades formativas de modo que los usuarios puedan ver de manera inmediata la utilidad de aquello que están obligados a aprender.
 - La formación es más efectiva cuando los usuarios participan en ella.
 - La formación es más efectiva cuando los usuarios pueden aplicar aquello aprendido de manera inmediata.
 - La implementación de la gestión documental de manera progresiva, por fases, beneficia a la organización y disminuye el nivel de riesgo, permitiendo disponer de recursos suficientes. Para el avance es

importante la retroalimentación de los trabajadores para solucionar de manera rápida los problemas que puedan darse, así como conseguir una mayor aceptación del cambio.

- Gestión de emergencias: ARMA la define como un enfoque planificado para la prevención de desastres referidos a la información y la documentación, incluyendo la respuesta a emergencias y la recuperación que sigue a una situación de emergencia o a un desastre (ARMA International 2009, p. 10). Se hace hincapié en que los desastres pueden ser tanto naturales (inundaciones o terremotos), como técnicos (incendios, robos y otros acontecimientos causados por un error humano) o civiles (conflictos bélicos, terrorismo o vandalismo). Dentro de esta área, a la hora de identificar riesgos, se contemplan estos dos aspectos: la prevención de desastres y la preparación para responder a un desastre. Desde el enfoque de lo que debe estar planificado se plantea la identificación de posibles amenazas que puedan afectar a los documentos y la información de cualquier organización.
 - La prevención de desastres implica la eliminación de amenazas, cuando sea posible, y la minimización de las pérdidas en caso de que ocurra un desastre. La mejor solución para la salvaguarda de los documentos críticos de una organización es el establecimiento de un programa de documentos esenciales.
 - La preparación para dar respuesta a un desastre se refiere a la planificación de la respuesta de la organización frente a una emergencia, con el fin de reducir las pérdidas potenciales. Debe involucrar a un equipo multidisciplinar, con representación de las áreas de gestión de documentos, tecnologías de la información, área legal y área de prevención. El proceso de planificación debe incluir lo siguiente (ARMA International 2009, p. 10):
 - Establecimiento de una estrategia para la respuesta frente a emergencias (acciones que deben llevarse a cabo durante e inmediatamente después de una emergencia) y una estrategia de recuperación (acciones que deben llevarse a cabo para la vuelta a la normalidad).
 - Desarrollo y documentación de un plan de continuidad del negocio.
 - Formación del personal, una vez aprobado el plan.
 - Revisión, actualización y comprobación del plan.

Riesgos en el control de los documentos

En esta categoría se incluyen los riesgos asociados con los principales procesos de gestión documental: clasificación, disposición y retención, y almacenamiento de los documentos. Es la categoría más operacional de las que propone ARMA en su cuadrante de riesgos y, por tanto, la más relacionada con la gestión de documentos propiamente. Se explican a continuación.

- Clasificación de los documentos³⁶: este proceso es especialmente importante cuando más de un departamento nutre de contenido un mismo expediente o se gestiona un trámite entre diversas áreas. Los metadatos proporcionan información descriptiva sobre los documentos, dotándolos de contexto y hacién-

³⁶ – ARMA incluye la descripción documental dentro de la clasificación.

dolos fácilmente recuperables, pero, para ello, debe existir un mínimo de metadatos obligatorios para la creación y el control de dichos documentos. Por último, también incluye la definición de directrices para nombrar documentos como otro modo de ayudar a la recuperación de información.

- Si los trabajadores de una organización no están concienciados sobre cómo definir la información sobre los documentos pueden realizar clasificaciones y descripciones distintas en función de la interpretación de cada individuo. Esto impedirá una recuperación rápida y pertinente de la información en un futuro. Con clasificaciones y descripciones inconsistentes o pobres es posible que la organización llegue incluso a perder información con el paso del tiempo.
 - Los metadatos son información específica y descriptiva sobre un documento, que puede ser utilizada como criterio de búsqueda para localizarlo. Es necesario establecer una buena definición de los metadatos básicos, como un complemento a la clasificación.
 - Las directrices sobre cómo nombrar un documento proporcionan convenciones que sirven como una herramienta más de la organización para la futura recuperación de la información. Es posible que algunos sistemas informáticos tengan limitaciones a la hora de nombrar documentos, como el número de caracteres que pueden utilizarse o la imposibilidad de usar espacios o signos de puntuación al guardar un documento.
- Retención y disposición de los documentos: dentro de esta área se mencionan dos aspectos a tener en cuenta: el establecimiento de tablas y políticas de retención, y la gestión por terceras partes. Las tablas y políticas de retención son necesarias para asegurar una gestión de documentos consistente, así como para evitar la destrucción prematura o no controlada de documentos. Respecto a la gestión por terceros, es obligación de la organización que externaliza parte de sus procesos asegurarse de que estos se llevan a cabo siguiendo las directrices y la legislación aplicables, así como tener presente la recomendación de llevar a cabo auditorías de manera periódica para comprobar que así se hace.
- Las políticas y tablas de retención son necesarias para asegurar que se conservan los documentos que es necesario conservar durante el tiempo que se requiera, para evitar eliminaciones antes de lo que marcan la ley y los requisitos, y para evitar eliminaciones tardías que pueden conllevar pérdidas económicas y de recursos en la organización. Un aspecto clave de la política de retención es su alineación con los requisitos legales y normativos aplicables. Se debe comprobar siempre, antes de la eliminación, que los documentos no están involucrados en ningún proceso legal o administrativo en curso.
 - Las organizaciones que externalicen la conservación y eliminación de su documentación son, en última instancia, responsables de los documentos y deben asegurarse de que la empresa contratada cumple con las tablas de retención de la organización. Lo más recomendable es llevar a cabo auditorías periódicas sobre las prácticas de la empresa contratada, así como exigirle informes y evidencias de cualquier eliminación llevada a cabo, previa verificación por parte de la organización que ha externalizado.
- Almacenamiento de los documentos: ARMA menciona tres aspectos importantes a la hora de identificar los riesgos: la evaluación del soporte, la migración y la disposición o eliminación. El almacenamiento de

documentos dependerá del soporte usado para almacenar, preservar, gestionar y eliminar dichos documentos. La organización debe decidir qué soportes va a utilizar en función de sus necesidades (por ejemplo, mediante un catálogo de formatos). También debe conocer los periodos de conservación de los documentos para poder decidir de manera coherente sobre los soportes, así como establecer procesos de migración de formatos para garantizar el acceso y la usabilidad a lo largo del tiempo que sea necesario. Estos procesos deben ser supervisados y testeados para asegurar que todos los componentes del documento, incluidos los metadatos, son migrados de modo que se asegure su fiabilidad, autenticidad, integridad y usabilidad. Además, cuando según las políticas de disposición se deban eliminar documentos, deberá poderse demostrar que estos no son accesibles de ninguna manera en ninguna de sus versiones.

- La decisión sobre el soporte requerirá de un entendimiento sobre los diferentes tipos existentes y su correlación con las necesidades de la organización. Se debe asegurar que se adquiere la tecnología adecuada para las necesidades de la organización. Debe crearse y aprobarse una lista de soportes (catálogo de formatos) para la organización, que identifique el tipo de soporte y la vida útil del mismo, con una breve descripción del contenido y la estimación de migraciones, si procede.
- La migración de soportes requerirá de un análisis previo por parte de la organización para determinar qué necesita ser conservado y durante cuánto tiempo, con la finalidad de planificar las migraciones con el fin de garantizar la accesibilidad. Debe asegurarse que se migrará todo el contenido de los documentos, así como los metadatos asociados de manera que pueda garantizarse su fiabilidad, autenticidad, integridad y usabilidad.
- Con relación a la disposición, cualquier organización debe ser capaz de demostrar que aquel documento que debía ser eliminado según la tabla de retención ha sido destruido en cualquier formato y versión existente, siendo imposible su recuperación. Deben conservarse evidencias de dicha eliminación con el fin de probar que se llevó a cabo siguiendo los requisitos legales y normativos aplicables (por ejemplo, mediante el registro de eliminaciones).

Riesgos legales o normativos

Son aquellos relacionados con el cumplimiento legal y normativo o reglamentario en relación con la gestión de documentos, de cualquier tipo de organización, ya sea pública, privada, no gubernamental, y de cualquier sector. ARMA incluye, en esta área, el cumplimiento legal y normativo, la capacidad de respuesta y la disponibilidad frente a posibles litigios.

- Cumplimiento legal y normativo: las organizaciones deben identificar aquellos requisitos que afectan a sus actividades y a la documentación que generan, reciben y gestionan. Se considera primordial para evitar posibles consecuencias negativas de incumplimiento legal. Se debe, por tanto, mantener actualizada la información sobre la legislación y normativa que les afecta, así como también todo lo referente a las buenas prácticas que aplican a su sector. En este punto, ARMA incluye una especificación con relación a las multinacionales, haciendo hincapié en la importancia de controlar la legislación referente a la retención y conservación de documentos, así como a las consideraciones de privacidad, ya que los requisitos de ambas pueden variar entre países (ARMA International 2009, p. 15).
- Cualquier profesional de la gestión de documentos debe entender completamente el entorno legal y normativo en el cual trabaja la organización en la que desarrolla su actividad. Este entorno incluye la legislación y normativa aplicable, así como la específica, según el sector en el que se enmarca. Tam-

bién, aquellas buenas prácticas existentes y sugeridas por los organismos estatales o los estándares internacionales. A nivel interno, debe desarrollarse una metodología actualizada para mantener la información sobre los requisitos legales y normativos, y para comunicar los posibles cambios a los departamentos afectados y las partes interesadas.

- La política de retención puede ser un aspecto crítico en las organizaciones multinacionales, debido a la coexistencia de diferentes contextos legales y al elevado número de regulaciones, leyes o normativas específicas, que pueden afectar a los requisitos aplicables a la retención y eliminación de los documentos de una misma organización.
 - Lo mismo puede ocurrir con la privacidad, ya que la mayoría de países han desarrollado leyes específicas para regular la protección de datos personales. Pueden darse diferencias legales entre dichas legislaciones, que puedan afectar a la captura, acceso, retención, localización y eliminación de documentos con información personal. Esto no solo afecta a información sobre clientes sino también a la información que custodia la organización sobre sus propios trabajadores.
- Capacidad de respuesta y disponibilidad frente a litigios: ARMA distingue entre la evaluación de dicha capacidad y la existencia de un plan para responder frente a litigios. Ambos aspectos comparten el objetivo de conseguir que la organización esté realmente preparada para responder con fiabilidad y pertinencia a cualquier solicitud de información en relación con un litigio o una auditoría. Para ello, algo fundamental es disponer de un buen SGD.
- La evaluación sobre la preparación de una organización frente a posibles litigios requiere la colaboración de personal de distintos ámbitos: gestión documental, tecnologías de la información, gestión de riesgos, departamento legal, así como diferentes unidades de negocio. Se deben evaluar varios aspectos como, por ejemplo, si la política de retención está actualizada, si la organización cumple dicha política o si existe un procedimiento establecido para hacer frente a litigios.
 - Un plan de respuesta frente a litigios garantiza a la organización que el resultado de un litigio, auditoría o investigación esté basado en algo substancial, más que en problemas de procedimiento. Dicho plan debe documentarse y puede incluir:
 - Roles y responsabilidades de gestión documental, tecnologías de la información, departamento legal y proveedores externos.
 - Políticas y procedimientos de gestión documental.
 - Inventario de aplicaciones informáticas de gestión documental, con la descripción de las mismas, y de las características del repositorio virtual de la organización.
 - Cumplimiento con las auditorías.

Riesgos tecnológicos

Dentro de cualquier SGD existen riesgos asociados con la tecnología. ARMA, dentro de esta categoría, se centra en tres aspectos: la seguridad de la información, las comunicaciones electrónicas y el control de las aplicaciones de software.

- Seguridad de la Información: incluye la creación de un programa de protección y pérdida de información, el desarrollo de controles de acceso y la comprensión de las necesidades de confidencialidad. El primero debe ser capaz de identificar contenido sensible de la organización e implementar controles para su creación, recepción, uso y distribución para prevenir cualquier incidencia, ya sea interna o externa. El acceso a la información también requiere de controles específicos para garantizar los niveles de confidencialidad. Debe existir un equilibrio entre acceso y seguridad.
 - Las incidencias relacionadas con la seguridad de la información se están incrementando en la actualidad, tanto aquellas relacionadas con ataques externos como los incidentes a nivel interno. Con el objetivo de proteger la información de la organización, se debe desarrollar, implementar y supervisar un programa efectivo para garantizar la seguridad de la información. Dentro de las actividades asociadas a dicho programa están, por ejemplo, la identificación de contenido sensible, así como la implementación de controles para la creación, recepción, uso y difusión o publicación de información y documentación. Cualquier vulnerabilidad en seguridad debe ser identificada.
 - Los controles de acceso a la información deben crearse como parte de la estrategia de seguridad. Deben desarrollarse cuadros de seguridad y acceso, con la definición de diferentes roles, con diferentes permisos y niveles de acceso a la documentación, buscando siempre el equilibrio entre los requisitos de seguridad y el acceso a la información.

- Comunicaciones electrónicas: las cuestiones clave identificadas por ARMA son: la creación autorizada de métodos de comunicación, la necesidad de realizar transmisiones seguras y la necesidad de gestionar los contenidos que los métodos de comunicación electrónica crean, transmiten o almacenan. Muchos procedimientos o trámites se inician con una comunicación electrónica y es por ello que estas comunicaciones deben gestionarse como si fueran documentos propios de la organización. Para ello es fundamental conocer las aplicaciones con las que se trabaja, su integración e interoperabilidad.
 - Cualquier organización necesita conocer todos los métodos de comunicación electrónica que se utilizan. Deben desarrollarse e implementarse políticas sobre comunicación electrónica para formar y concienciar a los trabajadores sobre el uso apropiado de las tecnologías de comunicación. Adicionalmente, pueden llevarse a cabo auditorías de cumplimiento de las políticas y acciones disciplinarias para reforzar dicho cumplimiento.
 - En el momento en que la información se envía fuera de la organización, se hace necesario tomar medidas que aseguren que el contenido queda totalmente protegido, en línea con los requisitos de confidencialidad aplicables. Deben crearse protocolos sobre transmisión de información y cumplirse de manera estricta.
 - Partiendo de que una gran parte del negocio se inicia y se completa vía correo electrónico, existe una necesidad de gestionar estas comunicaciones externas como si fueran documentos, para garantizar que se almacenan de manera adecuada, que se realizan las copias de seguridad necesarias y que todo ello se supervisa para su correcto cumplimiento.
 - Es necesario, además, llevar a cabo una revisión periódica de las aplicaciones que crean y conservan información y documentos de la organización. Es fundamental tener claros los requisitos, entender cómo las aplicaciones se integran entre ellas y con otras aplicaciones, y disponer de un plan de desmantelamiento del sistema para evitar la materialización de riesgos.

- Cuando se implementen nuevas tecnologías en la organización, es importante considerar el impacto que estas pueden tener en las ya existentes, con el objetivo de prevenir posibles problemáticas e incidencias en los procesos que ya se están llevando a cabo. Se debe, además, asegurar la compatibilidad y la usabilidad de las actualizaciones y el cumplimiento de las aplicaciones con las políticas, normativa y legislación aplicables, cuando proceda.
- Cuando se implementen nuevas tecnologías en la organización es muy importante considerar las necesidades sobre un posible desmantelamiento de sistemas o aplicaciones, y llevar a cabo una evaluación del impacto que esto puede tener sobre la información y los documentos, con el fin de evitar pérdidas irrecuperables.

En el sistema ARMA, a partir de estos ámbitos, se propone un cuestionario de 33 preguntas para la realización de la evaluación del riesgo de la información y los documentos. Este cuestionario se divide en cuatro apartados basados en las cuatro categorías del cuadrante de riesgos, que, a su vez, se subdividen en las once subcategorías o áreas explicadas anteriormente. El esquema general queda de la siguiente manera:

1. Riesgos administrativos
 - a. Gobernanza de la información
 - b. Gestión del cambio
 - c. Gestión de emergencias
2. Riesgos en el control de documentos
 - a. Clasificación
 - b. Retención y Disposición
 - c. Almacenamiento
3. Riesgos legales y normativos
 - a. Cumplimiento legal y normativo
 - b. Capacidad de respuesta frente a litigios
4. Riesgos tecnológicos
 - a. Seguridad de la Información
 - b. Comunicaciones electrónicas
 - c. Aplicaciones de *software*

Se asigna un valor numérico para cada respuesta, que debe sumarse para cada categoría, dando un resultado numérico que indicará el nivel de riesgo global, así como también por categorías. A menor valor, menor riesgo para la organización. En cambio, valores elevados reflejarán un alto potencial de riesgo e indicarán que la organización debe reexaminar su SGD con la finalidad de reducir la exposición al riesgo.

³⁷—La incertidumbre es el estado, incluso parcial, de deficiencia en la información relativa a la comprensión o al conocimiento de un suceso, de sus consecuencias o de su probabilidad (AENOR 2014, p. 7).

2.3.2 Metodología de identificación de riesgos propuesta por ISO en el informe técnico ISO/TR 18128

Para la identificación de riesgos documentales, el informe técnico ISO/TR 18128 identifica tres categorías relacionadas con la organización: contexto, sistemas y procesos. Dentro de estas, se definen diferentes áreas de incertidumbre³⁷, en su mayoría contextualizadas en entornos digitales o de documentos electrónicos, que se explican con mayor detenimiento a continuación.

La metodología es muy similar a la explicada por ARMA, aunque, en este caso, ISO se centra en las amenazas más que en los requisitos.

Contexto

Es fundamental, para poder identificar riesgos reales, conocer y analizar previamente el contexto de la organización, tanto interno como externo, puesto que las potenciales acciones que generan incertidumbre pueden ser tanto externas como internas a la organización.

La incertidumbre causada por cambios en el contexto puede diferir según la perspectiva de los diferentes niveles o capas de la organización (ver Figura 10).

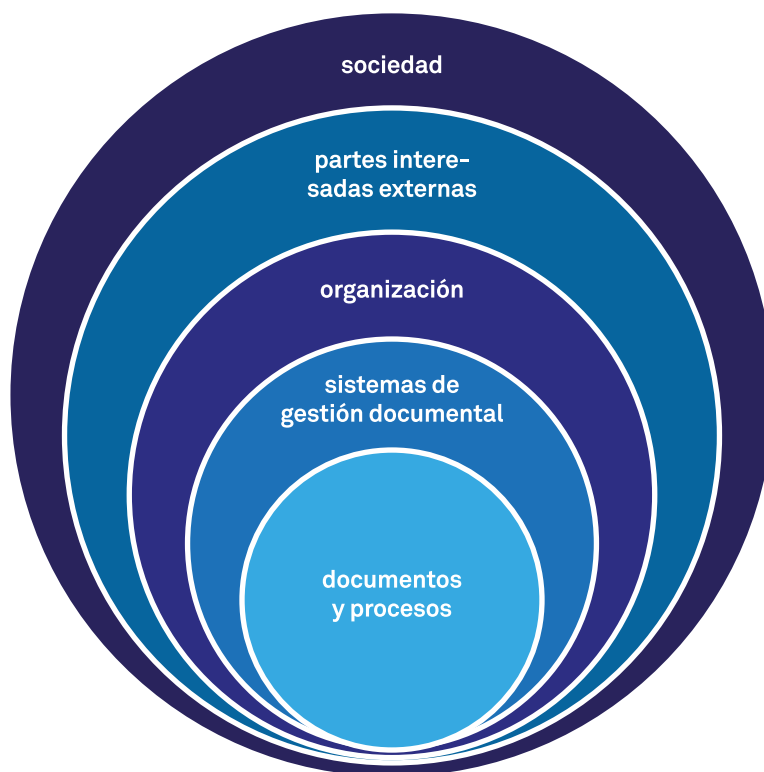


Figura 10– Múltiples capas de contexto de los documentos y los procesos de gestión documental de una organización (AENOR 2014, p. 10).

Se explican a continuación las áreas de incertidumbre que se incluyen en el contexto externo y el contexto interno.

- Contexto externo: se refiere al entorno político, social, macroeconómico y tecnológico, así como al entorno físico. Estos factores, pese a estar fuera del control de la organización, tienen un impacto en sus actividades, por lo que igualmente deben tenerse en cuenta. Este contexto incluye a las partes externas que tengan un interés especial en las actividades de la organización. Concretamente, incluye las siguientes áreas de incertidumbre: cambios en el entorno político-social, entornos macroeconómico y tecnológico, entorno físico e infraestructura, y amenazas de seguridad externas.
 - Cambios en el contexto político-social: estos cambios, ya sean en el ámbito nacional o internacional, pueden conllevar modificaciones legales y normativas con un posible impacto en las actividades u operaciones de la organización y, como consecuencia, en los requisitos de gestión de sus documentos. Algunos de los cambios pueden afectar al acceso a la información, a la privacidad, a los derechos de propiedad intelectual, a la responsabilidad social corporativa, entre otros. Algunos ejemplos incluyen (AENOR 2014, p. 11):
 - Cambios legales y normativos que afectan a los requisitos de gestión de los documentos de la organización.
 - Nuevos estándares o buenas prácticas que afectan a los documentos, sistemas y procesos de gestión documental.
 - Cambios en las expectativas de las partes interesadas.
 - Cambios en la reputación o en la confianza sobre la capacidad de la organización para prestar sus servicios.
 - Entorno macroeconómico y tecnológico: pueden tener un alto impacto en la organización, ya sea de manera gradual o puntual. Esto quiere decir que los cambios pueden ser continuos o puntuales. Se incluyen, entre otros, aspectos relacionados con el incremento de litigios, la introducción y adopción de nuevas tecnologías en la sociedad, o el aumento de la actividad de los organismos reguladores. Algunos ejemplos incluyen (AENOR 2014, p. 11):
 - Cambios en la propiedad de la organización, o en sus beneficios, que afectan a las prioridades de gestión, incluyendo la gestión de documentos.
 - Cambios en los objetivos, funciones y operaciones de la organización.
 - Incremento de la actividad de los organismos reguladores.
 - Introducción y adopción de nuevas tecnologías de modo transversal en la sociedad.
 - Cambios en el mercado y en los clientes de base de la organización.
 - Entorno físico e infraestructura: se refiere a la posibilidad de desastres, ya sean naturales o provocados por el hombre, que pueden afectar a la organización. Pueden causar un impacto directo en los documentos y en su almacenamiento. Algunos ejemplos incluyen (AENOR 2014, p. 11):
 - Fenómenos destructivos como terremotos, huracanes, ciclones, inundaciones, incendios o grandes tormentas.

- Potenciales acciones de guerra o terrorismo que pueden causar daños estructurales o interrupción del suministro a las instalaciones de la organización.
 - Cualquier otro trastorno relacionado con la energía, el agua, la gestión de residuos, las tecnologías de la información, los servicios de transporte u otras utilidades y servicios de la organización.
- Amenazas de seguridad externas: respecto a este tipo de situaciones, la identificación del riesgo debe incluir amenazas hostiles de seguridad, desde daños en las instalaciones o en la prestación de servicios hasta accesos no autorizados, tanto a las aplicaciones de gestión documental como a otras aplicaciones de gestión de la organización³⁸. Algunos ejemplos son (AENOR 2014, p. 12):
- Intrusiones o accesos externos no autorizados.
 - Cambios no autorizados en los documentos.
 - Fallos de seguridad o vulnerabilidad no identificados ni monitorizados, que conducen a la degradación o pérdida de información (como virus informáticos o brechas de seguridad).
 - Intrusiones físicas dentro de los depósitos de archivo de los documentos en papel.
 - Vandalismo.
 - Pérdida de servicios de terceros, de los cuales depende el SGD.
- Contexto interno: incluye aquellos factores internos no controlados por la persona responsable de los procesos y sistemas de gestión documental, como, por ejemplo, la estructura o las finanzas de la organización, el despliegue de tecnología, la dotación de recursos o la cultura de la organización. Esto influye en las políticas corporativas y en el modo en que se gestionan los documentos. Dentro de esta área, se analizan las siguientes áreas de incertidumbre: cambios en la organización, cambios tecnológicos, personas y competencias, y recursos económicos y materiales.
- Cambios en la organización: las decisiones sobre cambios como externalizaciones, reducciones, absorciones, reestructuraciones fusiones y otras, afectan al contexto interno, así como a los procesos y sistemas de gestión documental. Algunas incertidumbres relacionadas pueden ser, por ejemplo, la pérdida de la memoria corporativa, la no actualización de políticas o procedimientos, o los cambios en las responsabilidades sobre la documentación. Algunos ejemplos incluyen (AENOR 2014, p. 12):
- Cambios en la propiedad de los documentos y de los SGD que tienen como consecuencia traslados o transferencias de documentos a la organización y desde la organización.
 - Cambios en la propiedad de los documentos y de los SGD que tienen como consecuencia la migración forzosa de documentos o la fusión de sistemas.

³⁸ – Esta área de incertidumbre está directamente relacionada con la serie de normas ISO 27000 para la seguridad de la información.

- Cambio de los términos en los contratos de servicios con terceros.
 - Cambios en el personal de la organización que pueden afectar a las responsabilidades sobre los documentos.
- Cambios tecnológicos: la introducción de nuevas tecnologías y aplicaciones puede conllevar incertidumbres entre las que se incluyen la interoperabilidad entre sistemas y documentos, la migración de documentos, la capacidad de la infraestructura existente para cumplir con los nuevos requisitos resultantes del desarrollo tecnológico, o la efectividad en la implementación de los cambios, entre otros. Algunos ejemplos incluyen (AENOR 2014, p. 13):
- Cambios tecnológicos que afecten a la interoperabilidad entre sistemas de creación y control de documentos.
 - Compatibilidad con plataformas y aplicaciones existentes.
 - Capacidad de la infraestructura técnica existente para cumplir con los nuevos requisitos resultantes del desarrollo tecnológico de la organización y de los SGD.
- Recursos: personas y competencias. Las organizaciones necesitan personal capacitado y competente para desarrollar las funciones y actividades que les han sido asignadas, dentro de las cuales se incluyen las relacionadas con los procesos y sistemas de gestión documental. Las incertezas que afectan a esta área, entre otras, pueden ser la adecuación de las capacidades del personal para la creación y control de documentos, la pérdida de personal con habilidades clave y conocimiento en profundidad sobre la organización y sus políticas y procesos de gestión documental. Algunos ejemplos incluyen (AENOR 2014, p. 14):
- Número de personas que crean y controlan documentos.
 - Número de personas que diseñan y mantienen el SGD.
 - Pérdida de personal esencial con habilidades clave y conocimiento en profundidad de la organización o de su historia.
 - Deterioro de las habilidades del personal.
- Recursos: económicos y materiales. Además de los recursos humanos, también se incluyen en las áreas de incertidumbre del contexto interno los económicos y materiales, ya que el nivel de apoyo a la gestión documental en la organización afecta directamente a los recursos disponibles para poder llevar a cabo una adecuada gestión de los procesos y sistemas de gestión documental. Algunos ejemplos incluyen:
- Adecuación de los recursos económicos para alcanzar los compromisos y objetivos de gestión documental.
 - Adecuación de los recursos económicos para la adquisición, mejora o mantenimiento de los SGD.

- **Sistemas de Gestión Documental:** el SGD con que trabaja una organización cambia a lo largo del tiempo, en consonancia con las circunstancias económicas, cambios en las actividades y el personal, y cambios de tamaño y estructura. Por tanto, los sistemas se ven afectados por cambios en el contexto. Este apartado, según la metodología ISO, se refiere a los riesgos relacionados con los sistemas y aplicaciones que crean o controlan documentos. Engloba cinco áreas de incertidumbre: diseño de los sistemas, mantenimiento, sostenibilidad y continuidad, interoperabilidad y seguridad de los mismos.
 - **Diseño del sistema:** la configuración y el diseño del SGD son aspectos críticos para la creación y perdurabilidad de los documentos. Además, el diseño del sistema interactúa con la identificación de riesgos para los procesos de gestión documental y, por tanto, una buena documentación de la configuración del sistema es clave para abordar otras áreas de riesgo relacionadas. Algunos ejemplos de incertidumbre para esta área incluyen (AENOR 2014, p. 14):
 - La definición de los documentos que el sistema crea y gestiona de forma adecuada.
 - La correcta identificación de los requisitos de conservación.
 - La identificación y documentación de todos los procesos de gestión documental que se gestionan dentro del sistema.
 - La negociación de la dependencia del proveedor y el acceso a su documentación.
 - **Mantenimiento:** se refiere, sobre todo, a la plataforma tecnológica y a los aspectos que pueden verse afectados por cambios estructurales en la organización, cambios en el negocio y en los sistemas que afecten a los SGD, ya sea por la implementación de nuevas aplicaciones, por un cambio tecnológico o por la competencia y fiabilidad del proveedor y del soporte técnico. Algunos ejemplos incluyen:
 - Cambios en el negocio y en los sistemas operativos que afecten a los SGD.
 - Fiabilidad del proveedor del sistema y de su capacidad para mantener y conservar los sistemas actualizados.
 - Adecuación de los procedimientos de copias de seguridad para el SGD.
 - **Sostenibilidad y continuidad:** la sostenibilidad depende de que la supervisión de los cambios en el contexto interno y externo de la organización permita que el sistema se mantenga actualizado y sea capaz de responder a dichos cambios cuando sea necesario. El plan de continuidad se enmarca en el propio plan de continuidad del negocio y, para ello, se deben establecer prioridades de actuación y procedimientos para la restauración después de una interrupción del servicio. Algunos ejemplos de incertidumbre incluyen (AENOR 2014, p. 15):
 - La capacidad del SGD para mantener la usabilidad de los documentos.
 - La capacidad del SGD para importar documentos heredados de otros sistemas de gestión.
 - La migración de documentos a nuevos sistemas.
 - Cambios en otros sistemas o aplicaciones de los que el SGD depende.
 - **Interoperabilidad:** esta área se refiere a la capacidad de los sistemas de gestión documental de relacionarse con otros sistemas. Algunos ejemplos incluyen (AENOR 2014, p. 16):

- La identificación de las especificaciones requeridas para la interoperabilidad entre los SGD y otros sistemas de gestión.
 - La compatibilidad con normas o especificaciones para el intercambio de documentos o la interoperabilidad entre sistemas.
 - La gestión de metadatos relacionados con los controles de gestión documental para mantener la usabilidad y el significado de los documentos entre sistemas.
 - La dependencia del SGD de fuentes de datos externas y su capacidad para intercambiar, enlazar o referenciar los datos en estos sistemas (por ejemplo, en la nube o en servicios de almacenamiento externo).
- Seguridad: respecto a la seguridad del SGD, el informe técnico ISO/TR 18128 en su apartado 5.4.5 remite a la serie de normas ISO/IEC 27000 y en concreto a la norma ISO/IEC 27005³⁹, en la que se encuentran ejemplos de áreas de incertidumbre que son aplicables a cualquier sistema de información, en este caso, al SGD. Algunas de estas incertidumbres incluyen (AENOR, 2014, p. 17):
- La adecuación de la política de seguridad de la organización con respecto a los documentos, los procesos de gestión documental y el SGD.
 - La capacidad de aplicar y proteger las normas de acceso y los roles y permisos definidos por la organización, tanto para el personal interno como para los proveedores o personas que trabajan en nombre de la organización.
 - Las políticas y controles para terceros que trabajan en nombre de la organización y que afectan al almacenamiento, acceso y control de los documentos y al SGD.
- Procesos documentales: se refiere a los procesos de gestión documental, que engloban desde la creación hasta el control y la gestión de documentos. Se asume, según el informe técnico ISO/TR 18128, que los profesionales de la gestión de documentos utilizan como guía en el diseño de documentos y procesos de gestión documental, las normas ISO 15489⁴⁰, partes 1 y 2, e ISO 23081⁴¹, partes 1, 2 y 3. En esta categoría se analizan los riesgos de las siguientes áreas de incertidumbre: diseño de documentos, creación de documentos, implementación de sistemas de gestión documental, metadatos, uso de los documentos y los sistemas de gestión documental, mantenimiento de la usabilidad, y disposición.
- Diseño de documentos: es importante disponer de la información necesaria para el adecuado diseño de los documentos. Esto facilitará las tareas del día a día de la organización a partir de formatos estandarizados y documentos normalizados, siempre que sea posible. Algunas incertidumbres incluyen (AENOR 2014, p. 17):

³⁹ – ISO/IEC 27005: 2001. *Information technology - Security techniques - Information security risk management*.

⁴⁰ – ISO 15489-1, 2: 2001 – Información y documentación. Gestión de documentos. Parte 1: Generalidades; Parte 2: Directrices, traducidas al castellano en el año 2006. A día de la publicación del informe técnico ISO-TR 18128 seguían vigentes las dos partes de la norma ISO 15489 del año 2001. Actualmente han sido substituidas por la actualización de la norma publicada en 2016, que consta de una única parte.

⁴¹ – ISO 23081-1,2,3: 2008 – Procesos de gestión de documentos. Metadatos para la gestión de documentos. Parte 1: Principios. Parte 2: Aspectos conceptuales y de implementación. Parte 3: Lista de verificación. Esta familia de normas se está actualizando, habiendo sido publicada en 2017 la ISO 23081-1, que incluye los principios de la serie.

- Las actividades de negocio se analizan de manera adecuada para identificar los requisitos de gestión de documentos.
 - La recogida de requisitos se realiza de forma detallada para cada proceso de negocio, incluyendo las necesidades de todas las partes interesadas.
 - Idoneidad del diseño de los documentos para cumplir con los requisitos. Por ejemplo, la identificación del contenido y la definición de metadatos para identificar, describir y recuperar el documento, el historial de eventos y otros.
 - Clasificación adecuada.
- Creación de documentos e implementación de sistemas de gestión documental: se deben tener en cuenta todos los aspectos, incluso desde antes del momento de la creación y la captura de un documento, como la definición previa de los metadatos que se asignarán, las responsabilidades en todos los niveles de la organización o la integración de los procesos en los sistemas. Algunas incertidumbres incluyen (AENOR 2014, p. 17):
- Los momentos de creación y captura de todos los elementos de los documentos son apropiados para los diferentes procesos de negocio y para el SGD.
 - La efectividad de la integración de los procesos de creación y control de documentos con los procesos de negocio de la organización.
 - La definición, asignación y documentación de responsabilidades de los creadores de documentos y de otros agentes que participan en las actividades.
- Metadatos: las especificaciones de los metadatos deben ser accesibles para el personal autorizado y deben poder ser actualizadas cuando así lo requieran los procesos de negocio de la organización. Algunas incertidumbres incluyen (AENOR 2014, p. 18):
- Las especificaciones técnicas de los metadatos son accesibles.
 - La gestión de las especificaciones posibilita su actualización cuando sea necesario.
- Uso de los documentos y de los sistemas de gestión documental: el uso y la accesibilidad debe tener en cuenta todos los aspectos, desde la recuperación de información al control de accesos y la formación sobre los procesos asociados para garantizar que se cumplen los procedimientos establecidos en todos los niveles de la organización. Algunas incertidumbres incluyen (AENOR 2014, p. 18):
- Recuperación pertinente y a tiempo de los documentos, cuando se requiera.
 - Adecuación de la gestión de permisos de usuarios para todos los niveles de la organización y para todos los procesos de gestión documental.
 - Gestión de fallos de seguridad u otros controles de acceso.
 - Mantenimiento de la información sobre quién ha accedido o ha modificado documentos a lo largo del tiempo.
 - Adecuación de la formación del personal que trabaja con los procesos específicos.

- Mantenimiento de la usabilidad (relacionado con el punto anterior): además de lo anteriormente especificado, algunas incertidumbres relacionadas incluyen (AENOR 2014, p. 18):
 - Mantenimiento del significado de los metadatos a lo largo del tiempo, en especial los que dependen de datos o enlaces a sistemas externos.
 - Adecuación de los procesos de gestión documental para la preservación de la autenticidad y fiabilidad de los documentos a lo largo del tiempo.
 - Mantenimiento de la accesibilidad a los documentos a lo largo del tiempo.
 - Gestión de la utilización de la encriptación de documentos para las transmisiones.
 - Correcta gestión del historial de eventos para mantener su significado a lo largo del tiempo.
 - Aspectos relacionados con la obsolescencia del *software* (incluyendo los cambios de formato) y del *hardware*, relacionados tanto con los procesos de gestión documental como con los SGD.
- Disposición de documentos: debe implementarse y autorizarse, incluyendo el desarrollo de los procedimientos para llevarla a cabo. La destrucción debe hacerse siguiendo la legislación aplicable y debe estar debidamente autorizada y documentada. Del mismo modo, hay que garantizar la conservación de aquellos documentos que deban permanecer usables y accesibles a lo largo del tiempo. Algunas incertidumbres incluyen (AENOR 2014, p. 19):
 - Implementación de la disposición de los documentos tal y como ha sido diseñada y autorizada.
 - Procedimientos de disposición que incluyen la conservación más allá del periodo de retención, cuando se requiera. Por ejemplo, en relación con procedimientos legales o con el derecho de acceso a la información pública.
 - Destrucción de documentos autorizada y documentada de manera adecuada.

2.3.3 Comparativa entre las metodologías ARMA e ISO

Para realizar un análisis comparativo entre ambas metodologías, lo primero es visualizar la estructura global sobre la que se sustenta cada método. ISO divide la identificación de riesgos en tres grandes áreas: contexto, sistemas y procesos, centrándose así en la parte más operativa de la gestión de documentos y en aquellos aspectos que afectan directamente a los documentos. La metodología de ARMA hace una distinción en cuatro áreas: administración, control de documentos, legislación y tecnología, por lo tanto, es menos operativa y más generalista, e incluye aspectos que afectan a la gestión de documentos de manera indirecta.

La metodología descrita para la identificación de riesgos en el informe ISO/TR 18128 está más focalizada hacia la parte operativa, bajando muy al detalle en todos los aspectos referidos a los documentos, su creación, captura y control. En cambio, la metodología descrita por la organización ARMA está más enfocada a los riesgos de la gestión y la administración de los sistemas que crean, gestionan y controlan documentos. Aunque, en cualquier caso, ARMA

también dispone de un apartado específicamente enfocado a la identificación de riesgos asociados al control de los documentos. Eso sí, es un apartado de los cuatro del marco de trabajo.

Es posible que la diferencia de estructuras se deba a que el informe técnico ISO/TR 18128 es un desarrollo posterior de una norma general de gestión del riesgo, en la que se sustenta. No pasa lo mismo con la metodología ARMA, que no parte de un proceso general existente, sino que se define de principio a fin. Esto necesariamente conlleva la inclusión de aspectos globales de organización, planificación, gestión de recursos, entre otros, que, por el contrario, el informe técnico de ISO no necesita, puesto que ya están presentes en la norma ISO 31000. Esto puede resultar positivo con relación a que el ISO/TR 18128 se centra exclusivamente en aspectos operacionales, pero también incluye carencias importantes que, sin embargo, la metodología ARMA sí tiene en cuenta. Cabe mencionar también que, probablemente, el informe técnico de ISO puede ser más eficaz si se enmarca dentro de un sistema de gestión, es decir, si la organización que lo pone en práctica ya cuenta con un sistema normalizado tipo MSS. Del mismo modo, también puede resultar más eficaz si se trabaja dicho informe conjuntamente con la norma ISO 31000, con la finalidad de cubrir todos los aspectos organizacionales en el proceso, si bien en el informe no se especifica esta necesidad. Esto, a su vez, supone una debilidad de la metodología, puesto que implica trabajar con dos estándares en lugar de uno solo.

Por su parte, la metodología ARMA está pensada para aplicarse sin depender de otros sistemas o metodologías de gestión. Esto le proporciona una mayor autonomía que la que pueda tener el informe ISO.

En cualquier caso, aunque pueden trabajarse ambos modelos sin depender de otros sistemas de gestión, serán más eficaces si parten de sistemas de gestión documental implantados para poder resultar eficientes y aportar resultados útiles. De hecho, uno de sus objetivos es precisamente la mejora de la gestión documental en las organizaciones que decidan trabajar de acuerdo a las metodologías, tanto de ISO como de ARMA. Esta idea compartida debe ser la razón de ser de la gestión de riesgos documentales.

Otro punto de discordancia importante entre ambos modelos se relaciona con la idea de la mejora continua y la incorporación del ciclo PDCA en el informe ISO, que no se incluye en la metodología ARMA. Es una cuestión de suma importancia puesto que, como se ha mencionado anteriormente, la gestión de riesgos no es un proceso lineal, sino que debe entenderse como un proceso cíclico e iterativo, tal y como se indica en la introducción del ISO/TR 18128. En este sentido, el informe técnico se considera una mejor opción puesto que sí incluye en su metodología el ciclo de mejora para el proceso de gestión.

Partiendo de estas ideas, se considera que ambos sistemas, con sus semejanzas y discrepancias, son perfectamente válidos y que la mejor solución para una gestión global de los riesgos documentales dentro de una organización es la combinación de ambas metodologías, ya que, de ese modo, se contemplan aspectos de gestión y administración con aspectos operativos de la documentación y la información. Para que la gestión de riesgos documentales sea completa deben valorarse tanto aspectos puramente operativos como de la administración y gestión de los procesos y sistemas, y para ello, fusionar las dos metodologías es una de las mejores alternativas, ya que permite la identificación y la gestión de riesgos documentales de manera global.

Pero el proceso no finaliza ahí, sino que la organización y los responsables de gestión documental deben esforzarse, con el objetivo último de mejorar, implantando acciones y controles periódicos, designando responsables, implementando nuevos procesos, o revisando los ya existentes, para blindar el sistema de gestión documental y que este pueda cumplir su cometido. Para que esto ocurra los profesionales de la gestión de documentos deben adoptar una actitud proactiva, puesto que en muchos casos hay que anticiparse a lo que pueda pasar para conseguir prevenir los riesgos.

2.4 Implementación y mejora del proceso de gestión de riesgos documentales

Las áreas a tener en cuenta para una correcta implantación de la gestión de riesgos documentales, según ARMA, son (ARMA International 2009, p. 20): la estructura de la gestión de riesgos, las directrices de seguridad, la integridad de la información (datos y metadatos), y la formación y concienciación de los trabajadores sobre el cumplimiento de las directrices de gestión de riesgos. Estas áreas se explican con mayor detenimiento a continuación.

Estructura de la gestión de riesgos

En cualquier implantación de cualquier sistema de gestión, especialmente de gestión de riesgos, es fundamental contar con el compromiso y apoyo de la alta dirección. La introducción de la gestión del riesgo y la garantía de su eficacia continua requieren de un compromiso fuerte y sostenido de la dirección de la organización, así como de una planificación estratégica y rigurosa para conseguir el compromiso en todos los niveles (AENOR 2010, p. 16). El compromiso de la dirección asegura la eficacia y el mantenimiento de este sistema de gestión, aporta recursos y capacitación para ello, y la posiciona como parte estratégica, con el objetivo de conseguir el compromiso de las demás áreas y niveles de la organización. Siguiendo la estructura de MSS de ISO, es fundamental poder contar con una política de gestión de riesgo definida y aprobada de manera formal, así como unos objetivos específicos alineados con dicha política.

La información que se proporcione resulta fundamental para definir el marco de gestión del riesgo, que sirve como base para desarrollar las políticas y procedimientos para la gestión de documentos y sus riesgos asociados. Este marco define los criterios del riesgo para la organización, entre ellos el nivel de tolerancia⁴².

Es importante desarrollar una política de gestión del riesgo para la organización, que debe ser apropiada para las dimensiones y la naturaleza de la misma, incluir información comprensible sobre los roles y responsabilidades para la gestión de riesgos, resultar clara a la hora de definir los criterios de incremento del riesgo, asegurar que los procesos y la infraestructura para su identificación y gestión se mantienen y, finalmente, establecer mecanismos para el seguimiento de la implantación de esta política (Lemieux 2004a, p. 33).

Directrices de seguridad

Deben desarrollarse directrices de seguridad para cada proceso de negocio. Estas deben sentar las bases para el uso adecuado de las tecnologías en la organización, la creación de diferentes niveles de acceso a la documentación y la definición de protocolos para el envío de documentación fuera de la organización (ARMA International 2009, p. 20). Estas directrices deberán incluir descripciones y procedimientos sobre el uso de la información y los documentos por

⁴²– Tal y como se ha definido anteriormente, determinar el nivel de tolerancia es uno de los aspectos fundamentales en la gestión del riesgo. El nivel de tolerancia al riesgo es la máxima exposición posible al riesgo que se considera aceptable, basándose en los beneficios y costes asociados (ARMA 2009, p. 20). El nivel de tolerancia al riesgo debe revisarse de manera periódica teniendo en cuenta los cambios en procedimientos o políticas de la organización así como otros aspectos del contexto interno y externo.

personas externas a la organización. Si se da el caso de que dichas personas externas tengan que acceder a información que se encuentra dentro del sistema interno de gestión de documentos de la organización, se deben fijar una serie de requisitos que estas deben cumplir para poder acceder.

Es importante el trabajo en equipo con los profesionales de Tecnologías de la Información, puesto que todas las directrices definidas incluyen la implementación de medidas electrónicas de seguridad.

Integridad de la información (datos y metadatos)

Para que un documento pueda considerarse auténtico, la integridad de la información que contiene debe permanecer intacta. Cuando dicha información se transmite, ya sea física o electrónicamente, es fundamental que llegue a su destino manteniendo su integridad y su autenticidad. Si esto no se consigue se pone en duda, no solo el documento en sí, sino el sistema mediante el cual fue transmitido o enviado (ARMA International 2009, p. 21).

Es importante implementar y realizar periódicamente controles a nivel interno que garanticen la validez e integridad de la información. Es igualmente importante comprender los canales externos a través de los cuales se transmite la información para garantizar que se mantienen los datos y metadatos originales y auténticos. Puede ser también necesario trabajar de acuerdo con unos estándares de seguridad o métodos que aseguren que el contenido no se puede alterar o modificar fuera del sistema de la organización (ARMA International 2009, p. 21).

Formación sobre el cumplimiento

Las organizaciones dependen de contar con personal competente para realizar sus actividades, incluyendo los procesos y los sistemas de gestión documental (AENOR 2014, p. 13). En el caso de la gestión de riesgos documentales, la formación continua sobre el cumplimiento de directrices, procedimientos o requisitos es necesaria en todos los niveles de la organización para que todos sean conscientes de sus responsabilidades y obligaciones en el mantenimiento de la información y los documentos de la organización. Los programas de formación continua deben ser parte de los programas de formación a largo plazo que la organización tenga definidos. Del mismo modo, también habrá que realizar formación específica para diferentes tipos de trabajadores, grupos, equipos de trabajo y otros perfiles (ARMA International 2009, p. 21).

A estas cuatro grandes áreas, la norma ISO 31000, de gestión de riesgos, añade la obligación de rendir cuentas, la integración en los procesos de la organización, la asignación de recursos y el establecimiento de los mecanismos internos y externos de comunicación y de información. No es posible implementar la gestión de riesgos documentales sin añadir estas cuestiones.

Es destacable el establecimiento de la obligación de rendir cuentas, la autoridad y las competencias apropiadas para gestionar el riesgo, incluyendo la información y el mantenimiento del proceso de gestión del riesgo, así como también asegurar la idoneidad, la eficacia y la eficiencia de todos los controles (AENOR 2010, p. 17).

Todas las organizaciones deberían marcarse el objetivo clave de disponer de un nivel apropiado de desempeño en su marco de trabajo de la gestión del riesgo (AENOR 2010, p. 28). Sin embargo, siguen existiendo una serie de resistencias a la introducción de modelos integrales de gestión del riesgo en las organizaciones. Estas derivan principalmente

de la inexistencia de valores sobre el riesgo en la cultura corporativa (cultura del riesgo), la falta de apoyo y convencimiento del primer nivel de la estructura, la deficiencia en la comunicación, el predominio de búsqueda de medidas que mejoren la eficiencia operativa, la falta de cohesión entre la cultura del riesgo y la configuración organizativa, la escasez de recursos para respaldar la gestión del cambio y el mantenimiento de un Sistema de Gestión Integral del Riesgo, y la inexistencia de terminología común y procedimientos que orienten la gestión interna del riesgo (Martínez García 2009, p. 5).

Para combatir estas causas uno de los recursos fundamentales son los estándares internacionales. Por ejemplo, en la norma ISO 31000, en el Anexo A (informativo), se propone una serie de atributos a tener en cuenta para ayudar a las organizaciones a medir su propio desempeño con respecto al proceso de gestión del riesgo, proporcionando a su vez algunos indicadores para cada atributo. Estos atributos son (AENOR 2010, p. 28) la mejora continua, la responsabilidad sobre los riesgos, la aplicación de la gestión de riesgos a la toma de decisiones, la comunicación continua y la integración completa de este proceso en la estructura de gobierno de la organización. Se explican a continuación.

Mejora continua

Según la norma ISO 31000, la evaluación del desempeño de la gestión del riesgo es una parte integral de la evaluación del desempeño global de la organización y del sistema de medición de la práctica de los departamentos y las personas. Se pone énfasis en la mejora continua de la gestión del riesgo mediante el establecimiento de metas de desempeño organizacional, medición, revisión y la modificación posterior de los procesos, sistemas, recursos, la capacidad y las habilidades.

Algunos indicadores propuestos son: la existencia de objetivos de desempeño explícitos que permitan medir el desempeño individual de los responsables, así como el de la propia organización. En esta norma se recomienda una revisión anual, que puede complementarse con una revisión de los procesos y del establecimiento de los objetivos de desempeño revisados para el periodo siguiente.

Responsabilidad completa de los riesgos

Independientemente de la estructura organizativa para la gestión de riesgos, cualquier organización debe establecer los roles y las responsabilidades de cada parte interesada de manera que se identifiquen claramente y que puedan comunicarse (Lemieux 2004a, p. 30). Las personas designadas deben aceptar la responsabilidad de manera completa, tener las habilidades necesarias, disponer de los recursos adecuados y ser capaces de comunicar eficazmente a las partes externas e internas sobre todo aquello relacionado con los riesgos y su gestión. En el caso de la gestión de riesgos documentales, los profesionales mejor preparados son los archiveros o gestores de documentos, ya que conocen a la perfección el funcionamiento de los procesos e instrumentos de gestión documental de la organización.

Por su parte, la organización debe asegurarse de que todas las personas responsables disponen de todo lo necesario para cumplir su función, proporcionándoles la autoridad, el tiempo, la formación, los recursos y las capacidades necesarias para asumir sus responsabilidades.

Algunos indicadores propuestos por la norma son, por ejemplo, el hecho de que todos los miembros de la organización hayan tomado conciencia de los riesgos, de los controles y de las tareas de las que son responsables.

La definición de las funciones, la obligación de rendir cuentas y las responsabilidades en materia de gestión del riesgo deberían formar parte de todos los programas de acogida para las nuevas incorporaciones a un puesto o una función dentro de la organización (AENOR 2010, p. 28).

Aplicación de la gestión del riesgo en todas las tomas de decisiones

Cualquier toma de decisión de una organización, cualquiera que sea el nivel de importancia o relevancia, implica la consideración explícita de los riesgos y de la aplicación de la gestión del riesgo, a partir de su análisis y evaluación.

Algunos indicadores propuestos son, por ejemplo, la existencia de evidencias documentales de las reuniones y de las decisiones, donde se muestre la realización de las discusiones explícitas sobre los riesgos. Además, debe ser posible comprobar que todos los componentes de la gestión del riesgo están representados en los procesos de toma de decisiones clave de la organización.

Comunicación continua

Una gestión del riesgo optimizada incluye comunicaciones continuas con las partes interesadas, tanto a nivel interno como externo, incluyendo la existencia de informes documentados sobre el desempeño de la gestión del riesgo como parte del buen gobierno de la organización.

Los informes, tanto sobre los riesgos como sobre el desempeño de la gestión del riesgo, contribuyen sustancialmente a un buen gobierno y a un gobierno eficaz de la organización.

Algunos indicadores propuestos son, por ejemplo, las acciones de comunicación con las partes interesadas. La comunicación se contempla como un componente de doble sentido, de manera que se puedan tomar decisiones informadas de manera adecuada sobre el nivel de riesgo y sobre la necesidad de un tratamiento u otro en función de los criterios de riesgo establecidos previamente.

Integración completa en la estructura de gobierno de la organización

La gestión del riesgo se considera un aspecto central en los procesos de gestión de cualquier organización, de manera que los riesgos se tratan en términos de efectos de incertidumbre sobre la consecución de los objetivos. La estructura y el proceso de gobierno de la organización se basan en la gestión del riesgo y dicha gestión se considera un aspecto esencial para la consecución de los objetivos. La gestión de riesgos debe integrarse en la estrategia y los presupuestos de la organización, así como ser permeable a todos los niveles (Lemieux 2004a, p. 30).

Algunos indicadores propuestos por la norma son, por ejemplo, el lenguaje de la dirección en relación con la gestión del riesgo, así como los materiales escritos de la organización que utilizan el término “incertidumbre” en relación con los riesgos (AENOR 2010, p. 29).

La gestión efectiva del riesgo depende de la toma efectiva de decisiones sobre el uso de tecnología, los procesos y las personas. Por tanto, el modo en que la organización gestione su sistema de gestión de riesgos es algo crítico (Lemieux, 2004a, p. 29). Tener en cuenta los aspectos mencionados en este apartado facilitará enormemente la gestión y permitirá mantener la estrategia de mejora continua. Lo más destacable es, sin duda, la integración de la metodología en el funcionamiento cotidiano de la organización y que esta pueda aprovecharse de ello para una toma de decisiones informada. Pero, para que todo lo anterior se desarrolle normalmente, antes es necesaria una gestión adecuada del cambio, a nivel interno y en las relaciones con proveedores y partes interesadas. Solo así las organizaciones podrán disponer de sistemas de gestión del riesgo optimizados y que mejoran con el tiempo.

Capítulo 3.

Marco teórico de la Transparencia y la Rendición de cuentas

El presente capítulo se aproxima a los conceptos de transparencia y rendición de cuentas, así como a la relación que ambos tienen con la gestión de documentos. Para ello, en primer lugar, se profundiza sobre la rendición de cuentas, se explica su proceso y los distintos tipos en función de sus objetivos. En segundo lugar, se hace lo mismo con la transparencia, haciendo hincapié en las características y los tipos existentes. Finalmente, se incluye un apartado en el que se ahonda en la relación entre la gestión de documentos, la transparencia y la rendición de cuentas. Este último apartado pone de relieve las relaciones entre los tres conceptos desde un punto de vista práctico.

La transparencia y la rendición de cuentas son dos conceptos relacionados entre sí y que persiguen objetivos comunes. La rendición de cuentas se explica a partir del modelo conceptual de principal-agente. Se trata de una configuración de la teoría de juegos donde un principal (por ejemplo, un ciudadano o un accionista) quiere que un agente (por ejemplo, el gobierno o el CEO de una organización) desempeñe una tarea concreta. En este escenario, la transparencia se corresponde con la habilidad del principal de observar lo que hace el agente. A mayor información sobre el comportamiento del agente, mayor rendición de cuentas y más probabilidades de que este trabaje para el bien común (Prat 2006, p. 91). La transparencia, por tanto, contribuye a la rendición de cuentas en tanto en cuanto permite esta observación.

Ambas ideas se sustentan en la existencia de información y documentación para poder llevarse a cabo y, por este motivo, se relacionan de manera directa con una adecuada gestión documental. La importancia de los documentos para la rendición de cuentas ha llegado a la atención pública como resultado de escándalos de gobiernos, fraudes corporativos, degradación de estándares éticos y casos de corrupción (Iacovin, 2010, p. 181). Aun así, no debe relacionarse tan solo con este tipo de resultados, puesto que la gestión documental proporciona también información para procesos de rendición de cuentas en que las organizaciones han desarrollado sus actividades de manera correcta, aportando beneficios a la sociedad.

Por tanto, más allá de las visiones negativas asociadas a la rendición de cuentas y al auge de la transparencia, ambas deben entenderse como parte del funcionamiento normal de las administraciones públicas y, consecuentemente, en muchos casos sin mayor transcendencia noticiable.

3.1 Transparencia

El término “transparencia” ha alcanzado un significado casi religioso en el debate sobre la gobernanza y el diseño institucional (Hood 2006b, p. 3) y muchas son las definiciones que de él pueden encontrarse en la bibliografía. Al-

gunas de las utilizadas por organizaciones internacionales de amplio recorrido y reconocimiento, como la OCDE⁴³, apuntan hacia una visión amplia del término, entendido como el resultado de una vía de comunicación de dos direcciones entre gobiernos y otras partes interesadas, definición que también defienden Bellver y Kaufmann (Bellver y Kaufmann, 2005).

Una visión más pragmática se refiere a la transparencia como el aumento del flujo de información oportuna y fiable, económica, social y política, que es accesible para todas las partes interesadas pertinentes (Bellver y Kaufmann 2005, p. 4). Yendo más allá, y según Meijer, la transparencia se corresponde con la disponibilidad de información sobre un actor, permitiendo a los actores externos monitorizar las acciones y decisiones de ese actor (Meijer 2013, p. 430), en una clara alusión a los procesos de rendición de cuentas. Esta disponibilidad no solo es a través de documentos, sino que Meijer incluye el acceso a reuniones o publicaciones de las grabaciones de dichas reuniones. Se destaca la mención, en esta última definición, a la rendición de cuentas a través de la transparencia, ya que la transparencia no puede dissociarse de uno de sus objetivos más importantes como es el de rendir de cuentas ante los ciudadanos y ante las diferentes partes interesadas. No tiene como fin satisfacer la curiosidad de cualquier individuo, sino que está al servicio del interés general.

El paradigma dominante para entender la transparencia prioriza el concepto de la obligatoriedad de desclasificar (Bruno 2015, p. 5). La transparencia significa apertura o desclasificación activa, lo que en inglés se conoce como *active disclosure*. Esto implica que los gobiernos no solamente deben permitir que los ciudadanos los observen, sino que deben divulgar activamente la información y los documentos que poseen (Aguilar Rivera 2008, p. 8). Esta divulgación y publicación de documentos tiene como finalidad, entre otras, la evaluación de los gobernantes, la rendición de cuentas, el control del poder político e indirectamente la prevención de la corrupción. El simple hecho de saber que existe la posibilidad de un control directo de los ciudadanos, incita a las autoridades a actuar con prudencia y circunspección (Condeso 2011, p. 88).

Para ello, la transparencia debe cumplir con unos principios mínimos (Schnackenberg 2009, p. 14), que determinan el grado real de transparencia y que se relacionan entre sí (ver Figura 11):

- La desclasificación (*disclosure*) o apertura: por ejemplo, la cantidad de información presentada y a qué nivel se encuentra disponible.
- La claridad (*clarity*) de la información: por ejemplo, el grado en que se permite su comprensión mediante el contexto, la coherencia lingüística, el ruido en los datos aportados y la relevancia.
- La precisión (*accuracy*) de la información: por ejemplo, el grado en que dicha información se asemeja a lo que se percibe por parte de quien la desclasifica.

⁴³ – Fundada en 1961, la Organización para la Cooperación y el Desarrollo Económicos (OCDE) agrupa a 36 países miembros y su misión es promover políticas que mejoren el bienestar económico y social de las personas alrededor del mundo. La OCDE ofrece un foro donde los gobiernos puedan trabajar conjuntamente para compartir experiencias y buscar soluciones a los problemas comunes.

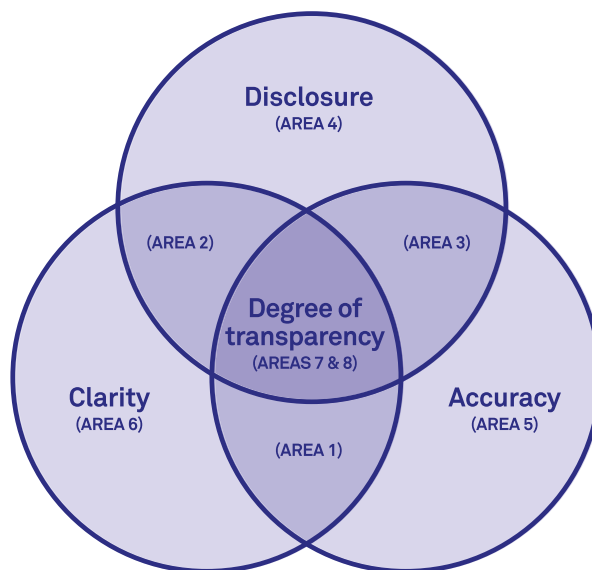


Figura 11 - Modelo conceptual de la transparencia según Schnackenberg.

Según el modelo de Schnackenberg, la desclasificación suele referirse a la cantidad de información, así como a su disponibilidad para las diferentes partes interesadas. Con relación a este aspecto, la calidad es un elemento claramente diferenciado de la cantidad, puesto que, por muchos documentos que se hagan públicos, si estos no son confiables la desclasificación perderá su valor. La precisión se define como el grado en que la información que los remitentes pretenden hacer pública es congruente con lo que ellos perciben que es preciso. Así, el análisis no se realiza a posteriori, sino que requiere de una comprobación por parte de los funcionarios antes de la publicación de la información, de acuerdo a sus percepciones de aquello que es válido y lo que no. Respecto a la claridad, es quizás el concepto más complejo o subjetivo, ya que implica la percepción, la habilidad y la capacidad de interpretación de quien recibe la información, junto con sus circunstancias concretas.

Junto a estas tres premisas se encuentra la de la relevancia de la información que se publica o desclasifica. Esta cuestión está íntimamente relacionada con la claridad y la precisión de la información y muchas veces se olvida, cuando se pretende que la publicación consista en un proceso unidireccional. Como ya se ha visto en algunas de las definiciones de la transparencia, esta debe ser un proceso bidireccional para poder resultar realmente efectivo. Cuando la información se hace pública, de manera precisa y clara, puede considerarse un proceso con un alto grado de transparencia (Schnackenberg 2009, p. 20). De este modo, puede cumplir con sus funciones, proporcionando beneficios a las sociedades democráticas, como son la evaluación de los gobernantes, la rendición de cuentas, el control del poder político, la participación de los ciudadanos, la prevención de la corrupción y, por ende, al buen gobierno.

La transparencia potencia la eficacia, la racionalidad y la calidad de la prestación de los servicios públicos, y permite a los ciudadanos supervisar a las autoridades públicas para prevenir o denunciar decisiones ilegales, arbitrarias, parciales, inoportunas, corruptoras (Condesso 2011, p. 93). Además, incentiva la participación de los ciudadanos, contribuyendo a la formación de la opinión pública, tal y como ya preconizaba Bentham, al proporcionar medios para el debate sobre las decisiones y opciones políticas y administrativas. Se asegura, de este modo, mantener a los ciudadanos informados sobre las leyes y decisiones que les afectan, asegurando también su acceso a la información necesaria para poder participar en el proceso de toma de decisiones (Darbshire 2010, p. 3). La transparencia, además, refuerza

la legitimidad de la administración pública, al permitir visibilizar con normalidad cómo funcionan los servicios públicos y poder controlar sus actuaciones y el desempeño de sus funciones. Este control se efectúa también a través de la vigilancia y la fiscalización de las acciones de los políticos y funcionarios, es decir, de la rendición de cuentas pública. A través de la transparencia la ciudadanía puede detectar los fallos y defectos de las políticas públicas en sus primeras etapas, cuando todavía pueden corregirse (Aguilar Rivera 2008, p. 30).

No solo hay aspectos positivos para los ciudadanos o usuarios de la administración, sino que, desde el punto de vista de los funcionarios, la transparencia y la publicación activa de información reduce y facilita sus tareas disminuyendo el número de solicitudes de información y simplificando el procedimiento administrativo en algunos casos. Un beneficio extra de una transparencia activa es que se promueve una mejor gestión de los documentos por parte de la administración, con el fin de optimizar los flujos internos de información, así como para poder dar una mejor y más rápida respuesta a las solicitudes de acceso a la información o a las desclasificaciones y publicaciones. Disponer de la información de acceso público contribuye, además, a su reutilización y a la creación o aumento de la actividad empresarial a partir de ella, aportando un valor añadido de inestimable valor para la sociedad.

No hay que olvidar la importancia de la rendición de cuentas asociada a la transparencia, que funciona de manera capacitadora del poder ciudadano, así como de inhibidora de conductas y acciones que atenten contra el interés público (Aguilar Rivera 2008, p. 29), es decir, como medida de prevención de la corrupción. La transparencia puede contribuir a la rendición de cuentas del gobierno de manera directa, por ejemplo reduciendo el riesgo de que los errores pasen inadvertidos o también, mostrando los objetivos de manera explícita para que, de este modo, no haya lugar a confusión dentro del propio gobierno (Hood 2010, p. 992).

3.1.1 El principio de publicidad

Las medidas actuales más importantes sobre transparencia, como la apertura de los archivos, las sesiones públicas de los organismos representativos y la publicación de documentos del gobierno, pueden rastrearse hasta las ideas sobre apertura de Jeremy Bentham (1748-1832)⁴⁴. Estas medidas se han convertido en requisitos básicos de los gobiernos democráticos (Meijer 2014, p. 507).

Sin embargo, previamente se encuentra esta noción en filósofos como John Locke (1632-1704) e Immanuel Kant (1724-1804). Por ejemplo, en los tratados de John Locke se afirma que el poder político solo se puede comprender si se deriva de su origen, de aquel Estado en que todos los hombres se encuentran por naturaleza (...) libremente, dotados de las mismas ventajas y por lo tanto, depositarios de los mismos derechos, derechos que le otorguen el poder tener vista de cómo proceden las cosas del Estado (Rodríguez Zepeda 2008, p. 5). Por su parte, Kant en el segundo apéndice

⁴⁴– Jeremy Bentham fue un filósofo, economista y pensador británico. Se le considera el padre del utilitarismo, una teoría y doctrina ética que establece que la mejor acción es la que maximiza la utilidad, entendida esta de manera general como el bienestar de los seres humanos.

a su obra *La paz perpetua*, “Del acuerdo entre la política y la moral según el concepto trascendental del derecho público”, afirma que son injustas todas las acciones referidas al derecho de otros hombres, cuyos principios no soporten ser publicados (Kant 2013, p. 75). Argumenta que sin la publicidad no habría justicia, pues la justicia solo puede pensarse como *manifestada públicamente*, ni habría tampoco derecho, pues este solo se otorga desde la justicia. Es por ello que, según Kant, toda pretensión jurídica debe poseer la posibilidad de ser hecha pública.

Bentham, por su parte, entiende el principio de publicidad como un mecanismo para hacer que el interés personal de los funcionarios coincida con el interés general sin que sea necesario vincularlo a la moral (Cruz Revueltas 2009, p. 24). Bentham identifica, en su libro *Tácticas parlamentarias*, cuatro razones justificativas o beneficios de la publicidad en los gobiernos, así como una serie de argumentos para rebatir las objeciones a la publicidad que existían en la época, y que se exponen a continuación. Aunque el autor tenía en mente la información de las asambleas legislativas, su argumento puede, como él mismo sugirió, extenderse a otras informaciones gubernamentales.

El primer beneficio de la publicidad es el de contener a los miembros de la asamblea dentro de su obligación, mediante la vigilancia del público (Bentham 2002, p. 84). Según Bentham, el cuerpo del público forma un tribunal, y uno que vale más que todos los otros juntos. Dentro de este razonamiento, identifica a tres enemigos de la publicidad que, en sus palabras, son: los malhechores, que quieren ocultarse de las miradas de su juez; el tirano, que intenta ahogar la opinión pública; y el hombre tímido o indolente, que censura la incapacidad general para encubrir la suya (Bentham 2002, p. 84).

El segundo beneficio de la publicidad es el de asegurar la confianza del pueblo y su consentimiento en las resoluciones legislativas. Para Bentham, el mejor proyecto, preparado en el secretismo, causará mayor espanto en ciertas circunstancias que el peor proyecto bajo la mayor publicidad. Recomienda al gobierno no hacer nada sin que lo sepa la nación, ya que el público le devuelve de manera duplicada la confianza que él manifiesta (Bentham 2002, p. 85). El autor no niega que en ocasiones el secretismo aleje los inconvenientes, pero afirma que a la larga estos vuelven en mayor número.

El tercer beneficio de la publicidad es el de proporcionar a los electores la facultad de obrar con conocimiento de causa. Bentham afirma que ocultar al público la conducta de sus mandatarios es agregar la inconsecuencia a la prevaricación⁴⁵ (Bentham 2002, p. 89).

El cuarto beneficio de la publicidad es el de proporcionar a la asamblea la facultad de aprovecharse de las luces (las ideas o el conocimiento) del público. Para Bentham, los hombres que cultivan su inteligencia tienen, rara vez, los medios para entrar en la carrera política, perdiéndose así grandes pensadores (cita a Locke, Newton, Hume y Adam Smith) y grandes ideas. Para él, mediante la publicidad podrían recogerse todas las luces de una nación y hacer resurgir pensamientos útiles (Bentham 2002, p. 90).

⁴⁵ – La prevaricación es el delito consistente en que una autoridad, un juez, o un funcionario, dicte a sabiendas una resolución injusta.

Además de la identificación de estos beneficios, Bentham también identifica y analiza una serie de objeciones a la publicidad, con el fin de proteger a los gobernantes de las injusticias del público y recompensarles por sus tareas. Para rebatir cada una de estas objeciones presenta una serie de argumentos que se explican a continuación.

La primera objeción a la publicidad consiste en que el público es un juez incompetente de las operaciones de una asamblea política, en razón de la ignorancia y las pasiones de la mayoría de los que lo componen (Bentham 2002, p. 91). Bentham argumenta que se puede afirmar que la publicación de documentos aumenta el número de los malos jueces en una proporción muy superior a la de los buenos. Para desarrollar su contraargumento explica que existen tres tipos de público: la parte más numerosa, que se ocupa muy poco de los asuntos públicos y que no dedica el tiempo a leer; la formada por los que hacen una especie de juicio basado en la palabra de otras personas, sin tomarse la molestia de formarse una opinión propia; y la parte compuesta por los que juzgan por sí mismos con relación a los informes y documentos que se les han proporcionado gracias a la publicidad. Según el autor, la publicidad solo puede perjudicar a la segunda parte, ya que la primera no juzga y la tercera lo hace antes de la publicidad y también con ella, aunque juzga mal debido a los informes poco puntuales y documentos poco precisos. Si se instruye mejor a esta última clase, con una mejora de las fuentes de información, se conseguirá que esta pueda juzgar con más criterio y que, indirectamente, la segunda clase que parte de los comentarios de otras personas, pueda recibir informaciones más exactas. Según este contraargumento, en realidad, la publicidad podría perjudicar únicamente a la clase que juzga, porque ella arrastra la opinión de las restantes. Pero si esta clase juzga mal, según Bentham, es debido a que ignora los hechos o no posee la información necesaria para poder formarse un buen juicio (Bentham 2002, p. 92). Por tanto, la objeción inicial queda rebatida.

La segunda objeción a la publicidad es que esta puede exponer al odio público a un miembro de la asamblea por actos que son por ventura dignos de la gratitud nacional. Esta objeción se relaciona claramente con la primera, ya que parte de un juicio equivocado de la información recibida. El contraargumento de Bentham es que la publicidad, bajo el aspecto de reputación, es mucho más útil que perjudicial para los miembros de la asamblea (Bentham 2002, p. 93), ya que les protege frente a las calumnias y no permite que se les atribuyan discursos falsos o disimular el bien que han hecho.

La tercera objeción a la publicidad es que el deseo de popularidad puede sugerir proposiciones peligrosas a algunos miembros de la asamblea. De nuevo entra en juego el juicio del público, aunque Bentham rebate que en realidad la publicidad de los debates ha arruinado más que beneficiado a los demagogos (Bentham 2002, p. 94) y que el deseo de una momentánea popularidad no produce más que ridiculez.

La cuarta objeción afirma que, en un estado monárquico, exponer la publicidad de las asambleas de los miembros al resentimiento del jefe del estado, puede perjudicar a la libertad de sus decisiones (Bentham 2002, p. 94). Bentham argumenta que, si para la asamblea existe algún peligro por parte del jefe del estado, no hay ninguna salvaguarda más que en la protección de la opinión pública y, afirma, que sería tan solo un pretexto argumentar que se necesita llevar a cabo la toma de decisiones en secreto para liberarse de la supervisión del jefe del estado. A través de la publicidad y del debate público, la relación entre el gobierno y la sociedad se vuelve menos vertical y más cooperativa, más dinámica y creadora de nuevas alternativas, puesto que se funda en una mayor circulación y calidad de la información y de la comunicación (Cruz Revueltas 2009, p. 32).

Sin embargo, pese a todos estos argumentos, Bentham era consciente de que la publicidad no es un valor absoluto y de que existen excepciones. No puede hacerse una ley absoluta de la publicidad porque es imposible prever todas las circunstancias en que una asamblea puede hallarse (Bentham 2002, p. 98).

Bentham ya advertía de los peligros de la inexacta o insuficiente información en la publicidad, haciendo hincapié en la necesidad y la obligación de publicar documentos y hacer pública la información con la que trabaja el gobierno. Sin embargo, una sociedad con un pleno derecho a la información no puede construirse solo sobre la base de la transparencia del gobierno. También es necesario pensar este derecho en términos de educación e ilustración de los ciudadanos, que son condiciones que permiten a estos actuar como sujetos autónomos, informados y con sentido crítico (Rodríguez Zepeda 2008, p. 11).

En la actualidad, es comúnmente aceptado el hecho de que se vive una era especial de la transparencia donde, en las últimas décadas, ha aumentado de manera abrupta su importancia como un principio de la política y del diseño institucional (Hood 2006a, p. 211). Sin embargo, pese a que estas ideas son anteriores al siglo XX, es difícil identificar alguna línea de continuidad institucional desde ellas hasta la actualidad y, de este modo, la transparencia parece más una idea reinventada tras haber sido olvidada, como también ocurre con otras ideas de Bentham (Hood 2006b, p. 19). Se remarca la idea de reinención, puesto que ni la palabra ni las doctrinas clave de la transparencia se inventaron en el siglo XX (Hood 2006b, p. 11).

Según Hood, en la mayoría de países occidentales la transparencia, probablemente, ha disminuido en lugar de haber aumentado en los últimos treinta años. La puesta en marcha de la legislación sobre privacidad y protección de datos siempre ha ido un paso por delante de los requisitos para la desclasificación de información de las organizaciones. Más allá, con la externalización de funciones por parte de los estados, la información sobre el desarrollo de las actividades y de algunos servicios en muchas circunstancias permite blindarse detrás de una capa de confidencialidad comercial. De hecho, esa información puede no estar disponible ni siquiera para la administración, puesto que la implementación de *software* y de diferentes programas informáticos se puede hacer mediante código propietario (Hood, 2006a, p. 213). A esto hay que añadir que muchas leyes no reconocen el derecho de acceso a documentos conservados por empresas contratadas. Algunos gobiernos han negociado contratos que contienen cláusulas de confidencialidad pensadas para prevenir la desclasificación de dichos contratos (Roberts 2006, p. 117).

Este es uno de los ejemplos más claros con relación a la situación de la transparencia en la actualidad. La transparencia no es fácil, no es una “condición natural” de las organizaciones gubernamentales. Por eso, la transparencia debe elaborarse, construirse, implementarse cuidadosamente, con una visión de largo plazo que asuma al mismo tiempo diferentes objetivos: legales, reglamentarios, políticos, organizacionales, educativos, culturales, dentro y fuera de las instituciones del Estado (Vergara 2008, p. 5).

A continuación, se explican distintos tipos de transparencia que se dan en la actualidad con la finalidad de contextualizar estas ideas.

3.1.2 Tipos de transparencia

Se distinguen distintos tipos de transparencia en función de la visión desde la que se estudie. En este apartado se hace un recorrido por ellos.

En la categorización de la transparencia, Heald diferencia entre cuatro tipos distintos (Heald 2006, p. 27). Esta distinción distingue dos direcciones, dentro de las cuales se enmarcan dos posibilidades. Presenta estos tipos mediante un diagrama de Venn (ver Figura 12), mostrando, a su vez, las diferentes interrelaciones que se producen al combinar la transparencia en diversas direcciones. Esto da como resultado dos grandes tipos de transparencia: vertical y horizontal, que se explican a continuación.

La transparencia vertical puede incluir (Heald 2006, p. 27):

- Transparencia hacia arriba (*upwards - U*): se da cuando el superior jerárquico puede observar la conducta, comportamiento y/o resultados del subordinado jerárquicamente.
- Transparencia hacia abajo (*downwards - D*): se da cuando el gobernado puede observar la conducta, comportamiento y/o resultados de sus gobernantes. El derecho de los gobernados en relación con sus gobernantes aparece en la teoría y práctica democráticas, a menudo como el paraguas de la rendición de cuentas (Heald 2006, p. 27).

Mientras coexistan la transparencia hacia arriba y hacia abajo, existirá una transparencia vertical simétrica o recíproca que, en caso contrario, quedaría ausente o sería asimétrica.

La transparencia horizontal puede incluir (Heald 2006, p. 28):

- Transparencia hacia el exterior (*outwards - O*): se da cuando desde la organización se puede observar qué pasa fuera de la misma. Es fundamental para cualquier organización ser capaz de entender el contexto en el que se encuentra.
- Transparencia hacia el interior (*inwards - I*): se da cuando desde el exterior se puede observar lo que ocurre dentro de la organización. Este tipo de transparencia es relevante para la rendición de cuentas, así como en el desarrollo de la legislación del derecho de acceso a la información.

La transparencia horizontal evoca la posibilidad de ver desde fuera qué sucede dentro, permitiendo, además, que desde dentro se tenga la percepción del mundo exterior, perspectiva indispensable para que los gobernantes puedan orientar su acción hacia el interés general (Oficina Antifrau de Catalunya 2013, p. 91). Cuando exista transparencia en estas dos direcciones, existirá una relación horizontal recíproca o simétrica, en caso contrario, esta relación quedaría ausente o sería asimétrica.

La explicación de las relaciones entre la direccionalidad de la transparencia se puede ver claramente en el gráfico que presenta Heald (Heald 2006, p. 28), mediante la representación de los conceptos en un diagrama de Venn (ver Figura 12).

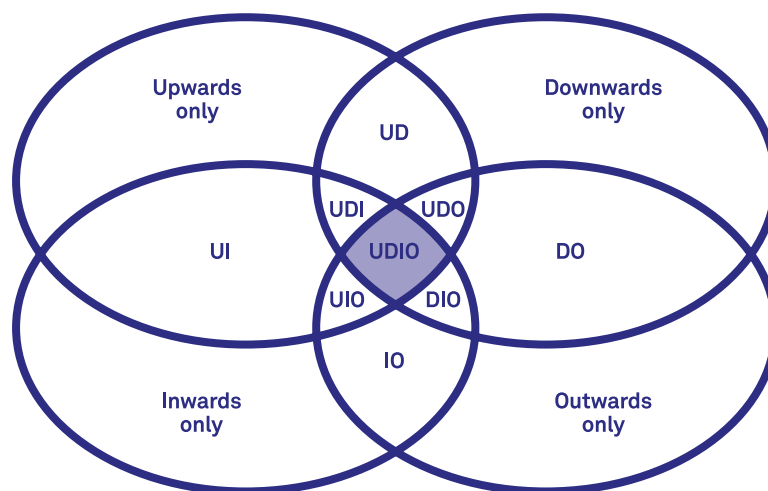


Figura 12. Diagrama de Venn – Cuatro direcciones de la transparencia.

El área central, en color azul, indica la presencia de las cuatro direcciones de la transparencia de manera simultánea, transparencia totalmente simétrica (Heald 2006, p. 29), una situación que podría considerarse utópica, pero ideal.

Aparte de la direccionalidad, Heald también distingue entre diferentes clases de transparencia analizadas desde el punto de vista de tres dicotomías (Heald 2006, p. 29). Estas son⁴⁶: la transparencia de un hecho o de un acontecimiento frente a la transparencia de un proceso (en inglés, *event versus process transparency*); la transparencia retroactiva frente a la transparencia en tiempo real (en inglés, *transparency in retrospect versus transparency in real time*); y la transparencia aparente frente a la efectiva (en inglés, *nominal versus effective transparency*).

En relación con la transparencia del hecho o acontecimiento frente a la transparencia del proceso, los hechos representan momentos que son visibles externamente y, en principio, medibles. Según Heald, y en referencia a la administración pública, se puede distinguir, en este marco, entre entradas (*inputs*), salidas (*outputs*) y resultados (*outcomes*) como tres entidades dentro del concepto del hecho o acontecimiento. Estas tres entidades se enlazan mediante procesos, que se llevan a cabo para convertir las entradas en salidas y las salidas en resultados. Los procesos son más difíciles de medir que los hechos, aunque pueden ser descritos si la información sobre ellos está disponible. De esta diferenciación pueden deducirse dos aspectos importantes. Por un lado, una metodología distinta a la hora de hacer

⁴⁶ – Las dicotomías se han traducido del inglés por la autora.

pública la información sobre un hecho o sobre un proceso, ya que la segunda necesitará de información adicional (como la explicación del proceso) para que el receptor sea capaz de entenderlo y se necesitará un modo de enlazar ambas informaciones (hechos y procesos relacionados) para poder ser transparentes de un modo realmente comprensible. Por otro lado, existirán unas necesidades de medición distintas en función de si estas se refieren a la definición del proceso, al desarrollo del proceso en un caso concreto, a los resultados, las entradas o las salidas.

En relación con la transparencia retroactiva frente a la transparencia en tiempo real, la primera permite a las organizaciones desarrollar sus actividades y, a intervalos periódicos, desclasificar y hacer pública información relevante sobre su rendimiento. Por el contrario, la transparencia en tiempo real implica que los procesos internos de la organización son continuamente susceptibles de hacerse públicos. El contraste se da entre un ciclo de publicaciones de información que caracteriza la transparencia retroactiva y la vigilancia o supervisión continua que caracteriza la transparencia en tiempo real.

En relación con la transparencia aparente frente a la transparencia efectiva, Heald afirma que puede haber divergencias entre estos dos tipos. La brecha o diferencia entre ambas se conoce como la “ilusión de la transparencia”, incluso cuando parece que la transparencia se incrementa, al medirla se hace patente que la realidad es bien diferente. Esto no solo depende de las políticas de desclasificación, sino que también se deben tener en cuenta otros factores para que la transparencia sea realmente efectiva, como, por ejemplo, que existan receptores capaces de procesar, asimilar y utilizar la información. Otra de las premisas para conseguir este objetivo es disponer de sistemas de gestión documental, ya que sin una estructuración de la información será muy difícil recuperarla y, consecuentemente, hacerla pública conllevará demoras importantes e incluso fracasos.

Otra distinción de categorías de transparencia, la clasifica en tres tipos (Oficina Antifrau de Catalunya 2013, p. 91): clásica, colaborativa y orientada.

La transparencia clásica deriva del derecho de todo ciudadano a conocer el funcionamiento de las instituciones. El acceso ciudadano oportuno, suficiente y garantizado a información relativa al desempeño de las funciones públicas (Aguilar Rivera 2008, p. 11), relacionada totalmente con la rendición de cuentas.

La transparencia colaborativa implica que los ciudadanos actúan como proveedores de información en una relación de carácter bidireccional. Otros autores (Cerrillo-i-Martínez, 2012) definen este tipo de transparencia como la que permite reutilizar la información que se hace accesible por ciudadanos u organizaciones, ya sea con fines comerciales o no.

En el caso de la transparencia orientada a la difusión de información, se convierte en un instrumento político con la finalidad de prevenir riesgos de corrupción y de mejorar los servicios públicos. Se conoce también como transparencia preventiva.

Es interesante la inclusión de la transparencia colaborativa, entendiendo que ya no solo depende de los gobiernos o la administración, sino también de la ciudadanía, desde la perspectiva de que esta pueda proveer de información al estado. En contraste con otros tipos de transparencia, existe una colaboración más estrecha entre quienes diseñan las políticas de transparencia y sus usuarios. Los ciudadanos, que tradicionalmente han sido los usuarios de la información, pueden convertirse, gracias a las nuevas tecnologías, en fuentes de información para el Estado (Fung, Graham,

y Weil 2007, p. 152). Bautizada como la tercera generación de la transparencia, según Fung, Graham y Weil, esta se diferencia de la transparencia clásica o de la orientada en que, a través de las nuevas tecnologías de la información y la comunicación, se empoderará a los mismos usuarios de dicha información para que provean y compartan muchos de los datos esenciales. Además, los medios de acceso a los datos serán mucho más interactivos y personalizados, y podrán ser revisados a un ritmo mucho más acelerado (Fung *et al.* 2007, p. 152).

Otra clasificación posible queda definida por la Oficina Antifraude de Cataluña en su informe del año 2014 sobre el “Derecho de acceso a la información pública y transparencia”, identificando dos tipos de transparencia, que no anulan a los otros tipos ya explicados. Estos son: activa y pasiva.

La transparencia activa se refiere a toda aquella información que los poderes públicos ponen a disposición de la ciudadanía sin una petición previa. Este tipo de transparencia constituye la dimensión objetiva del derecho en tanto que implica una determinada concepción de la relación de la Administración con los ciudadanos. También llamada por otros autores como transparencia o desclasificación proactiva (Darbishire, 2010).

La transparencia pasiva se da cuando una persona solicita el acceso a determinada información y la Administración tiene el deber de facilitarla. Constituye la dimensión subjetiva del derecho de acceso a la información pública. Es lo que se conoce como derecho de acceso a la información pública propiamente y que algunos autores diferencian del concepto de transparencia (Aguilar Rivera, 2008).

Estos dos tipos de transparencia se basan tanto en el grado en que los gobiernos publican información, como el grado en que los ciudadanos pueden solicitar y recibir información no publicada. Es importante considerar que la información proporcionada no debe ser solo accesible, sino también relevante, de buena calidad y fiable (Bellver y Kaufmann 2005, p. 4). Para que esto sea así, la gestión documental debe incluirse en las políticas de transparencia de las organizaciones, por ser la única garante de que estas conserven y sean capaces de gestionar información y documentación fiable, auténtica, íntegra y usable. El ejercicio del poder político es, entre otras cosas, una forma de distribución de recursos de distinta índole. Algunos de los recursos que de manera privilegiada distribuye el poder político son la información y el conocimiento (Rodríguez Zepeda 2008, p. 16).

Otra distinción interesante incluye diferentes aspectos de la transparencia que también deben tenerse en cuenta al estudiarla (Meijer 2013, p. 430) y que pueden relacionarse de manera directa con los procesos de rendición de cuentas. Meijer entiende la transparencia de tres modos distintos: como una relación institucional, como un intercambio de información o como la transparencia del trabajo y del desempeño.

Entendida como una relación institucional, un actor sería objeto de la transparencia en el sentido de que puede ser monitorizado, mientras el otro actor sería el sujeto de la transparencia monitorizando al primero. La relación puede analizarse en materia de normas, interacciones, poder u otros. Se aprecia claramente la relación con los procesos de rendición de cuentas, en tanto en cuanto existe un actor (A) y un foro o principal (P) a quien A debe dar explicaciones.

Entendida como un intercambio de información, la transparencia es como una representación de la realidad: decisiones, acciones y otras circunstancias relevantes que se documentan de diferentes maneras. Estos documentos

forman la base de una subsecuente reconstrucción de esas decisiones, acciones y circunstancias relevantes, ya que fueron creados con unos objetivos específicos.

Con relación a la transparencia del trabajo y del desempeño del mismo, esta se refiere también a aspectos relacionados con la organización del gobierno, como acciones, decisiones, circunstancias relevantes o responsabilidades. Meijer relaciona directamente este aspecto con la idea de Heald sobre la transparencia del proceso y del acontecimiento, afirmando que ambos deben ser transparentes y accesibles a los ciudadanos.

3.2 Rendición de cuentas

La rendición de cuentas pública⁴⁷ es el sello de calidad del gobierno democrático (Bovens 2005, p. 182), por tanto, debe ser un valor central de la democracia y uno de los principios básicos del buen gobierno (Nonell 2006, p. 17). Pese a que el término en inglés aparece durante los inicios del siglo XVII, permanece culturalmente inocuo hasta las décadas de 1960 y 1970, cuando se aprecia una recuperación aguda y creciente de su uso, el cual continúa hasta el siglo XXI (Bovens, M; Schillemans, T.; Goodin 2016, p. 1). En este sentido, se puede apreciar un cierto paralelismo con el término de transparencia, explicado en apartados anteriores.

Denota, de un modo general, el deber de un individuo u organización de responder de alguna manera sobre cómo ha desempeñado sus obligaciones, sus actos, omisiones, decisiones, políticas y gastos. Cualquier acto o actividad del gobierno es, en un análisis final, una actividad de los ciudadanos en tanto que los representan y esto requiere de una estructura diseñada cuidadosamente para la rendición de cuentas que asegure, para los ciudadanos, los mejores esfuerzos de aquellos que actúan en su representación (Hughes 2012, p. 186). Todos los centros de decisión que se configuran, tanto en la órbita del Estado como en la sociedad, afectan a la vida de los ciudadanos. Dentro de estos, hay que incluir tanto al gobierno como a la administración pública, la defensa, la seguridad, la justicia, la formación escolar y universitaria y la investigación pública, así como todos aquellos organismos independientes que regulan los mercados (Nonell 2006, p. 19).

La rendición de cuentas es un requisito previo esencial para el funcionamiento del proceso democrático, ya que proporciona a los ciudadanos y a sus representantes la información necesaria para juzgar la conducta del gobierno (Bovens, M; Schillemans, T.; Goodin 2016, p. 14). Se debe tener en consideración que el término puede tener diferentes definiciones según los autores consultados, si bien es cierto que siempre tendrá un significado dual: por un lado, se trata de enumerar y contar “cosas” importantes (posesiones, acuerdos, deudas, promesas) y, por otro lado, se trata de proporcionar un informe acerca de este recuento. Esto conlleva la explicación de una historia, basada en ciertas obligaciones y con algunas consecuencias previsibles.

⁴⁷– Cuando aparezca, a lo largo de este u otros apartados, la expresión “rendición de cuentas” siempre se está refiriendo a la rendición de cuentas pública, de administraciones públicas de cualquier tipo.

La rendición de cuentas incluye proporcionar explicaciones. Esto se refiere a la capacidad de respuesta hacia quienes tienen la legitimidad de realizar las preguntas y de exigir la rendición de cuentas (Bovens, M; Schillemans, T.; Goodin 2016, p. 6). La palabra original de este concepto en inglés es *accountability* (*public accountability*), término que no tiene un equivalente en castellano y que se puede encontrar traducido por control, fiscalización o responsabilidad. Ser responsable no comunica lo que significa rendir cuentas, responder, obligarse y otros términos. Los sinónimos normalmente son más similares que equivalentes y este vacío (la diferencia) puede resultar en malentendidos, no solo sobre idiomas, sino también sobre contextos (Dubnick 2016, p. 26). La traducción más cercana al significado original es rendición de cuentas. Pese a que, normalmente, se traducen como iguales, ambos términos tienen matices que separan los dos conceptos. Mientras *accountability* conlleva un sentido claro de obligación, la noción de rendición de cuentas se relaciona más con la voluntariedad, con una condición generosa del soberano que rinde cuentas por voluntad propia y no por necesidad. De este modo, puede precisarse que *accountability* es la rendición obligatoria de cuentas (Schedler 2008, p. 11). En esta investigación se utiliza el término “rendición de cuentas” como traducción exacta del término *accountability*, con la connotación de obligatoriedad incluida.

La rendición de cuentas implica, por tanto, que una persona debe seguir las normas o reglas estipuladas y alcanzar los objetivos preestablecidos; de otra manera, será castigada (Lewin 2007, p. 3). La idea es que dichas personas rindan cuentas tanto de sus acciones como de sus omisiones, convirtiéndose la rendición de cuentas en una actividad retrospectiva (Bovens, M; Schillemans, T.; Goodin 2016, p. 6). Para ello es necesario disponer de unos estándares de conducta, evaluaciones sobre el rendimiento, así como determinar quién puede quedar exento. La rendición de cuentas funciona mejor cuando se pueden identificar unas mínimas condiciones sobre buena conducta y rendimiento, como, por ejemplo, cuando alguien incumple la ley o suspende una evaluación (Lewin 2007, p. 4).

A menudo, en el discurso político, se utiliza el término rendición de cuentas como una promesa de un gobierno justo y equitativo. Este concepto se usa como sinónimo para muchos deseos políticos, como la promesa de igualdad y justicia, de aprendizaje y mejora, de transparencia y democracia, o de integridad y ética. El término, utilizado como una herramienta retórica por los políticos, se ha convertido en una especie de icono del buen gobierno (Bovens 2005, p. 184). Sin embargo, pese a que este término ha formado parte del paradigma de la gobernanza moderna desde hace aproximadamente un milenio, ha sido ahora cuando se ha convertido en la manifestación icónica del buen gobierno (Dubnick 2016, p. 24).

La crisis de confianza en las administraciones públicas, la reducción de la participación ciudadana en los procesos democráticos y la apatía hacia la política de finales del siglo XX en las democracias occidentales han dado origen a la búsqueda de nuevas relaciones entre Administración y ciudadanía para promover un diálogo más activo y una mayor participación en la formulación de las políticas públicas, con el fin último de incrementar la confianza de los ciudadanos en las instituciones públicas (Royo Montanés 2008, p. 33).

La rendición de cuentas se define, finalmente, como una relación en la cual un actor siente o tiene la obligación de explicar y justificar su conducta frente a otro actor o foro, que puede plantear cuestiones y emitir juicios sobre dicha conducta. Esta relación, en principio sencilla, contiene un número de variables a tener en cuenta. El actor, o quien rinde cuentas, puede ser una persona o un organismo; el foro, o a quien se debe rendir cuentas, puede ser la ciudadanía en general, un individuo, un político, un gestor público, una institución (como el parlamento), entre otros; la obligación puede ser formal (por ejemplo, frente a una comisión parlamentaria) o informal (por ejemplo, una rueda de prensa); y las preguntas y juicios pueden llevar asociadas consecuencias, que pueden ser positivas o negativas (Hughes 2012, p. 187).

La práctica de la rendición de cuentas se puede considerar, por tanto, como un conjunto de relaciones sociales (Bovens 2005, p. 184). Más en detalle, tal y como explica Bovens, esta relación contiene cinco elementos (Bovens 2005, p. 185):

1. Acceso público al hecho por el que se rinde cuentas, no solo internamente.
2. Explicación y justificación de su conducta, no de manera propagandística o con la provisión de información o instrucciones al público en general.
3. La explicación debe dirigirse al foro específico y no darse de manera aleatoria.
4. El actor debe sentirse obligado a ponerse a disposición, en lugar de tener la libertad de no rendir cuentas en absoluto.
5. Debe existir la posibilidad para el debate y el juicio, incluyendo la imposición opcional (o informal) de sanciones por el foro, para que el proceso no se convierta en un monólogo sin compromiso.

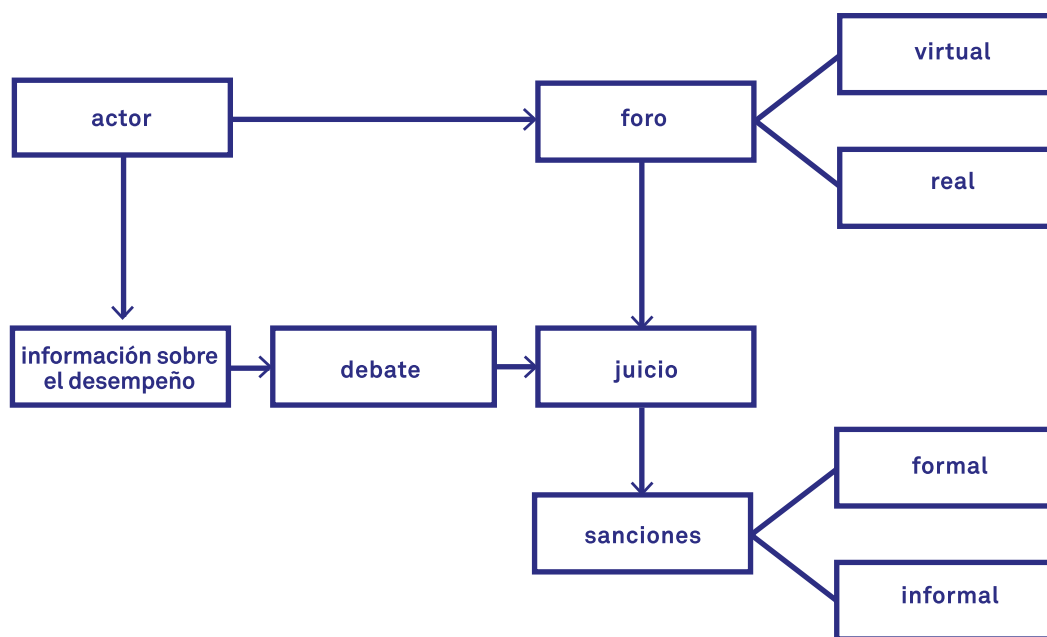


Figura 13. Proceso de rendición de cuentas pública según Bovens (Bovens 2005, p. 186).

La Figura 13 refleja el proceso de rendición de cuentas de manera detallada. Existe un actor, que debe rendir cuentas frente a un foro. La manera en que puede hacerlo es a través de datos, información y documentos sobre sus actuaciones, decisiones, resultados y el desempeño de sus obligaciones. Esta información pasa a ser debatida por el foro, que deberá juzgarla y tomar decisiones al respecto. Estas decisiones pueden implicar sanciones para el actor, en caso de no haber cumplido sus obligaciones de manera adecuada. Tal y como plantea Bovens, el foro puede ser real o

específico, como por ejemplo una persona o una agencia, o también puede ser una entidad virtual⁴⁸, como por ejemplo el público o la sociedad (Bovens 2005, p. 184). Según este mismo autor, y siguiendo la misma línea que Hughes, la obligación de rendir cuentas puede ser formal o informal. En el primer caso se basa en normativa y legislación aplicable bajo la que el actor está obligado a rendir cuentas frente a distintos foros, como por ejemplo agencias supervisoras, comisiones parlamentarias o auditores. En el segundo caso, la obligación es informal y, de hecho, puede incluso ser autoimpuesta, como es el caso de ruedas de prensa o confesiones públicas, entre otras situaciones. De aquí deriva el tipo de sanciones que pueden aplicarse en ambos casos, pudiendo ser en el primero multas, medidas disciplinarias o incluso sanciones penales, mientras que en el segundo puede implicar dar explicaciones frente a la prensa o un daño de la imagen pública del actor, entre otros.

Por otro lado, cabe tener presente que existen distintas áreas de la rendición de cuentas (Nonell 2006, p. 12) y que esta no corresponde tan solo a las administraciones públicas⁴⁹ sino que hay otros organismos que pueden ser objeto de este tipo de procesos. Estas áreas son:

- a. Las organizaciones públicas y las agencias independientes que dependen de la financiación pública. Se trata de contar con un instrumento que ayude a mejorar las decisiones políticas y financieras del gobierno haciendo más transparentes los beneficios que produce con los recursos públicos que gestiona. La transparencia permite mayor capacidad de crítica sobre los resultados (Nonell 2006, p. 23). Es importante destacar aquí la importancia de la relación y dependencia de la transparencia y la rendición de cuentas.
- b. El conjunto de organizaciones intermedias de la sociedad, tales como fundaciones, asociaciones y organizaciones no gubernamentales. La sociedad civil está compuesta de un entramado complejo de asociaciones de interés económico (sindicatos y patronales), fundaciones y organizaciones voluntarias y sin ánimo de lucro que son un componente esencial de las democracias actuales. Estas organizaciones tienen obligaciones respecto de sus empleados, de sus clientes, de sus financiadores, y hacia el público en general, así como hacia los gobiernos locales y nacionales (Nonell 2006, p. 25), frente a los que deben rendir cuentas.
- c. Las empresas, a través de la responsabilidad social corporativa, que afecta no solo a los accionistas, sino también a todos aquellos ciudadanos que se ven influidos por sus decisiones y con los que comparten intereses. La responsabilidad social de las empresas incluye, en primer lugar, aspectos relacionados con el producto que producen, garantizando las condiciones de seguridad y de calidad del mismo y también los aspectos relacionados con el trabajo, la necesidad de invertir en la comunidad, las relaciones laborales, la creación y mantenimiento del empleo (Nonell 2006, p. 25).

Esta investigación se centra en las dos primeras, especialmente en las administraciones y el sector público en general. En este contexto el término “público” puede tomar diferentes referentes. Por ejemplo, puede referirse a “abierto” o “transparente” en cuanto a que la rendición de cuentas pública no se lleva a cabo discretamente o a puerta

⁴⁸ – Bovens, con el término virtual, se refiere a entidades no específicas como por ejemplo, en el caso de los devotos cristianos podría ser Dios o la conciencia individual, o, en el caso de gestores públicos podría ser el público en general o la sociedad. Esto diferencia a estas entidades de aquello específico, como por ejemplo sería el caso de una persona concreta o una organización determinada.

⁴⁹ – Debe entenderse administración pública en el sentido más amplio del término, incluyendo órganos políticos y servidores públicos.

cerrada. Al contrario, está en sus principios el permanecer abierta al público en general. La información que se proporciona sobre el actor es generalmente accesible y se debate en público para que el foro pueda promulgar su juicio. El término “público” también puede referirse al objeto sobre el que se rinde cuentas, a que este sea de dominio público o se refiera a cuestiones de interés público. Esto no se limita necesariamente a organizaciones públicas, sino que, como apuntaba Nonell, puede extenderse a organismos privados que ejerzan funciones públicas u organismos privados que reciban capital público. En general, al hablar de rendición de cuentas pública, de lo que se habla es de rendir cuentas en, y sobre, el dominio público (Bovens, M; Schillemans, T.; Goodin 2016, p. 7).

Además, en el ámbito político, la noción de rendición de cuentas tiene dos dimensiones básicas: por un lado, la obligación de los políticos y funcionarios de informar sobre sus decisiones y de justificarlas en público (lo que en inglés se conoce como *answerability*) y, por otro lado, la capacidad de sancionar a políticos y funcionarios en caso de que hayan incumplido sus deberes públicos (lo que en inglés se conoce como *enforcement*) (Schedler 2008, p. 12). Estas dos dimensiones se incluyen dentro del proceso general de la rendición de cuentas (ver Figura 14). Para prevenir y corregir abusos de poder, se obliga al poder a abrirse a la inspección pública, se le exige explicar y justificar sus actos y se supedita a la amenaza de sanciones (Schedler 2008, p. 13). Para que esto sea posible, para poder afirmar que los políticos son responsables de una determinada acción, debe darse el caso de que dichos políticos actúen bajo un objetivo, que dispongan de cierta autonomía, y que sean capaces de elaborar estrategias y distinguir entre alternativas (Lewin 2007, p. 4). Básicamente, que sean autónomos.

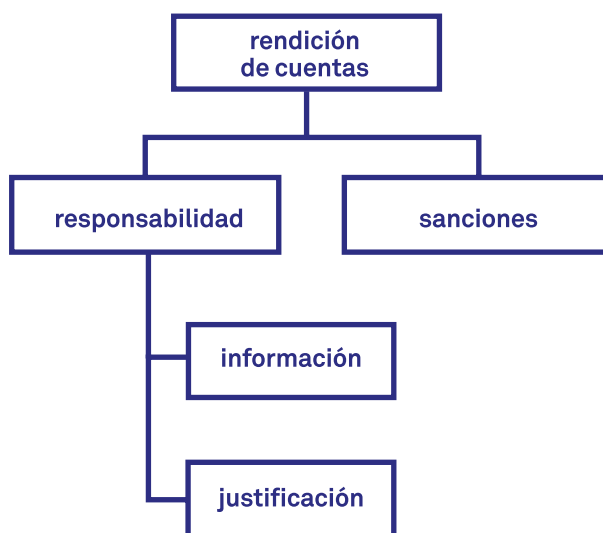


Figura 14 – Los pilares de la rendición de cuentas según Schedler.

En la Figura 14 se refleja la importancia de la responsabilidad de quien rinde cuentas y las sanciones que puede conllevar el incumplimiento de dicha responsabilidad, poniendo ambas al mismo nivel y relacionándolas de manera directa. Se parte de la base de proporcionar información y de permitir a quien rinde cuentas que justifique, a partir de dicha información y los documentos y evidencias que considere necesarios, sus acciones partiendo siempre de la responsabilidad. En caso de haber incumplido con su responsabilidad se podrán imponer sanciones. La rendición de cuentas es un derecho a la crítica y al diálogo (Schedler 2008, p. 15).

A partir de lo expuesto, de manera global se pueden encontrar dos grandes corrientes sobre la rendición de cuentas. Dentro del discurso político y académico en Estados Unidos, esta suele usarse como un concepto normativo, como un conjunto de estándares para la evaluación del comportamiento de los trabajadores públicos. Rendir cuentas es visto como una virtud, como una cualidad positiva y deseada de las personas, organizaciones o estados. De esta manera, los estudios sobre rendición de cuentas se centran en aspectos normativos, en estándares y en cómo evaluar el comportamiento actual de los trabajadores públicos (Bovens 2010, p. 947). El concepto de rendición de cuentas como una virtud es considerado una característica positiva de las organizaciones o los trabajadores. En sentido amplio, la rendición de cuentas, desde esta perspectiva, se relaciona de cerca con la formalidad y la responsabilidad, con una disposición para actuar de un modo transparente, justo, íntegro y equitativo (Bovens, M; Schillemans, T.; Goodin 2016, p. 8). Para ello, se requiere una serie de normas sobre el comportamiento de los actores implicados. Esto conlleva una problemática a la hora de hacer una evaluación, puesto que no existe un consenso general acerca de los estándares de un comportamiento adecuado para la rendición de cuentas y porque, además, dichos estándares podrían diferir en función del tipo de organización, la perspectiva política o el contexto institucional.

En la segunda corriente, dentro de los debates académicos británicos, australianos, canadienses y del viejo continente, la rendición de cuentas es considerada un mecanismo social, como una relación o acuerdo institucional por el cual un agente puede ser llamado a rendir cuentas por otro agente o institución (Bovens 2010, p. 948). De esta manera, los estudios se centran en el modo en que estos instrumentos o relaciones funcionan, y no en cómo se comportan los trabajadores públicos. Se centran en si estos pueden ser llamados a rendir cuentas a posteriori frente a los foros que los evaluarán (Bovens, M; Schillemans, T.; Goodin 2016, p. 9). El término se vincula con una relación social específica o un mecanismo que conlleva la obligación de explicar o justificar una conducta e implica una relación entre un actor, quien rinde cuentas (puede ser un individuo o una organización u organismo), y un foro, frente a quien el actor debe rendir cuentas (puede ser un individuo o una organización u organismo). Este proceso no solamente implica el hecho de proporcionar información sobre el desempeño, sino también la posibilidad de debatirla o cuestionarla por el foro y de responder por el actor y, finalmente, la posibilidad de que este último sea juzgado. Este juicio implica la imposición de sanciones formales o informales si quien rinde cuentas no ha obrado del modo adecuado. Por este motivo, también puede llamarse “rendición de cuentas pasiva” porque se produce a posteriori.

Ambas perspectivas son útiles para el estudio y el debate sobre los gobiernos democráticos, sin embargo, deben diferenciarse una de la otra ya que cada una centra su objeto de estudio en aspectos y problemáticas distintas y, por tanto, implican marcos conceptuales, estándares y dimensiones analíticas diferentes (Bovens 2010, p. 948).

Pese a estas diferencias, los procesos de rendición de cuentas comparten una serie de características comunes. Según Lindberg, se distinguen cinco elementos o condiciones para el proceso de la rendición de cuentas (Lindberg 2013, p. 79):

1. Un agente o institución que debe rendir cuentas (A).
2. Un área, responsabilidades, o dominio sujeto a la rendición de cuentas (D, de dominio).
3. Un agente o institución a quien A debe rendir cuentas (P, de principal).
4. El derecho de P a requerir a A que informe y explique o justifique sus decisiones con respecto a D.
5. El derecho de P a sancionar a A si esta falla en informar y/o en explicar o justificar sus decisiones con respecto a D.

Las condiciones 1 y 2 implican que una persona u organismo identificables deben tener poder sobre un cierto dominio y que este está sujeto a la rendición de cuentas. Las condiciones 3 y 4 implican que existe otro agente o institución con derecho a requerir al agente o institución A explicaciones y justificaciones sobre las decisiones y acciones con relación al dominio o área especificada. Esto no implica que las acciones llevadas a cabo por A tengan una incidencia directa en P.

En línea con estas condiciones presentadas por Lindberg, Meijer amplía la lista a seis elementos para el proceso de la rendición de cuentas (Meijer 2001, p. 362), con algunos matices:

1. Desencadenante: un evento o hecho que desencadene el proceso de la rendición de cuentas.
2. Persona u organización que debe rendir cuentas (equiparable a A).
3. Situación: debe darse una acción o situación por la cual la persona es susceptible de rendir cuentas (equiparable a D).
4. Foro: grupo frente al que la persona u organización rinde cuentas (equiparable a P).
5. Criterios: el proceso de rendición de cuentas requiere de unos criterios que son aplicados con el fin juzgar una acción o situación. Dichos criterios pueden derivar de una ley o de estándares o normativas políticos.
6. Sanciones: en algunos casos pueden imponerse sanciones a la persona u organización que rinde cuentas (equiparable al derecho de P a sancionar a A).

Al comparar ambos listados, se ven algunos elementos que coinciden, como son el agente o persona u organización que debe rendir cuentas (A), el foro, agente o institución frente a la que se rinde cuentas (P) o el derecho a sancionar, presentado en ambos casos como una opción o posibilidad. En la lista de elementos de Lindberg faltaría incluir los criterios a partir de los cuales se puede evaluar la actuación de A, así como la información y justificación de A frente a P. Pese a no estar en la lista, sí los menciona más adelante en su artículo, citando a Schedler y a Knouse, según los cuales debe existir un conjunto de criterios para medir el comportamiento objeto de la rendición de cuentas (Lindberg 2013, p. 211), ya que si no existen unos estándares o unas expectativas medibles respecto a la información, justificación, decisiones y desempeño, no puede haber rendición de cuentas. Además, se debe tener clara la diferencia de lo aceptable y lo que no lo es, para poder saber qué es necesario sancionar.

Por lo demás, ambas listas son similares y dan una idea general de aquello que debe incluir el proceso de rendición de cuentas, porque rendir cuentas es también establecer un diálogo, abrir un puente de comunicación permanente, institucional, sin pretextos entre funcionarios y ciudadanos (Schedler 2008, p. 7). De hecho, en un gobierno democrático representativo, los ciudadanos son los principales primarios y transfieren su soberanía a los representantes políticos quienes, a su vez, depositan su confianza en un gabinete o consejo de ministros. El consejo de ministros delega la mayor parte de sus poderes a los cientos o miles de servidores públicos de cada ministerio, quienes, a su vez, transfieren muchos poderes a organismos públicos o agencias independientes. Las agencias y organismos, al final de la cadena, gastan billones de dinero público (recaudados de los impuestos de los ciudadanos) y usan su poder y autonomía de decisión para aplicar políticas públicas, imponer multas, garantizar bienes y servicios, entre otros.

A partir de aquí, pueden distinguirse diferentes funciones de la rendición de cuentas (Bovens 2005, p. 192): control democrático, garantía y mejora de la integridad del gobierno, mejora del rendimiento o del desempeño, mantenimiento y mejora de la legitimidad del gobierno, balance de lo ocurrido y poder empezar de cero. Se explican a continuación:

1. La primera y principal función de la rendición de cuentas debe ser el control democrático. Cada uno de los eslabones de la cadena de delegación quiere controlar el ejercicio de los poderes transferidos mediante la rendición de cuentas del siguiente eslabón, hasta llegar a los ciudadanos, que son quienes finalmente juzgan las actuaciones y quienes pueden sancionar a sus representantes políticos en las elecciones. La rendición de cuentas en un gobierno democrático representativo es un proceso necesario, porque es lo que acaba proporcionando, tanto a los representantes políticos como a los ciudadanos, información suficiente para juzgar la integridad, efectividad y eficiencia de la gestión.
2. Otra de las funciones de la rendición de cuentas es la de garantizar y mejorar la integridad del gobierno. El carácter público de la rendición de cuentas permite la prevención frente a la corrupción, el nepotismo, el abuso de poder y otras formas de comportamiento y gobierno inapropiado. Es un modo de disuadir a los políticos y funcionarios de utilizar su poder para fines no apropiados, además de proporcionar supervisiones periódicas que deben disponer de información esencial y suficiente para poder realizar la trazabilidad de los abusos.
3. La tercera función es la de mejorar el rendimiento o el desempeño. La rendición de cuentas tiene el objetivo de fomentar el aprendizaje institucional, ya que no solo implica control, sino también prevención. El funcionario que debe rendir cuentas es informado acerca de los estándares, procedimientos y directrices a tener en cuenta que, en un futuro, pueden ser requeridos en un proceso de rendición de cuentas sobre su rendimiento y su conducta. Además, los procesos de rendición de cuentas conllevan retroalimentación sobre el funcionamiento de los individuos u organismos, cosa que puede fomentar la mejora y el aprendizaje a partir de la información recopilada.
4. Estas tres primeras funciones juntas dan lugar a una cuarta función, que es la de mantener y mejorar la legitimidad del gobierno. Si tenemos en cuenta los factores de transparencia, responsabilidad y obligación de respuesta, la rendición de cuentas funciona como un mecanismo de mejora de la confianza de los ciudadanos en el gobierno, así como un puente para unir a los ciudadanos con sus representantes y entre gobernados y gobernantes.
5. Por último, la rendición de cuentas también es importante en caso de tragedias, procesos de reconciliación tras un conflicto armado u otras situaciones de esta índole, pudiendo servir como catarsis para los ciudadanos (Bovens 2005, p. 193). Puede ayudar, tras un periodo trágico, con el objetivo de hacer balance sobre

lo ocurrido y poder empezar de cero. De este modo, puede ser una oportunidad de penitencia, reparación y perdón.

3.2.1 Fases de la rendición de cuentas

Los procesos de rendición de cuentas normalmente comprenden tres fases: la fase de información, la fase de discusión y la fase de sanción (Meijer 2001, p. 363).

La primera fase, de información, tiene como premisa principal la disponibilidad de los documentos. Se presupone que para que el foro pueda discutir y decidir si sancionar o no una acción de un individuo, lo primero que necesita una administración o un gobierno es reconstruir qué ha pasado (Meijer 2001, p. 363). Para ello, la información se convierte en algo indispensable y los documentos públicos pasan a ser la piedra angular y la fuente de información del proceso. Son precisamente estos los medios que podrán hacer viables la rendición de cuentas, desde el momento en que se facilita la puesta a disposición a las autoridades o ciudadanos de todos los documentos que evidencian los actos y actividades administrativas realizadas en el ejercicio de la función pública (Mendoza Navarro 2004, p. 75).

Se parte de la base de que las administraciones, para funcionar adecuadamente, crean y mantienen documentos, ya que requieren de la información en ellos contenida para su correcto funcionamiento. Por tanto, una adecuada gestión de documentos se convierte en requisito fundamental de cualquier gobierno o administración pública. Para cumplir con el proceso de rendición de cuentas, se necesita desarrollar e implementar sistemas de gestión documental que garanticen que estos son íntegros, fiables, auténticos y serán accesibles y usables a lo largo del tiempo que sean necesarios. Si estos sistemas funcionan y se mantienen de manera adecuada, la rendición de cuentas estará garantizada.

Una vez el foro reconstruye la situación de la cual se rinde cuentas, se pasa a la segunda fase, la de debate o justificación por parte de quien rinde cuentas ante el foro. Los servidores públicos deben enfrentarse a múltiples procesos de rendición de cuentas y pueden ser sujetos de ella por diferentes elementos de su conducta y frente a distintos foros. La rendición de cuentas está directamente asociada con la autoridad, aunque no necesariamente deba ser la autoridad política, sí se debe tener autonomía para la toma de decisiones de las cuales se debe rendir cuentas. Un subordinado que cumple con lo que le ordena un superior no puede ser responsable y, por tanto, no se le puede exigir rendir cuentas ni justificar la decisión. Deberá exigirse a quien tomó la decisión.

Analizada la documentación y reconstruida la situación o acontecimiento, se inicia la tercera fase, donde el foro decide si es necesario sancionar o no. La responsabilidad, con la doble exigencia de información y justificación que conlleva, no es el proceso completo de la rendición de cuentas. Adicionalmente, este también contiene elementos de coacción y castigo. Lo que cabe destacar es el aspecto impositivo, el esfuerzo por asegurar el cumplimiento con las normas por medio de la imposición de sanciones (Schedler 2008, p. 16). El derecho a sancionar está limitado al derecho a castigar un fallo de quien rinde cuentas, habiendo aportado la documentación suficiente para la reconstrucción y contextualización del hecho. Cabe diferenciar las sanciones por no aportar la información requerida por el foro (para poder llevar a cabo el proceso de rendición de cuentas) de las sanciones por la equivocación en la decisión

tomada. Esta faceta de la rendición de cuentas implica que quienes rinden cuentas no solamente expliquen qué han hecho y por qué, sino que también asuman las consecuencias de sus actos.

3.2.2 Tipos de rendición de cuentas

La rendición de cuentas lleva asociadas varias características: es *externa* cuando se produce hacia una persona u organismo ajeno a quien debe rendir cuentas; conlleva *interacción social e intercambio*, cuando una parte, la que busca la rendición de cuentas, busca respuestas y rectificación, mientras la otra parte, la que rinde cuentas, responde y acepta sanciones; implica un *derecho de autoridad*, de quien exige la rendición de cuentas sobre quien debe rendirlas, incluyendo derechos de solicitud de respuesta e imposición de sanciones (Mulgan 2000, p. 555).

Existen en la bibliografía diferentes propuestas de categorización para los tipos de rendición de cuentas. Para el desarrollo de este apartado se han seleccionado tres autores: Schedler, Bovens y Lindberg.

Se ha podido apreciar en apartados anteriores de este capítulo que este tipo de procesos son complejos e incluyen múltiples factores, actores u objetivos. Es a partir de estas y otras variables que los distintos autores proponen distinguir entre tipos diferentes de rendición de cuentas. No todos ellos coinciden en la categorización, debido a que no parten de las mismas variables. Schedler se centra en la direccionalidad del proceso. Bovens parte de los actores y finalidades de la rendición de cuentas. Finalmente, Lindberg se basa en las dimensiones del proceso, siendo este un enfoque más teórico que los de Bovens y Schedler. A continuación, se explican los diferentes tipos de estos tres autores.

Tipos de rendición de cuentas según Schedler

La distinción original entre rendición de cuentas horizontal y vertical que introdujo el politólogo argentino Guillermo O'Donnell es el punto de partida de la categorización de Schedler (Schedler 2008, p. 33). En esencia, la rendición de cuentas horizontal se refiere a relaciones de control entre agencias del Estado, mientras que la vertical se refiere a relaciones de control de la sociedad hacia el Estado. A continuación, se explican ambas en detalle, así como otros tipos derivados de la direccionalidad del proceso: vertical, horizontal, diagonal, transnacional y recursiva.

La rendición de cuentas vertical describe una relación entre desiguales, entre superiores y subordinados, entre principales y agentes. En las democracias representativas encuentra sus dos expresiones fundamentales en los controles electorales y de la sociedad. La primera se basa en la capacidad de los votantes para premiar o castigar el desempeño de sus representantes a través de elecciones periódicas. La segunda se basa en la capacidad de los ciudadanos, asociaciones cívicas y medios de comunicación de vigilar, interpelar y sancionar a políticos y funcionarios.

El concepto de controles verticales puede fluir de abajo hacia arriba, como los de la sociedad o electorales, o de arriba hacia abajo (ver Figura 15). Estos últimos forman parte indispensable de cualquier ejercicio de poder, ya que cualquier gobierno se preocupará por la rendición de cuentas burocrática.

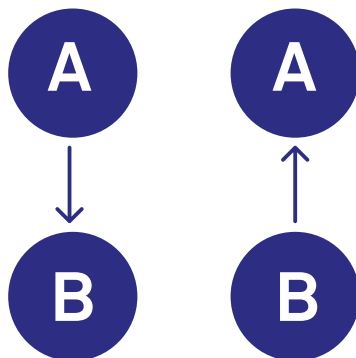


Figura 15 - Transparencia vertical (elaboración propia).

La rendición de cuentas horizontal describe una relación entre iguales, en la que principal y agente están en posiciones de poder equiparables (ver Figura 16). En la teoría democrática, la expresión paradigmática de una relación horizontal de este tipo es la clásica división de poderes (Schedler 2008, p. 34). La teoría afirma que los poderes ejecutivo, legislativo y judicial se limitan y controlan mutuamente en un sistema balanceado de pesos y contrapesos. Sin embargo, una agencia que exige cuentas a otra no puede estar literalmente en igualdad de condiciones con la agencia que rinde cuentas, sino que el controlador debe tener mayor poder que el controlado para una efectividad en el proceso, además de contar con la autonomía y autoridad suficientes.

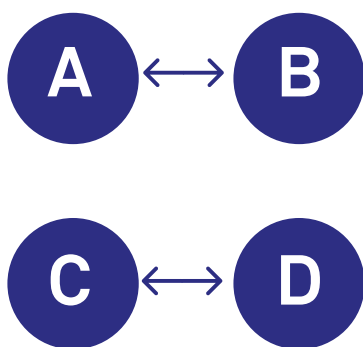


Figura 16 - Transparencia horizontal (elaboración propia).

Si se concibe la idea de los controles horizontales de manera literal, las relaciones inevitablemente asimétricas entre agentes y sujetos de control aparecen como “anomalías” empíricas. Para corregir esta imprecisión, Schedler introduce la noción de controles “diagonales” u “oblicuos”. Estas categorías intermedias entre lo horizontal y lo vertical evitan los malentendidos sobre la equivalencia de poder entre el controlado y el controlador (ver Figura 17).

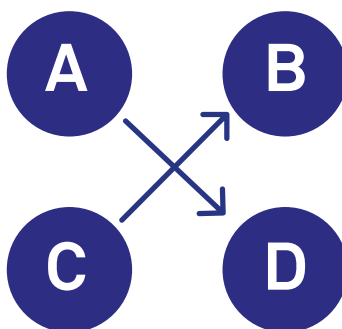


Figura 17 - Transparencia diagonal (elaboración propia).

Los tipos explicados se reducen a controles dentro de los límites de sistemas políticos nacionales, pero, debido a la globalización y a una realidad cada vez menos sectorizada, aparece un nuevo tipo, el que controla a nivel internacional y entre estados, globalizando también la práctica de la rendición de cuentas. Así, ha surgido una gama muy amplia de agentes de rendición de cuentas que actúan a través de las fronteras de los estados, dando como resultado la categoría de transparencia transnacional (ver Figura 18). Algunos ejemplos son Amnistía Internacional, la Corte Penal Internacional, el Fondo Monetario Internacional, entre otros. Estos actores transnacionales no encajan en los tipos anteriores, ya que parten de la premisa de un estatus “extranacional”, rigiéndose por normativas y estándares muy distintos, así como por mecanismos más complejos, pese a que la idea original de la rendición de cuentas se mantiene intacta.

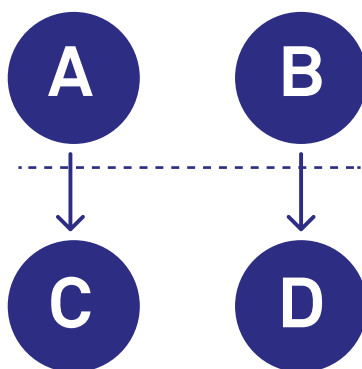


Figura 18 - Transparencia recursiva (elaboración propia).

Finalmente, Schedler añade la transparencia recursiva. En este tipo se enmarca la “meta-rendición” de cuentas, con la finalidad de garantizar que los agentes de rendición de cuentas rindan cuentas también ellos mismos. En este caso, se debe huir de la idea de verticalidad y buscar una opción más en línea con la idea diagonal, en la que una red de agencias de control mantengan relaciones de rendición de cuentas entre ellas, de manera que la agencia A rinda cuentas a la agencia B, que, a su vez, rinde cuentas a C, que, a su vez, rinde cuentas a A nuevamente (Schedler 2008, p. 37) (ver Figura 19). De este modo ninguna agencia está por encima de las demás, pero se establecen controles periódicos sobre los propios controladores.

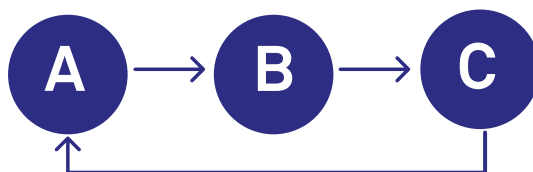


Figura 19 - Transparencia recursiva (elaboración propia).

Tipos de rendición de cuentas según Bovens

Para Bovens, los diferentes tipos de rendición de cuentas pueden clasificarse a partir de tres preguntas (Bovens 2010, p. 953), como son: a quién se rinde cuentas, quién debe rendir cuentas y por qué se debe hacer. La respuesta a cada una de estas tres preguntas da como resultado una clasificación de diferentes tipos, que se explica a continuación.

La primera pregunta es a quién o para quién se rinde cuentas. La respuesta proporciona una clasificación en función del foro frente al cual el actor requiere rendir cuentas. En el caso de foros políticos, se da una *rendición de cuentas política*. En el caso de foros que ejercen, de manera independiente y externa, una supervisión o auditoría administrativa y financiera se da una *rendición de cuentas administrativa*. En el caso de foros de la sociedad civil, como organizaciones sin ánimo de lucro, se da una *rendición de cuentas social*.

La siguiente cuestión plantea quién debe rendir cuentas. En el caso de organizaciones o corporaciones que deben cumplir ciertas leyes o procedimientos legales se da una *rendición de cuentas organizacional o corporativa*. En muchos casos, la rendición de cuentas se da en la alta dirección de las organizaciones, que es llamada a rendir cuentas interna o externamente. En este caso, Bovens se refiere a la *rendición de cuentas jerárquica*. Un claro ejemplo son los ministros o altos cargos de administraciones públicas en países con sistemas parlamentarios. Dentro de este grupo, por último, se encuentra la rendición de cuentas colectiva, que se refiere a la rendición de cuentas de un grupo o colectivo, como por ejemplo cuando un parlamento o un congreso deben rendir cuentas.

La tercera pregunta que plantea Bovens es por qué un agente determinado debe rendir cuentas. Este aspecto se refiere a la naturaleza de la relación entre quien rinde cuentas y el foro frente al cual lo hace, en el sentido de si esta es contractual, jerárquica, voluntaria u obligatoria, entre otras. Suele realizarse la clasificación basándose en una metáfora espacial, dando como resultado tres tipos de rendición de cuentas: *vertical*, *horizontal* y *diagonal*. Estos tipos coinciden con la idea de direccionalidad planteada por Schedler, ya explicada anteriormente, aunque el punto de partida sea distinto.

En la siguiente figura puede verse la clasificación de Bovens de manera esquemática (ver Figura 20).

PREGUNTA	TIPOLOGÍA
¿A / Para quién?	política
	administrativa
	social
¿Quién?	corporativa
	jerárquica
	colectiva
¿Por qué?	vertical
	horizontal
	diagonal

Figura 20 – Tipos de rendición de cuentas según Bovens (elaboración propia).

Tipos de rendición de cuentas según Lindberg

Lindberg parte, para su categorización, de tres dimensiones desde las que estudia la rendición de cuentas. Estas son la fuente, el grado de control y la direccionalidad (Lindberg 2013, p. 212).

La primera dimensión se refiere a la fuente (agente o A) o el origen del proceso, si rinde cuentas interna o externamente. Por ejemplo, los gestores públicos y funcionarios rendirán cuentas normalmente hacia sus superiores (principales o P) con carácter interno, en cambio los políticos y altos cargos rendirán cuentas hacia el exterior, a los ciudadanos (principal o P).

La segunda dimensión se refiere al control que ejerce el principal (P) o quien exige la rendición de cuentas sobre el poder o agente (A). Por ejemplo, en qué grado los votantes ejercen un control sobre sus representantes y los efectos e influencias que esto produce sobre su comportamiento. Los efectos serán diferentes que los que produzca la realización de una auditoría de cuentas o una auditoría del desempeño de la gestión basada en estándares internacionales.

La tercera dimensión se refiere a la direccionalidad de las relaciones entre quien rinde cuentas (A) y a quién se rinde cuentas (P). Puede ser vertical, tanto hacia el nivel superior como hacia el inferior. Por ejemplo, cuando los políticos rinden cuentas a los ciudadanos sobre sus decisiones lo hacen de manera vertical, hacia abajo. También se dan relaciones entre iguales (Lindberg 2013, p. 213), que se denominan horizontales, por ejemplo cuando el tribunal constitucional revisa las leyes aprobadas por el poder legislativo⁵⁰.

A partir de estas tres dimensiones y sus combinaciones, Lindberg elabora una tabla en la que se contemplan todos los tipos de rendición de cuentas (ver Figura 21). En esta tabla también pueden encajar algunos tipos explicados por otros autores, como Bovens y Schedler.

FUENTE	CONTROL	DIRECCIONALIDAD		
		VERTICAL		HORIZONTAL
		hacia arriba	hacia abajo	
interna	alto	de negocio	burocrática	auditoría
	bajo	patrón - cliente	cliente - patrón	profesional
externa	alto	representativa	fiscal	legal
	bajo	de la sociedad	política	reputación

Figura 21 – Tipologías de rendición de cuentas según Lindberg (Lindberg 2013, p. 213)

Análisis comparativo de tipos

Se parte de tres propuestas de tres autores distintos y realizadas a lo largo del tiempo. La primera es de Schedler, del año 2008; la segunda es de Bovens, del año 2010; y la tercera es de Lindberg, del año 2013. De este modo, puede apreciarse también la evolución del término y de la aplicación del proceso de rendición de cuentas a diferentes ámbitos y desde diferentes perspectivas. En las tres propuestas se tienen en cuenta algunos aspectos comunes a la hora de establecer los tipos, como son la direccionalidad del proceso y la fuente o el agente (A) sujeto de la rendición de cuentas.

Respecto a la direccionalidad, las tres propuestas contemplan la horizontalidad y la verticalidad, aunque solo en dos de ellas se introduce el concepto de rendición de cuentas diagonal, en referencia a aquellas ocasiones en que or-

⁵⁰ – Lindberg toma como referencia la distinción entre rendición de cuentas horizontal y vertical que introdujo el politólogo argentino Guillermo O'Donnel, tal y como también lo hace Schedler en su definición de tipologías.

ganismos con el mismo peso rinden cuentas entre sí. Si bien es cierto que podría incluirse dentro del tipo horizontal, Schedler apunta que las relaciones de poder entre iguales no siempre son horizontales y el controlador debe tener poder sobre el controlado para que el proceso de rendición de cuentas sea realmente efectivo.

Respecto al sujeto de la rendición de cuentas, se encuentran referencias en Bovens y Lindberg, pero no en Schedler. Lindberg diferencia entre rendición de cuentas interna o externa refiriéndose a la relación entre el agente (A) y el principal (P). Si esta relación se produce internamente, dentro de la misma organización, la denomina interna. Si esta relación se abre hacia el exterior, por ejemplo, entre votantes y representantes políticos, la denomina externa. Cabe mencionar que la distinción de Lindberg en este caso se utiliza como un criterio para establecer su tipo, es decir, no solamente habla de rendición de cuentas interna y externa a nivel general, sino que su propuesta incluye también la direccionalidad y la relación (interna o externa).

A esto hay que añadir el factor del foro o principal (P), es decir, quien evalúa al agente (A). Este elemento se debe leer en complementariedad con la relación entre A y P, pero, en este caso, desde la perspectiva del foro o principal (P). Bovens menciona tres foros, que pueden enmarcarse en procesos de rendición de cuentas externos: foros políticos, foros administrativos y foros sociales, realizando, de este modo, una diferenciación entre tres tipos de rendición de cuentas.

Los aspectos que se mencionan tan solo por uno de los autores a la hora de realizar la categorización son el territorio, el grado de control y la meta-rendición de cuentas.

Respecto al territorio, se presupone que los tres autores enmarcan los procesos de rendición de cuentas a nivel nacional o estatal. Schedler añade a este factor la rendición de cuentas transnacional, con relación a la globalización en las relaciones políticas, administrativas y de otra índole que se dan hoy en día y que necesitan de procesos que van más allá de lo nacional, incluyendo organismos internacionales de control y auditoría.

El grado de control puede afectar en el comportamiento del agente (A), así como en las consecuencias del proceso de rendición de cuentas, aunque no afectará a la metodología o elementos del proceso.

Por último, se considera de especial relevancia el concepto introducido por Schedler sobre la meta-rendición de cuentas o rendición de cuentas recursiva, referida al control sobre quien controla. Es fundamental que los organismos de rendición de cuentas sean transparentes, íntegros y confiables y de aquí surge la necesidad de que también sean objeto de la rendición de cuentas.

3.3 Gestión documental, transparencia y rendición de cuentas

Sin una evidencia documental fiable y auténtica como apoyo a cualquier proceso de rendición de cuentas, el gobierno, la sociedad civil y el sector privado no pueden garantizar la transparencia, garantizar la rendición de cuentas, o tener en cuenta el ejercicio del buen gobierno (Barata, Cain, y Thurston 1999, p. 106). La rendición de cuentas está anclada en la práctica de la gestión de documentos y da lugar a la narración en un contexto de relaciones sociales (poder) dentro de las cuales se aplican unos estándares y donde el cumplimiento de las obligaciones es una previsión razonable (Bovens, M; Schillemans, T.; Goodin 2016, p. 2).

La información es uno de los pilares de la democracia y permite al ciudadano incorporarse más al desarrollo de la misma e implicarse en el futuro de las sociedades (Nonell 2006, p. 27). La sociedad civil juega un papel fundamental en cualquier proceso de rendición de cuentas, pero, para ello, es necesario conseguir que se implique en el proceso y esto pasa por poder disponer de información fiable, accesible y, sobre todo, comprensible. De hecho, Thurston afirma que el éxito del gobierno abierto reside en la capacidad de los gobiernos de crear y conservar documentos íntegros, confiables y rigurosos como evidencia de las políticas, acciones y transacciones del gobierno, así como también en la capacidad de los ciudadanos de acceder a estos. Los ciudadanos necesitan saber que pueden confiar en la información que las administraciones proporcionan, que esta información les ayudará a proteger sus derechos y sus privilegios, que servirá como prueba de que la justicia se reparte de modo imparcial, así como que puede ser usada para ayudarles a escrutar lo que las administraciones están llevando a cabo (Thurston 2012, p. 1).

Para facilitar la transparencia, así como para aumentar la confianza en los procesos de rendición de cuentas se necesita disponer de un sistema que sea capaz de permitir y facilitar la localización de la información y los documentos de la organización. Esto puede ser una realidad cuando se hayan implantado sistemas de gestión documental en las administraciones públicas, ya que únicamente a través de la normalización en los procesos de gestión de documentos se puede disponer de información fácilmente recuperable, además de íntegra, fiable y usable. De nada sirve poder acceder a un documento si no puede visualizarse (usabilidad), si la información contenida ha sido alterada (integridad), si el documento es incompleto o contiene informaciones falsas (fiabilidad) o si el documento no tiene garantía de autenticidad (que haya sido creado por quien dice que lo ha creado y en qué momento lo ha creado). En cualquiera de estas situaciones ni la transparencia ni la rendición de cuentas quedarían satisfechas.

Teniendo en cuenta que el objeto de la transparencia y el medio para la rendición de cuentas son, mayoritariamente, documentos y la información que contienen, se considera necesario incluir las políticas de gestión de documentos, de manera generalizada, junto con los objetivos y políticas de transparencia en las administraciones públicas. La gestión del ciclo de vida de los documentos ya contempla el acceso y la difusión de información y documentos en su estructura, por tanto, incluirla en la definición de estrategias para la transparencia solo puede aportar beneficios. En caso contrario, el cumplimiento con las obligaciones de transparencia y rendición de cuentas se verá siempre coartado de una de sus bases necesarias para ser efectivo y confiable: la existencia de información íntegra, auténtica, fiable y accesible.

Sin embargo, la información es un bien que tiene un coste en términos de tiempo, para adquirirla, y en términos de formación, para utilizarla adecuadamente. En muchos casos es difícil obtener información de calidad, transparente y asequible y, por lo tanto, es necesario crear los mecanismos adecuados para facilitar la accesibilidad a la misma (Nonell 2006, p. 27). Pero no se trata solo de facilitar la accesibilidad, sino que las administraciones públicas, antes de

nada, necesitan conocer con qué información y documentación cuentan y qué parte de la misma debe ser accesible. En los procesos de rendición de cuentas, por tanto, juegan un papel básico las evidencias documentales, pero también una adecuada gestión de las mismas, puesto que, sin una correcta gestión, preservación y accesibilidad de los documentos, no puede darse transparencia ni rendición de cuentas.

Los documentos son, por tanto, una parte fundamental ya que son la base sobre la que el foro puede reconstruir los hechos y las decisiones (Meijer 2013, p. 430), así como juzgar, a partir de datos objetivos, el comportamiento de los individuos u organismos. Los documentos sirven de evidencia para poder reconstruir de manera precisa las acciones y las decisiones tomadas. Cabe recalcar la capacidad del documento de servir como evidencia o como prueba, entendiendo que este contiene la información contextualizada y proporciona testimonio de una acción, actividad, decisión. El término “evidencia” no debe entenderse en el sentido legal de la palabra, sino que implica que el documento puede ser utilizado cuando sea necesario demostrar que una actividad se llevó a cabo. Además, cabe tener en cuenta que el documento proporciona evidencia de una relación derecho-deber, no solo entre las partes que intervienen directamente en la acción, sino que también para todos aquellos afectados por dicha acción (Iacovino 2010, p. 198).

Por tanto, los documentos, primero y principalmente, proporcionan evidencia de las transacciones de las cuales forman parte. De aquí derivan su significado y su valor informativo. Es esencial, por lo tanto, que estos sean completos, fiables y exactos. Su creación y gestión es crítica para su uso y para el rol que estos juegan en las relaciones del gobierno con la sociedad a lo largo del tiempo. Su creación y su gestión efectivas son precondiciones para una sociedad altamente informada, siendo también los pilares que apuntalan la rendición de cuentas pública, el acceso a la información y la legislación sobre privacidad y protección de datos personales, así como otros derechos de los ciudadanos, sin olvidar la calidad del patrimonio documental compuesto por documentos de archivo con valores continuos (McKemmish y Upward, 1993, p. 1).

Documentos pobremente organizados, fragmentados o ilocalizables pueden dar como resultado retrasos y obstáculos para dar respuesta a las solicitudes de acceso a la información. Cuando los documentos no están bien gestionados, la información puede ser manipulada, eliminada, fragmentada o puede perderse, y los documentos pasan a ser no confiables. Sin un adecuado control de la gestión documental, los ciudadanos no pueden probar un trato injusto o desigual, las violaciones de derechos humanos son difíciles de combatir y las personas no pueden realizar contribuciones de una manera informada en los procesos participativos. Los sistemas de gestión documental débiles, además, pueden conllevar dificultades a la hora de determinar qué documentos pueden hacerse públicos y cuáles deben reservarse (Thurston 2012, p. 5).

De este modo, reconocer la importancia y las implicaciones que puede conllevar la gestión de los documentos permite a las organizaciones ser conscientes de la necesidad de contar con sistemas de gestión documental, dentro de los cuales se implementen políticas de disposición y de acceso, para garantizar que aquellos documentos necesarios se conservan y pueden ser accesibles durante el tiempo necesario. De hecho, Nonell afirma que las bases de cualquier proceso de rendición de cuentas están en el desarrollo de una serie de principios básicos (Nonell 2006, p. 14) entre los que se encuentran precisamente los sistemas de información. Estos principios son:

- La conducta ética y su traducción en un compartimiento regulado por determinados códigos.
- Unos sistemas de información que suministren datos entendibles, asequibles y transparentes y que permitan a los ciudadanos identificar los beneficios sociales que produce la actuación política. Se refiere a los sistemas de gestión documental, que gestionan documentos, información y datos.

- La voluntad política de llevar a cabo el desarrollo de estos principios que permitan liderar un cambio en la gestión pública y en la elaboración de las políticas públicas para favorecer las innovaciones.

Los sistemas de gestión documental, por tanto, contribuyen enormemente a los objetivos de transparencia y de rendición de cuentas y lo hacen gracias al desarrollo de instrumentos y procesos normalizados. Entre los mencionados en el capítulo 2, para estos objetivos cabe destacar la clasificación, la descripción, la disposición y el acceso.

La clasificación permite identificar todos los documentos que se deben crear y proporciona un método para agruparlos de acuerdo a la actividad y función que desarrollan. Estas agrupaciones permiten la automatización de procesos, como puede ser la publicación de documentos en los portales de transparencia o la eliminación de restricciones de acceso pasado el tiempo estipulado, entre otros. La clasificación, además, permite sistematizar y controlar la eliminación de documentos, garantizando el cumplimiento con la legislación aplicable en cada caso. De este modo, las administraciones públicas pueden asegurarse de que disponen de aquellos documentos de los que deben disponer, en los momentos en que sea necesario.

De manera complementaria, los modelos de descripción y los esquemas de metadatos contribuyen a una fácil recuperación de la información. Normalizan la descripción de los documentos mediante un conjunto de metadatos que se usan para identificarlos, describirlos y gestionarlos. Estos se vinculan a los documentos desde el momento de su creación y los acompañan a lo largo de toda su vida. Incorporan información para identificar el contexto de creación de los documentos, para describirlos, para aplicar el calendario de conservación, gestionar la preservación digital y gestionar el acceso (Casadesús de Mingo, Mauri Martí, y Perpinyà Morera 2016, p. 13). De este modo, permiten el seguimiento de la trazabilidad de los documentos, lo que conlleva un mayor control sobre la integridad y la fiabilidad de la información. Las evidencias circunstanciales del hecho, las personas involucradas y sus intenciones, independientemente del resultado, se basan en los metadatos capturados y preservados en un sistema de gestión documental (Iacovino 2010, p. 199).

Con relación a la disposición, lo que interesa mayoritariamente a las administraciones públicas es conservar los documentos durante todo el tiempo en que estos son necesarios, siguiendo siempre la legalidad vigente. Es imposible pensar en transparencia o en rendición de cuentas si la documentación ha sido destruida. Preservar documentos para establecer derechos es un aspecto de la rendición de cuentas que puede relacionarse con un hecho que acaba de pasar, está a punto de pasar o pasó hace algún tiempo. La visión hacia los usos futuros de los documentos, así como a lo largo del pasado, son cuestiones centrales sobre la rendición de cuentas para los archiveros (Iacovino, 2010, p. 185).

Es por ello que resulta fundamental disponer de calendarios de conservación y eliminación de documentos para controlar y autorizar la toma de decisiones sobre qué documentos y durante cuánto tiempo deben ser conservados. Para ello debe existir un procedimiento interno sobre valoración documental y sobre destrucción documental, debe llevarse a cabo y documentarse la identificación de los requisitos legales y normativos que es necesario cumplir, debe elaborarse y aprobarse de manera formal el calendario de conservación, donde se indiquen los periodos de conservación y la posibilidad de eliminación de cierta documentación pasados unos plazos establecidos de acuerdo con la legislación.

El calendario de conservación es uno de los instrumentos más potentes de gestión documental para minimizar los riesgos relacionados con la eliminación no controlada de los documentos, puesto que cada expediente y documento incorpora en sus metadatos la información relacionada con su calendario vital (Casadesús de Mingo *et al.* 2016, p. 13). Lo interesante de esto es poder automatizar el proceso de destrucción, sirviendo como método de prevención para eliminaciones no controladas o no autorizadas. También cabe destacar que, al asegurar la cadena de custodia ininterrumpida de la documentación, se evitan pérdidas de documentos y se contribuye a garantizar su integridad.

Otro de los instrumentos fundamentales en este sentido es el registro de eliminaciones. Este recopila la información de las eliminaciones documentales efectuadas por la administración pública, previo establecimiento de los plazos en el calendario de conservación, siempre a partir de la legislación vigente. El registro de eliminaciones es un mecanismo de control para evitar destrucciones no permitidas y fraudulentas, así como para combatir el riesgo de inaccesibilidad derivado.

Relacionado directamente con la valoración documental, se encuentra el régimen de acceso a la información, que normalmente se controla mediante el cuadro de seguridad y acceso. De este modo, se establece el modelo de roles y permisos a aplicar para fijar los derechos de acceso, consulta y modificación de la documentación. El acceso se vincula a la clasificación y a la valoración documental. Se convierte en una herramienta imprescindible para la trazabilidad sobre el acceso a la información a lo largo de todo el ciclo de vida, permitiendo saber con exactitud quién y cuándo ha accedido a qué documentos. Esto sirve como medida preventiva y persuasiva sobre las personas que pretendan modificar o eliminar documentos sin autorización, puesto que el sistema permite identificar al autor de las gestiones y acciones que se han llevado a cabo con cada documento. El acceso, además, permite mantener el control sobre las restricciones, así como también sobre aquello que debe publicarse en los portales de transparencia. Mediante la asignación de metadatos, se pueden también automatizar estas publicaciones, así como mantener o eliminar las restricciones de acceso (como los cifrados) en el momento en que sea necesario.

Finalmente, los sistemas de gestión documental permiten enlazar la información publicada en portales de transparencia o los documentos empleados para procesos de rendición de cuentas con la fuente, es decir, el documento original que se creó como parte de la actividad que se hace pública o que se juzga. En la mayoría de ocasiones, estos procesos se llevan a cabo mediante copias simples de los documentos y no se da importancia a la comprobación de que la información realmente es veraz y auténtica. Sin embargo, para que sean realmente efectivos es absolutamente necesario ser capaz de enlazar la fuente documental original con el fin de corroborar la autenticidad de la información.

Se puede apreciar, a partir de estas explicaciones, cómo los procesos y los instrumentos de gestión documental contribuyen de manera inequívoca a una mejora de las condiciones para la transparencia y para los procesos de rendición de cuentas. Esto se consigue a partir de la implantación, el mantenimiento y la mejora de sistemas de gestión documental, que incluyen en su razón de ser ambos objetivos. Hasta tiempos recientes, los sistemas de gestión documental de las administraciones públicas se percibían como algo centrado exclusivamente en el control de los documentos a nivel interno, y básicamente, de los documentos en papel. Sin embargo, en la actualidad, para dar respuesta a las obligaciones de transparencia y rendición de cuentas que establece la legislación, los sistemas de gestión documental deben entenderse más allá de la gestión interna, para poder garantizar que la información pública pueda ser puesta a disposición de la ciudadanía garantizando su autenticidad, integridad, trazabilidad y reutilización. De hecho, el cumplimiento de las obligaciones de transparencia pública exige que la transparencia se incorpore en el propio diseño de los sistemas de gestión documental para, más allá de permitir gestionar la creación o la generación de información y documentos, se facilite también su difusión y permita la reutilización, plasmándose estas dimen-

siones en las diferentes fases de su ciclo de vida (Casadesús de Mingo y Cerrillo i Martínez 2018, p. 7). Estos conceptos ya estaban contemplados en la primera versión de la norma ISO 15489, publicada en el año 2001, que se basaba en la Norma Australiana AS 4390, Records Management, del año 1996. En ella se afirmaba que un sistema de gestión documental se convierte en una fuente de información sobre las actividades de la organización que puede servir de apoyo a posteriores actividades y toma de decisiones, al tiempo que garantiza la rendición de cuentas frente a las partes interesadas presentes y futuras (AENOR 2006b, p. 9). Por tanto, la gestión documental no solo debe entenderse como una herramienta de gestión interna, sino también como un instrumento necesario para la transparencia y la rendición de cuentas.

A su vez, la rendición de cuentas implica transparencia, apertura, confianza y responsabilidad, en oposición al secretismo, el encubrimiento y la corrupción. En países con gobiernos elegidos democráticamente esto es sinónimo de acceso abierto a los documentos públicos (Iacovino 2010, p. 181), que se custodian en los archivos de los organismos y administraciones públicas. El documento de archivo se define por su contextualidad y su transaccionalidad, esto es, su relación con las transacciones u operaciones para las que fue generado. Por tanto, principalmente los documentos proporcionan evidencia de las operaciones de las que han formado parte, derivando de ahí su significado y su valor informativo.

Como se ha visto en la figura 13 de este apartado, la primera fase para que pueda iniciarse el proceso de rendición de cuentas pasa por el acceso a una determinada información. Cualquier organismo público utilizará, por tanto, documentos como apoyo para la rendición de cuentas, para probar o evidenciar que ha cumplido con sus obligaciones o que ha trabajado de acuerdo a las mejores prácticas. Los organismos públicos están sujetos a la rendición de cuentas de muchas maneras: deben cumplir con requisitos legales, normativos y fiscales, y pasar auditorías e inspecciones de varios tipos; deben ser capaces de dar explicaciones sobre las decisiones tomadas o las acciones llevadas a cabo. El uso de los documentos es el medio primario por el cual las organizaciones pueden defender sus acciones en caso de ser llamadas a rendir cuentas por su conducta (Shepherd y Yeo 2003, p. XI). Por tanto, los documentos son la base indispensable de este proceso, pero, para que ello ocurra, los organismos públicos deben tener la voluntad de ser transparentes.

Para su propio funcionamiento y control, la administración pública debe definir políticas de gestión de documentos, así como implantar sistemas de gestión documental, que ya incorporan en su diseño los procesos de acceso, publicidad y rendición de cuentas (Casadesús de Mingo y Cerrillo i Martínez 2018, p. 14). Se trata de simplificar estos procesos, consiguiendo a la vez una mayor capacidad para cumplir con la normativa en estas materias. Los sistemas de gestión documental permiten, como se ha explicado, automatizar y sistematizar la publicidad activa, gestionar el acceso a la información, garantizar las limitaciones de la transparencia y la protección de datos personales, facilitar las conversiones a formatos abiertos y reutilizables, y permitir la actualización de información, entre otros. Por tanto, no es necesario desarrollar nuevas metodologías, sino aplicar las ya existentes y aunar esfuerzos a nivel interno para conseguir una mejor organización para la transparencia pública.

Capítulo 4.

Análisis de las percepciones de los profesionales sobre la gestión de riesgos documentales a través de la metodología del *Focus Group*.

El método del *Focus Group* consiste en la realización de una entrevista en grupo, cuyo objetivo es profundizar y enfatizar sobre un tema o una materia específicos. Un moderador guía la entrevista mientras un pequeño grupo de personas debate sobre los temas que el entrevistador va introduciendo (Morgan 1998b, p. i). El objetivo principal es el de recopilar datos e información que puedan ser analizados. Para ello es imprescindible la escucha activa.

El *Focus Group* no es una actividad pasiva dentro de la investigación, sino que requiere de una planificación adecuada, de una selección exhaustiva de los participantes y de la decisión de los temas a tratar, para la profundización y generación de conclusiones relevantes, para la investigación, entre otros aspectos.

Esta metodología se ha empleado anteriormente en investigaciones archivísticas y de gestión documental, mayoritariamente en países anglosajones como Australia, Canadá o el Reino Unido, aunque también se encuentran estudios en los países nórdicos. Algunas de estas investigaciones estudian aspectos como la gestión documental para el acceso a la información pública⁵¹, el uso de redes sociales desde los archivos⁵², la transformación digital de la pequeña y mediana empresa⁵³ o la formación y las competencias de los profesionales para la gestión de documentos electrónicos⁵⁴. Como puede apreciarse, las temáticas son muy diversas, sin embargo, los *Focus Groups* que se han tomado como ejemplo suelen coincidir en el número de grupos seleccionados. Suelen emplear uno, dos o cinco grupos de debate, siendo el porcentaje más alto el que realiza el estudio con dos grupos. De los artículos consultados como ejemplo, el más antiguo fue publicado en el año 2005 y el más reciente es del año 2013.

⁵¹ – Shepherd, E., Stevenson, A. & Flinn, A., 2010. Information governance, records management, and freedom of information: A study of local government authorities in England. *Government Information Quarterly*, 27(4), pp. 337–345.

⁵² – Williams, S.P. & Hardy, C.A., 2011. Information Management Issues and Challenges in an Enterprise 2.0 Era: Imperatives for Action. *24th Bled eConference eFuture: Creating Solutions for the Individual, Organisations and Society*, June 12–15, pp. 56–67.

⁵³ – Smyth, Z.A., 2005. Implementing EDRM: has it provided the benefits expected? *Records Management Journal*, 15(3), pp. 141–149.

⁵⁴ – Partridge, H. & Hallam, G., 2004. The double helix: A personal account of the discovery of the structure of [the Information Professional's] DNA. *ALIA Biennial Conference*; Johare, Rusnah. 2006.

4.1 Propuesta y Objetivos

La decisión de utilizar la técnica del *Focus Group* viene de la necesidad de aproximarse al conocimiento que tienen los profesionales del sector acerca de la gestión de riesgos documentales, ya que es un tema muy poco trabajado en el ámbito de la archivística y la gestión de documentos a nivel estatal. Justo se está introduciendo en nuestro territorio y es por ello que resulta de gran interés conocer qué percepción tienen los profesionales.

La técnica del debate, entre diferentes expertos de distintos ámbitos relacionados con el mundo de la gestión documental, se considera más dinámica que la realización de entrevistas o encuestas. Este dinamismo ayuda a aflojar temáticas y discusiones que, de otro modo no serían posibles. Asimismo, con el debate entre distintas personas con perfiles diferentes se consigue, además de obtener respuestas a las preguntas, observar la interacción entre los participantes de cada grupo.

Para esta investigación se organizan dos grupos de debate con intención de realizar una pequeña intrusión del tema entre personas con una amplia trayectoria profesional. El objetivo final es conocer el grado de conocimiento y las expectativas de los participantes, de ambos grupos, sobre el impacto de la gestión de riesgos documentales en la implantación de sistemas de gestión documental en las organizaciones. Se opta por seguir la metodología del *Focus Group* poco estructurado, ya que este resulta de mayor utilidad para propuestas exploratorias (Morgan 1998a, p.47), como es el caso de esta investigación. Con este fin, además, se definen una serie de preguntas abiertas para que los distintos participantes aborden el tema y generen ideas. Es importante remarcar que los *Focus Groups* poco estructurados no son grupos de debate desenfocados o desestructurados, sino que son grupos de debate sobre temas más amplios, cuyo objetivo se alcanza a través de un conjunto de preguntas amplias y abiertas (Morgan 1998a, p.49).

Las preguntas formuladas a ambos grupos son, por tanto, definidas de manera amplia para obtener respuestas abiertas de los distintos participantes a través de sus experiencias profesionales en el campo de la gestión documental, la gestión de riesgos documentales y cómo estos pueden afectar al objetivo de la rendición de cuentas en las administraciones públicas.

A continuación, se enumeran los objetivos del *Focus Group*:

1. Conocer y comparar la visión sobre la gestión de riesgos documentales de los profesionales de gestión documental y disciplinas relacionadas⁵⁵, en función del perfil profesional, de manera individual y por grupos (A y B).
2. Analizar el grado de importancia que los profesionales dan a la gestión de riesgos en el campo de la gestión documental a partir de las opiniones de los participantes de ambos grupos, de manera individual, en función del perfil, y entre grupos (A y B).
3. Identificar riesgos documentales desde la experiencia de los distintos profesionales participantes.

⁵⁵– Disciplinas relacionadas engloba aquellas que, por su campo de actividad, contribuyen a la implantación de SGD junto con los especialistas en gestión documental. Pueden ser: especialistas en tecnologías de la información, en derecho administrativo, en gestión por procesos, administración electrónica, entre otras.

4. Comparar los resultados de la identificación de riesgos documentales entre ambos grupos para estudiar posibles semejanzas o diferencias.
5. Recabar información, a través de la opinión y perspectiva de los distintos participantes, sobre la relación existente entre la gestión de riesgos documentales y el objetivo de rendir cuentas de las administraciones públicas.
6. Analizar las respuestas obtenidas sobre la relación entre la gestión de riesgos documentales y el objetivo de rendir cuentas de las administraciones públicas.

Uno de los objetivos principales es el de poder comparar las respuestas entre ambos grupos, en los cuales participan profesionales con perfiles distintos. Su composición variada puede arrojar dos posibles resultados: que ambos grupos aborden el tema de manera similar o que cada grupo aborde el tema desde una perspectiva diferente.

Para facilitar la comparación se formulan las mismas preguntas a ambos grupos.

4.2 Composición de los grupos

Se opta por la realización de dos *Focus Groups* con participantes de perfiles distintos, con la finalidad de poder comparar las respuestas e ideas surgidas durante el debate, ya que se considera que variar la composición entre ambos grupos mejora la dinámica dentro de cada uno de ellos y, además, crea la oportunidad de comparaciones útiles entre grupos (Morgan 1998a, p. 59).

Se considera oportuno, para el primer grupo, reunir a una serie de expertos en gestión documental y archivos de diferentes sectores y tipos de archivo, que se encuentren en activo a día de la realización del *Focus Group* y que tengan una trayectoria considerable en el campo de la gestión documental.

Se considera oportuno, para el segundo debate, reunir a un grupo multidisciplinar de perfiles que hayan trabajado de manera regular en equipos de diseño, implantación y mantenimiento de sistemas de gestión documental en las organizaciones, ya sea como trabajadores en las mismas o como consultores externos. La composición de ambos grupos se describe a continuación.

Grupo A

Técnicos expertos en gestión documental, que están en activo y han trabajado en distintos proyectos de diseño, implantación y mantenimiento de sistemas de gestión documental. Se trata de disponer de un grupo con participantes de perfiles distintos, pero con trayectorias similares. El grupo A está formado por:

1. Un representante de la Generalitat de Catalunya, concretamente de la Dirección General de Archivos, Museos y Bibliotecas⁵⁶. Se trata de la unidad directiva que tiene como finalidad impulsar la gestión documental en el conjunto del sector público catalán. Una de sus funciones más destacadas es la relacionada con el impulso del acceso y la valoración de la documentación, que se realiza mediante la dirección y soporte técnico a la acción de la Comisión Nacional de Acceso, Valoración y Selección Documental (CNAATD, por sus siglas en catalán).
2. Un representante de un archivo de una diputación. Las diputaciones tienen un carácter territorial limitado a su provincia y su función principal es la de gestionar sus intereses económico-administrativos. Como órganos de la administración local, junto con los ayuntamientos, son las administraciones más próximas y más conocedoras de las realidades territoriales y de las necesidades de las personas. Las funciones básicas de un archivo de diputación son las de custodiar, conservar, organizar y seleccionar la documentación generada por dicha diputación desde el año de su creación.
3. Un representante de un archivo comarcal. Los archivos comarcales tienen las funciones de conservación, tratamiento y difusión del patrimonio documental desde su entorno de procedencia originaria. También tienen la obligación de ofrecer servicios complementarios y de soporte a otros archivos de su ámbito territorial, especialmente servicios de asistencia en los archivos municipales de los municipios de menos de 10.000 habitantes (Parlamento de Cataluña 2001, p. 34). Este tipo de archivos, contribuyen al equilibrio territorial en el ámbito del patrimonio mediante toda la actividad cultural que se deriva, que es muy diversa. Además, al conservar los documentos de la administración de la Generalitat de Cataluña en su territorio, contribuyen a su eficacia administrativa y a su transparencia⁵⁷.
4. Un representante de un archivo judicial. Se entiende por archivo judicial tanto el conjunto orgánico de documentos judiciales como el lugar en el que quedan debidamente custodiados y clasificados los documentos judiciales. Estos archivos ofrecen un servicio de préstamo y consulta al órgano judicial del cual custodian la documentación⁵⁸.
5. Un representante de una empresa pública. Se entiende como tal, aquella que es propiedad del Estado, sea esta estatal, municipal o de cualquier otro estrato administrativo, y ya sea de modo total o parcial. La empresa pública incluida en este estudio, dentro de su organización y estructura, está compuesta por distintos órganos administrativos de carácter plurititular, formados por diferentes miembros con funciones atribuidas de gobierno y decisión, propuesta, asesoramiento, control y participación.

⁵⁶ – Para más información se puede consultar la página web de la Dirección General: http://cultura.gencat.cat/ca/departament/estructura_i_adreces/organismes/dgpc/temes/arxius_i_gestio_documental/gestiodocumental/ (consultado el 16/07/2017).

⁵⁷ – Para más información se puede consultar la página web de la Red de Archivos Comarcales: <http://xac.gencat.cat/ca/inici/> (consultado el 15/07/2017).

⁵⁸ – Para más información se puede consultar la página web de la Red de Archivos Judiciales de Cataluña: http://administraciojusticia.gencat.cat/ca/seccions_rematiques/arxius/ (consultado el 16/07/2017).

6. Un representante de un archivo municipal. Estos se definen como archivos de las municipalidades o de otras autoridades de gobierno local. Son los archivos más numerosos en el territorio, puesto que ya en la Ley 10/2001, de 13 de julio, de archivos y documentos, en su artículo 31.1, se incluye la obligatoriedad de que “*los Ayuntamientos de los municipios de más de diez mil habitantes y las Diputaciones Provinciales deben tener un archivo propio*” (Parlamento de Cataluña 2001, p. 35). Estos organismos definen, implantan y mantienen el sistema de gestión de la documentación administrativa en fase activa y semiactiva, y gestionan y conservan la documentación en fase semiactiva y fase histórica.
7. Un representante de un archivo universitario. Los archivos universitarios están constituidos por el conjunto de documentos generados, reunidos o recibidos por los diferentes órganos de una universidad en el desarrollo de sus funciones y actividades. Se entiende igualmente por archivo universitario el servicio especializado en la gestión, conservación y difusión de los documentos con finalidades administrativas, docentes, investigadoras y culturales de las universidades.

Todos los participantes están trabajando en archivos que forman parte del Sistema de Archivos de Cataluña (SAC)⁵⁹. Este se define, según el artículo 16 de la Ley 10/2001, de 13 de julio, de archivos y documentos, como el conjunto de órganos de la administración y archivos que, con normas y procedimientos, garantizan de acuerdo a sus valores, la gestión, la conservación, la protección, la difusión correctas de la documentación de Cataluña, y el acceso a esta documentación (Parlamento de Cataluña 2001, p. 25). Los archivos que forman parte del SAC deben aplicar el sistema de gestión de la documentación que corresponda a los fondos que conservan, de acuerdo a las normas técnicas básicas fijadas por la Generalitat de Cataluña, también deben disponer de personal suficiente, disponer de las instalaciones necesarias para garantizar la presentación de los fondos documentales y tener unas instalaciones y un horario de apertura al público que permita el acceso.

En este primer grupo se cuenta con expertos, reconocidos en la profesión archivística y de gestión documental, que están trabajando en los tipos de archivos de la administración pública enumerados, con puestos de responsabilidad, así como con poder de decisión. Se pretende representar los distintos tipos de archivos, eso sí, sin olvidar el grado de semejanza de los perfiles para favorecer la comodidad y el debate dentro del grupo. Se cuenta con 4 hombres y 3 mujeres, de edades comprendidas entre los 37 y los 54 años. Todos los participantes cuentan con una experiencia en el ámbito de la gestión documental de entre 10 y 27 años⁶⁰. Con relación al tiempo de trabajo en el tipo de archivo concreto por el cual son convocados al debate, los años de experiencia van desde los 6 a los 11. Se aprecia, por tanto, mayor experiencia en el ámbito general de la gestión de documentos y archivos y menor en el tipo de archivos en los que están especializados por su trayectoria profesional (ver Figura 22).

⁵⁹ – Para más información sobre el SAC se puede consultar su página web: http://cultura.gencat.cat/ca/departament/estructura_i_adreces/organismes/dgpc/temes/arxius_i_gestio_documental/sistema_d_arxius_de_catalunya_sac/ (consultado el 4/11/2017).

⁶⁰ – El representante del archivo judicial y el representante del archivo universitario no facilitaron datos sobre sus años de experiencia ni sobre su formación.

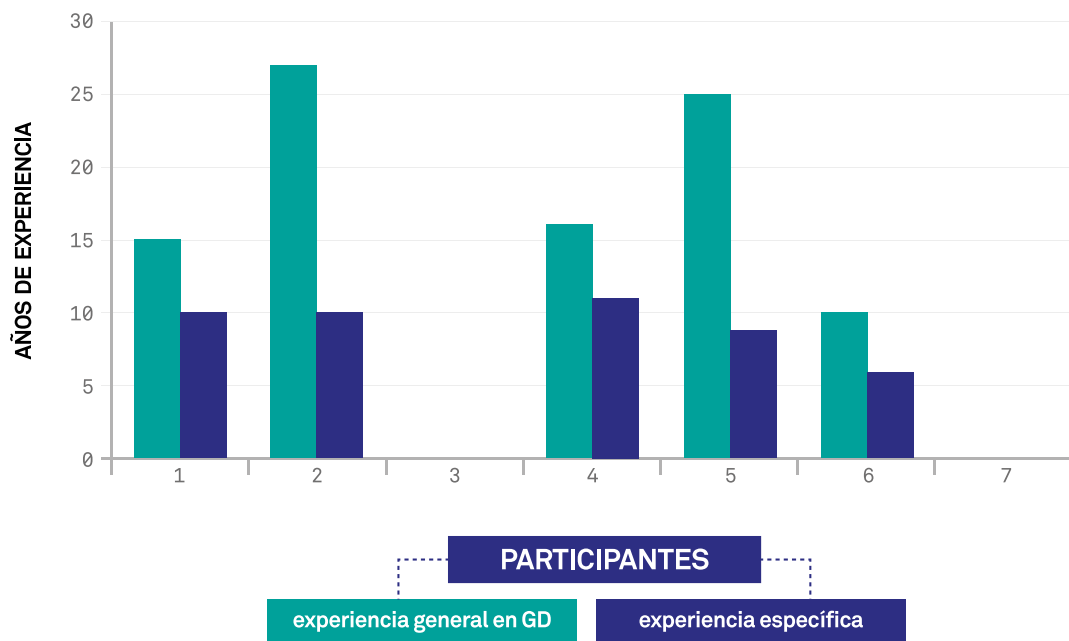


Figura 22 - Comparativa entre años de experiencia para el Grupo A (elaboración propia).

Con relación a la formación, todos los participantes cuentan con estudios universitarios y todos ellos han realizado estudios de máster y de postgrado (ver Figura 23). Destacan los participantes 1 y 2 con dos títulos de máster y el participante 1, con dos títulos de postgrado. En el grupo A no hay ningún participante con título de Doctor.

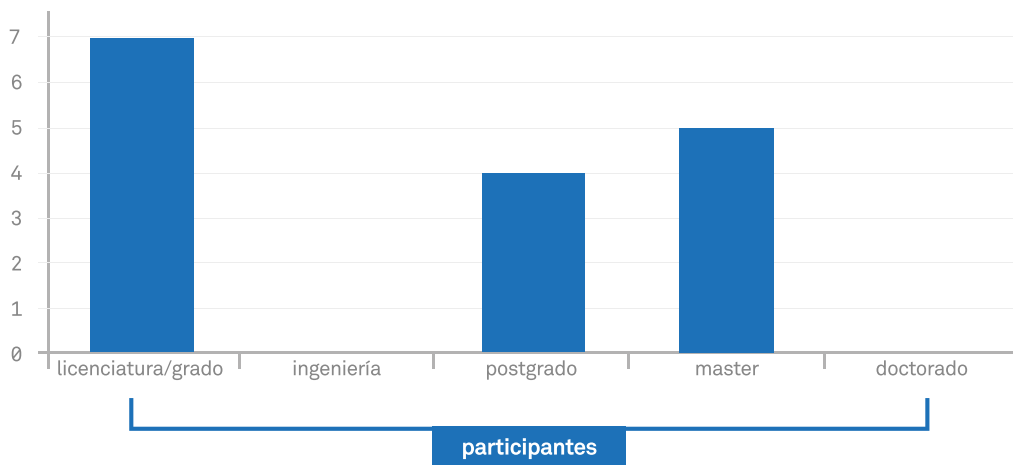


Figura 23 - Formación de los participantes del Grupo A (elaboración propia).

Es importante contar con participantes con cierto poder de decisión y responsabilidad en los centros de trabajo, ya que estos son quienes tienen una mayor visión global de la gestión documental en las organizaciones. Interesa este perfil, además, porque se cuenta con una amplia trayectoria profesional al haber desempeñado distintas funciones en centros de archivo a lo largo del tiempo y, por tanto, conocer la realidad del sector profesional.

Grupo B

Expertos de diferentes ámbitos que trabajan en proyectos de gestión documental. Este grupo es menos homogéneo a nivel técnico. Pese a ello, se cree oportuna esta selección multidisciplinar por corresponderse mayoritariamente con el equipo de trabajo que puede formarse en cualquier administración pública para liderar el diseño, implantación y mantenimiento de un sistema de gestión documental. De hecho, la homogeneidad de este grupo parte de la compatibilidad como equipo de trabajo. El grupo B está formado por:

1. Un consultor experto en Gestión Documental. Es importante contar con un especialista que trabaje desarrollando proyectos de gestión documental para la Administración Pública con una visión externa, puesto que actualmente muchas administraciones contratan consultorías para este tipo de proyectos.
2. Un experto en Prevención de Riesgos Laborales. En todas las administraciones se cuenta con una persona responsable de riesgos laborales, pero no por ello se amplía el uso de esta metodología a la prevención de otro tipo de riesgos. Interesa este perfil para contrastar metodologías y conocer las posibilidades de establecer sinergias y puntos de encuentro.
3. Un experto en Derecho Administrativo y Administración Electrónica. El derecho administrativo es la base para la actuación de las administraciones, que cada vez más están viviendo la transformación digital.
4. Un experto en Tecnologías. También en línea con la transformación digital es necesario contar con un experto en nuevas tecnologías en cualquier equipo de implantación de sistemas de gestión documental, ya que los sistemas cada vez más serán electrónicos. Sea el soporte mayoritario el papel o el electrónico, en todas las administraciones se trabaja con diferentes aplicaciones informáticas que es necesario conocer y gestionar adecuadamente.
5. Un experto en el área de Procesos. Para que la gestión de las administraciones sea sistemática se incorporan expertos en organización y procesos. Estos profesionales se encargan de diseñar y mejorar los flujos de información, los flujos documentales, así como los circuitos administrativos necesarios para el buen funcionamiento de organismos públicos.
6. Un experto del área de Archivo. No puede faltar un archivero en el equipo multidisciplinar, puesto que el tema central es la gestión de documentos. De este modo, se cuenta con la visión externa (del consultor) así como con la visión interna de un experto en gestión documental.

En este segundo grupo se cuenta, por tanto, con expertos de distintos ámbitos. El objetivo es disponer de un equipo multidisciplinar de expertos con los que, en una situación normal, se contaría para la implantación de sistemas de gestión documental en cualquier administración pública.

El grupo está compuesto por 4 hombres y 2 mujeres, con edades comprendidas entre los 48 y los 57 años. Todos los participantes, excepto el experto en prevención de riesgos laborales, cuentan con más de 10 años de experiencia en el campo de la gestión de documentos y archivos. En cuanto al ámbito de especialización por el que son convocados a participar en el debate, el mínimo es de 9 años, frente a un máximo de 32 años de experiencia en dichos ámbitos. El participante con menor experiencia es el especialista en procesos y el participante con mayor experiencia es el consultor en gestión documental. Los demás participantes cuentan con entre 15 y 20 años de especialización. Esta información contrasta con la experiencia del Grupo A, en el que los años de especialización son menores que los años dedicados a la gestión de documentos y archivos. En el Grupo B esta tendencia se invierte, y la especialización es mayor (ver Figura 24).

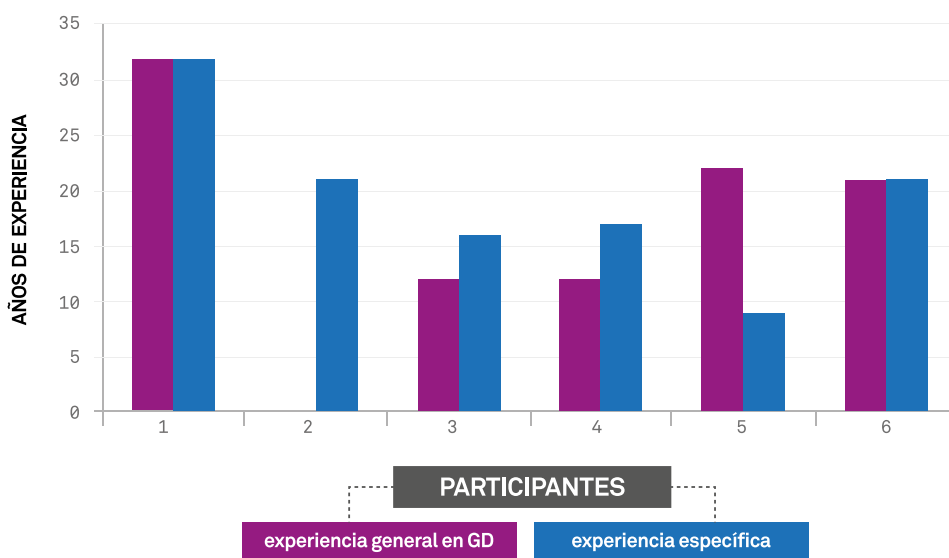


Figura 24 - Comparativa entre años de experiencia para el Grupo B (elaboración propia).

Con relación a la formación de los participantes, todos cuentan con educación universitaria superior (ver Figura 25). Además, el participante experto en prevención de riesgos laborales es Doctor en Prevención y Seguridad Integral. A su vez, los participantes 5 y 6 han iniciado estudios de doctorado, sin haberlos finalizado. Los participantes 1, 5 y 6 han cursado postgrados de especialización en administración electrónica, archivística y documentación, archivos y técnicas de gestión, y gestión de documentos electrónicos. El participante 4 es Ingeniero en Informática.

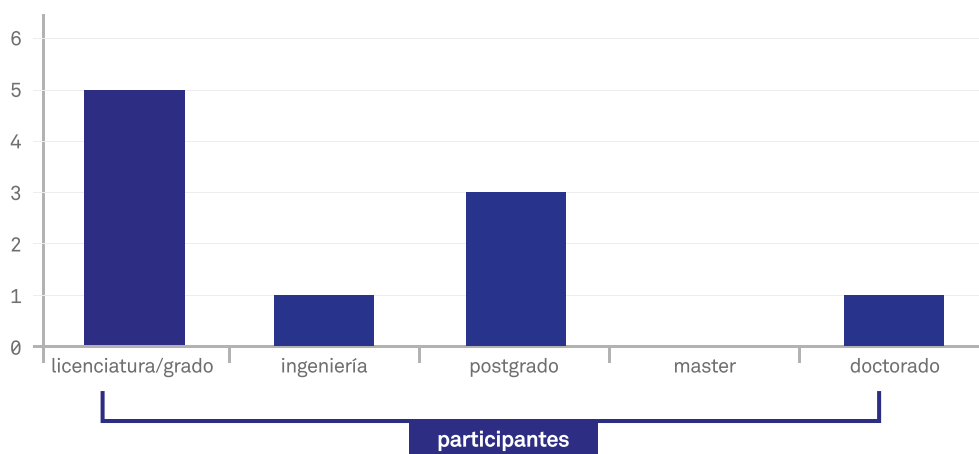


Figura 25 - Formación de los participantes del Grupo B (elaboración propia).

Preguntas

Para la selección y diseño de las preguntas se parte de la base de que no todas tienen la misma importancia ni todas deben ser iguales. Según Krueger (Morgan *et al.* 1998), se utilizan diferentes tipos de preguntas en las diferentes fases de un *Focus Group* y cada pregunta tiene un propósito diferente. Estos tipos son:

- Preguntas de apertura (A): la finalidad es que los participantes se conozcan y se sientan conectados. Ayuda a que todos puedan hablar por primera vez en el debate. No deben ocupar mucho tiempo.
- Preguntas introductorias (I): la finalidad es empezar con el tema de discusión. Se introduce el tema general de estudio y se proporciona a los participantes la oportunidad de reflejar sus experiencias y conexiones con el tema.
- Preguntas de transición (T): la finalidad es mover la conversación hacia las preguntas clave, que conducirán el estudio, pero de manera suave y no forzada.
- Preguntas clave (C): la finalidad es obtener conocimiento en las áreas centrales del tema de estudio. Estas serán las que moverán el estudio y suelen ser entre 2 y 5.
- Preguntas de finalización (F): la finalidad es ayudar al investigador a llevar el debate a su conclusión. Dentro de esta categoría hay varios tipos: las preguntas que permiten que los participantes den su opinión

última sobre las áreas críticas, las preguntas que sirven para resumir los temas tratados y asegurarse de que los participantes tienen la misma visión de cómo ha ido el debate, y las preguntas finales propiamente, cuyo propósito es asegurarse de que los aspectos críticos no se han pasado por alto.

Según la fase del debate, será más útil la utilización de unas u otras, además de permitir modular el tiempo de manera que los participantes vayan introduciéndose en el debate paulatinamente. Las preguntas que se formulan se enumeran a continuación, incluyendo el tipo de pregunta, así como la previsión de tiempo para cada una de ellas, en función del tipo:

1. (Apertura) Nombre y tipo de archivo en el que trabaja, para el grupo A; nombre y campo de experiencia, para el grupo B. Esta es la única pregunta que varía ligeramente entre grupos, debido a la diferencia de perfiles seleccionados. (Hasta el minuto 7)
2. (Introductoria) ¿Habéis oído hablar alguna vez de la gestión de riesgos documentales? ¿En qué contexto? (Del minuto 7 al minuto 20)
3. (Transición) ¿Podéis enumerar diferentes riesgos documentales (dos o tres principales) que afecten a la organización en la que trabajáis o con la que colaboráis? (Del minuto 20 al minuto 40)
4. (Clave) ¿Cómo definiríais la gestión de riesgos documentales? (Del minuto 40 al minuto 50)
5. (Transición) ¿Cuáles creéis que pueden ser los beneficios de la gestión de riesgos documentales para el correcto funcionamiento de un SGD? (Del minuto 50 al minuto 60)
6. (Clave) ¿Creéis que la gestión de riesgos documentales puede tener alguna repercusión en el proceso de rendición de cuentas de las administraciones públicas? ¿Cuál? (Del minuto 60 al minuto 75)
7. (Clave) ¿En qué momento/fase del proceso creéis que debería llevarse a cabo la identificación y análisis de riesgos documentales? (De 75 a 80 minutos)
8. (Finalización) De lo hablado anteriormente, ¿qué consideráis que es lo más importante? (Del minuto 80 al minuto 85)
9. (Finalización) ¿La sensación al finalizar el debate es positiva o negativa? (Del minuto 85 del minuto 90)

Se estima un tiempo concreto para cada una de las preguntas, en función de su tipo (de inicio del debate, de introducción, de transición, clave, o de finalización). Esto debe facilitar el ritmo de la conversación y conseguir incluir todas las preguntas en el límite de tiempo establecido de 90 minutos.

En la siguiente tabla se puede ver la correlación entre las preguntas y los objetivos planteados para el *Focus Group* (ver Figura 26). La pregunta 1 no se corresponde con ningún objetivo por ser el modo de introducción y presentación entre los participantes. Cabe mencionar que la práctica totalidad de los participantes de ambos grupos ya se conocen a nivel profesional, con lo que la presentación debe contribuir a romper el hielo de la conversación, así como a proporcionar algo más de información sobre cada uno de ellos. Se opta por el uso de un lenguaje coloquial para facilitar el desarrollo del debate.

PREGUNTAS	OBJ. 1	OBJ. 2	OBJ. 3	OBJ. 4	OBJ. 5	OBJ. 6
1						
2	X	X				
3			X	X		
4	X	X		X		
5	X	X				X
6					X	X
7		X	X		X	X
8	X	X				
9	X	X				

Figura 26 - Correlación entre preguntas y objetivos para el Focus Group (elaboración propia).

Cuestiones éticas

Un *Focus Group* inevitablemente conlleva compartir información (en ocasiones sensible) y, por tanto, la privacidad es uno de los puntos éticos centrales y críticos en esta técnica de investigación. Una de las cuestiones principales en esta metodología es la protección de la privacidad de todos los participantes. Para ello, se elaboró un documento de Consentimiento Informado (ver Anexo A) que todos debieron aceptar y firmar antes de iniciar el debate. En este documento se deja constancia de la importancia y el compromiso, por parte de todos, de la preservación de la privacidad propia y de los demás. También a la hora de analizar los debates y exponer los resultados se tiene en cuenta este compromiso ético, manteniendo la confidencialidad de los participantes.

4.3 Participación

Debido a las distintas procedencias de los participantes y la distancia física que los separa, para ambos debates se les permite escoger entre participación presencial o a través de videoconferencia. Esta es una de las posibilidades del *Focus Group* para facilitar la asistencia de todos los expertos seleccionados.

Para la realización de la videoconferencia se decide utilizar la herramienta *Cisco WebEx Meetings*⁶¹, que permite reunir a un número amplio de personas mediante conexión a través de internet. Esta aplicación no requiere de la instalación de programas adicionales ni de la suscripción o pago para el uso, sino que cualquier persona puede unirse a una reunión de manera gratuita, sin necesidad de registrarse ni tener que aportar datos personales o de contacto. Es un método sencillo para poder conectar a todos los participantes en una misma sala y a la misma hora, además de permitir la grabación de la sesión. Esto, además, ayuda a la hora de analizar los debates y extraer las conclusiones.

Del grupo A, tan solo uno de los participantes opta por la videoconferencia, se corresponde con el 14,3 %. Del grupo 2, el 100 % de los participantes optan por la videoconferencia, situación que confirma la importancia de haber contado con esta posibilidad para permitir la realización de los debates. Además, da una idea de las ventajas de utilizar las nuevas tecnologías en la investigación científica, ya que sin este tipo de recursos no habría resultado posible realizar ninguno de los debates previstos con la misma calidad de participación.

4.4 Análisis y Resultados

El análisis empieza con una escucha activa del debate. Se combinan diferentes elementos de la investigación cualitativa y, además, se añade la complejidad de la interacción del grupo (Krueger 1998, p. 20). Esto se trabaja proporcionando conexión de vídeo y audio para todos los participantes del debate, y eso posibilita que en el *Focus Group* que se desarrolla 100 % *online*, los asistentes puedan verse entre sí y ver a la moderadora. Del mismo modo, también le permite a ella observar las reacciones e interacciones de los participantes. En el debate del grupo A (en el que hay un 14,3 % de asistencia virtual) también se facilita que los participantes presenciales puedan ver e interactuar con el participante virtual, y viceversa. De este modo, no se pierden las reacciones normales de un debate, puesto que todos los participantes están conectados con voz e imagen, como si hubiesen estado en una misma sala.

⁶¹ – *Cisco WebEx Meetings* permite la realización de videoconferencias a través de su página web, de manera gratuita y con una alta calidad de audio y vídeo. Permite la compartición de archivos y de la pantalla de cualquiera de los invitados a la videoconferencia, haciendo más interactivas las reuniones. Se puede consultar más información en: <https://www.webex.es/> (consultado el 01/05/2017).

4.4.1 Análisis del debate – Grupo A

Duración

El debate se realiza el 17 de mayo de 2017 y tiene una duración total de 90 minutos.

Asistentes

Del listado inicial de participantes, finalmente no pueden asistir ni el representante de la diputación ni el representante del archivo universitario, que excusan su presencia por diferentes motivos. Esto proporciona una participación del 71,42 %, y la lista final queda en cinco participantes, con los siguientes perfiles:

1. Un representante de una Administración Autonómica, concretamente de la Dirección General de Archivos, Museos y Bibliotecas de la Generalitat de Catalunya (participante 1). Este participante asiste a los primeros 40 minutos del *Focus Group*, excusando su participación en el debate restante.
2. Un representante de un Archivo Comarcal (participante 2).
3. Un representante de un Archivo Judicial (participante 3).
4. Un representante de una empresa pública (participante 4).
5. Un representante de un Archivo Municipal (participante 5).

Descripción del debate

Nº PARTICIPANTE	TIPOLOGÍA DE ARCHIVO QUE REPRESENTA
1	administración autonómica
2	archivos cormarcales
3	archivos judiciales
4	empresa pública
5	archivos municipales

Figura 27 - Tabla de participantes para el Grupo A (elaboración propia).

Para llevar a cabo el análisis, a continuación, se describen las respuestas de los participantes a cada una de las preguntas, siguiendo el mismo orden de realización de las mismas dentro del *Focus Group*. No se cree oportuna la transcripción exacta del debate para poder facilitar la lectura y comprensión de la conversación.

Para dar comienzo, la moderadora explica el tema de debate, los objetivos del *Focus Group* de manera general, así como la dinámica a seguir. Hecho esto, se da paso a los participantes para que respondan a la pregunta número 1.

1. Nombre y tipo de archivo en el que trabaja, para el grupo A

Los participantes realizan, cada uno, su presentación de manera individual, indicando su nombre, su experiencia laboral y su actual lugar de trabajo. Cabe destacar que todos ellos se conocen previamente. Esto facilita la fluidez en el debate desde el inicio, y proporciona un marco cómodo para la conversación.

2. ¿Habéis oído hablar alguna vez de la gestión de riesgos documentales? ¿En qué contexto?

Todos los participantes han oído hablar de la gestión de riesgos asociada a la gestión documental. Los contextos son distintos, así como también la identificación que hacen de los objetivos y beneficios de llevar a cabo la gestión de riesgos en sus organizaciones. Se explican sus respuestas a continuación de manera descriptiva, siguiendo el orden de participación.

El representante de la empresa pública (en adelante, participante 4) dice que oyó hablar por primera vez del tema a través de los estándares internacionales (normas ISO). Concretamente, hace alusión a la norma ISO 15489 del año 2001 y a su actualización del año 2016. Explica que, desde su punto de vista, existe una inconsciencia por parte de las administraciones públicas sobre lo que puede llegar a pasar si no se controlan y gestionan adecuadamente los documentos. Relaciona el conocimiento de los riesgos documentales con la toma de decisiones informada en las organizaciones y con el mantenimiento de las garantías de los ciudadanos por parte de las administraciones, así como la garantía de derechos y deberes tanto de ciudadanos como de administraciones. Introduce, además, el concepto de documentos esenciales como una prioridad a la hora de identificar y prevenir riesgos.

El representante de la Administración Autonómica (en adelante, participante 1) dice que oyó hablar por primera vez del tema en relación con el servicio que proporciona la administración al ciudadano, gracias a una adecuada gestión documental. Comenta la casuística de los archivos históricos, manifestándose totalmente de acuerdo con los comentarios del participante 4. Afirma que, si uno de los principales servicios de un archivo es el de proporcionar acceso a la información, pero no se dispone de un sistema de gestión documental implantado (contando con que la documentación esté descrita y clasificada de manera adecuada), existe un riesgo muy alto de no cumplir con este servicio al ciudadano. Introduce la idea de transformación digital con relación a los riesgos de preservación y accesibilidad de los objetos digitales, achacando la precaria situación actual a una falta de inversión y exigencia en los archivos históricos de administraciones públicas.

El representante de Archivos Comarcales (en adelante, participante 2) se manifiesta de acuerdo con lo presentado por el participante 1 con relación a los archivos históricos y sus problemáticas y riesgos actuales. Comenta que, en los archivos comarcales trabajan, no solo con documentación histórica, sino también con semiactiva (antigüedad a partir de 15 años). Dice que la primera vez que oyó hablar de riesgos fue en relación con la automatización de procesos de gestión documental. Si bien es cierto que en los procesos manuales también existen, afirma que trabajar con sistemas automatizados de gestión documental implica mayores riesgos (adquisición y utilización del *software*, trabajo de los flujos de información, entre otros), más allá de la preservación digital comentada por el participante 1. Menciona, además, el importante papel de la administración pública como garante de derechos ciudadanos a través, entre otras obligaciones, de la transparencia. Añade que las administraciones están obligadas a automatizar la publicación de información de manera periódica por la legislación en materia de transparencia y acceso a la información (automatizar la gestión documental, al fin y al cabo, afirma).

El representante de Archivos Judiciales (en adelante, participante 3) dice que oyó hablar por primera vez del tema en unas jornadas de archivos y seguridad⁶². Habla de varios aspectos. Por un lado, hace alusión a la automatización de procesos, y la relaciona con situaciones de riesgo y alude, como un factor de riesgo añadido, a la falta de profesionales capacitados (archiveros y gestores de documentos) en las administraciones públicas. También introduce la idea de la posibilidad de los ataques⁶³ desde fuera de las organizaciones, y hace mención a los costes que supondría perder las horas de trabajo invertidas en un proyecto por culpa de un ataque informático. Por último, comenta que la externalización de servicios (como la custodia, la gestión o la transformación digital) le provoca una sensación de falsa seguridad, debido a que estas empresas también pueden sufrir ataques o incluso quebrar.

El representante de Archivos Municipales (en adelante, participante 5) relaciona los riesgos documentales con los riesgos generales de cualquier negocio, entendiendo el término en su sentido más amplio. Para él, los riesgos existen incluso antes de iniciar cualquier proceso y antes de crear cualquier documento, extendiéndose posteriormente a la tramitación. Los riesgos no son únicamente de seguridad o de gestión o recuperación de la información, sino que los riesgos son globales y generales a la organización. Incluye la necesidad de incorporar equipos multidisciplinares (como, por ejemplo, servicios jurídicos, archiveros y técnicos) y también hace alusión a la falta de profesionales especializados en las administraciones públicas como un factor de riesgo. Este participante no menciona en qué contexto oyó hablar de riesgos documentales por primera vez.

Una idea general que comparten todos los participantes es la de la falta de consciencia con relación a los riesgos documentales existentes en las administraciones públicas. Todos coinciden, además, en la importancia de la gestión de los riesgos documentales para la transparencia y para garantizar los derechos de los ciudadanos a través de la gestión documental.

⁶²– Se refiere a las VIII Jornadas de Estudio y Debate organizadas por la Asociación de Archiveros de Catalunya bajo el título “Archivos seguros: ¿Cómo protegemos los documentos?” en mayo del año 2008.

⁶³– Cabe mencionar que días antes de llevar a cabo este debate se produjo un ataque informático masivo (*WannaCry*) que afectó a muchas organizaciones (públicas y privadas) entre las que se vieron afectadas algunas de las administraciones en las que trabajaban los participantes del focus group.

3. ¿Podéis enumerar diferentes riesgos documentales (dos o tres principales) que afecten a la organización en la que trabajáis o con la que colaboráis?

Para el participante 1, un riesgo importante es no trabajar en equipo o no disponer de expertos en gestión documental en los equipos que implantan sistemas de gestión documental. Esto es así, ya que implantar este tipo de sistemas sin profesionales especializados puede ocasionar riesgos en la medida en que los procesos no se diseñen de manera adecuada. Afirma que siempre se van a encontrar con intereses empresariales a la hora de trabajar que condicionan ciertas decisiones, pero opina que si el equipo de trabajo está unido, se pueden conseguir los objetivos de manera adecuada.

El participante 4 explica el riesgo que supone la documentación que no se controla, con relación a cómo llegan los documentos al archivo y a través de qué nuevos canales, que ocasionan un riesgo importante de pérdida de información. También para él es importante el riesgo de replicar documentos de manera no autorizada, lo que puede ocasionar filtraciones hacia el exterior y un descontrol de versiones. Incluye, además, la “patrimonialización” de los documentos, explicando que muchas veces los trabajadores públicos creen que los documentos y la información con la que trabajan son suyos (de su propiedad) y eso ocasiona una mala gestión de los mismos.

El participante 3 diferencia entre riesgos endógenos y exógenos. Los primeros los vincula al modo en que se funciona dentro de las organizaciones, ya sea con trabajadores o proveedores, y los relaciona con factores como la ética, la inconsciencia u otros aspectos que pueden derivarse tanto de la manipulación humana como de automatismos en procesos. También habla sobre fugas de información, ya sean provocadas desde dentro de la organización o desde fuera. Este participante afirma que los ataques informáticos cada vez ocurren con más frecuencia y se deben habituar a convivir con este riesgo. Incluye en la lista de riesgos la falta de mantenimiento de los sistemas de gestión de documentos. Comenta que muchas veces se ponen todos los esfuerzos en la implantación del sistema y, una vez implantado, se olvida su mantenimiento y se deja de disponer de los recursos necesarios. No se tiene en cuenta que se trata de un proceso continuo.

El participante 4, a raíz de lo mencionado por el participante 3, añade la falta de formación, o la mala formación, como riesgos importantes relacionados, precisamente, con el mantenimiento de los sistemas de gestión documental. Para trabajar con el sistema implantado, los trabajadores necesitan haber recibido formación al respecto.

El participante 2 habla de la filosofía de las organizaciones y enumera la gestión docucéntrica y la datacéntrica. Comenta que muchas veces se confunde en cómo se está trabajando en cada organización y, añade, que en las administraciones públicas se está funcionando, mayoritariamente, de manera datacéntrica, y el rol de los archiveros y gestores de documentos está quedando en un plano secundario a nivel de responsabilidades, ya que, según él, el 90 % del sistema se controla por expertos informáticos, y queda, además, fuera del campo de conocimiento y experiencia de los profesionales de la gestión documental. Para el participante 2, el riesgo más importante son las inconsistencias del sistema y la opacidad en el funcionamiento de los mismos. También incluye el concepto de honestidad, y la mala fe y mala praxis de las personas como riesgos, en contraposición.

El participante 5 se muestra de acuerdo con el participante 2 en la importancia de la gestión de datos, más que de documentos. Para él, lo que de verdad importa no es la manifestación (o visualización) de la información en forma de documento, sino los datos que permiten la gestión y de los que se extrae la información.

Una cuestión fundamental de prevención para el participante 4 es la definición y la identificación de los documentos esenciales. Al tener identificados los documentos esenciales de una organización, se pueden focalizar las medidas de prevención y tratamiento de los riesgos y se puede dar una mejor, y más efectiva, respuesta en caso de suceder un evento negativo. El resto de participantes se suman a esta opinión y así lo manifiestan, aunque el participante 3 añade que, describir ciertos documentos como esenciales y darles mayor importancia, también puede suponer un riesgo, ya que son más fácilmente identificables, localizables y, por tanto, susceptibles de sufrir ataques, robos, manipulaciones u otras casuísticas. Su explicación está enfocada a documentos en formato papel.

Un punto de encuentro entre todos los participantes es la existencia de un mayor riesgo en la gestión de documentos electrónicos que en la de documentos en papel: desde su generación, la realización de copias, la transmisión o envío del documento o el control de versiones. Otro aspecto de concordancia entre los participantes es la incorporación de las nuevas tecnologías, no solo como instrumentos al servicio de la gestión documental, sino también con relación a nuevos formatos (como formatos no controlados, redes sociales o datos abiertos) y su conservación a largo plazo. Esto también supone un riesgo importante.

Otro aspecto en el que están de acuerdo los participantes es en que uno de los riesgos principales es, precisamente, la inexistencia de sistemas de gestión documental implantados en las administraciones.

4. ¿Cómo definiríais la gestión de riesgos documentales?

Para el participante 2, la gestión de riesgos documentales es equivalente a definir un modelo de datos. La gestión de riesgos está muy normalizada, se dispone de aplicaciones informáticas capaces, de metodología y de personas, pero no de modelos de datos definidos y documentados. Este participante, además, relaciona la gestión de riesgos documentales con la honestidad. Para él, no solo es una cuestión de seguridad, sino que también se incluye la gestión del cambio en este tipo de proceso. Esta debe ayudar a adaptarse a los cambios en las aplicaciones y en la manera de trabajar, siempre sin olvidarse de la documentación en papel.

Para el participante 4 hay un riesgo elevado en la conservación del papel porque todo se tiende a digitalizar. Los documentos en papel quedan en un segundo plano.

Para el participante 5, la gestión de riesgos empieza por un trabajo en equipo. Opina que, más allá de la seguridad, el riesgo básicamente se encuentra al principio del sistema de gestión documental. Si este no está bien definido e implementado se preserva documentación sin sentido, como por ejemplo copias y documentos de soporte. Por tanto, para él los riesgos van más allá de la seguridad y se encuentran en todas las fases de la gestión documental. Todos están de acuerdo con el participante 5.

El participante 4 habla sobre la inexistencia de políticas de gestión o de prevención de riesgos en las administraciones, empezando por la Generalitat de Cataluña. En esta línea, y para definir la gestión de riesgos documentales, menciona la importancia de identificar los documentos vitales e invertir en su integridad y preservación como

medida de prevención de riesgos. Según su punto de vista, cada administración debe tener identificados los documentos vitales o esenciales, siguiendo las normativas existentes y, de este modo, focalizar los recursos y esfuerzos en ellos. Afirma que, si la administración se preocupa de desarrollar una política de gestión de riesgos, identificando este tipo de documentos, es todo más fácil.

El resto de participantes manifiestan estar de acuerdo con lo explicado por el participante 4.

5. ¿Cuáles creéis que pueden ser los beneficios de la gestión de riesgos documentales para el correcto funcionamiento de un SGD?

El participante 3, antes de nada, opina que la gestión de riesgos puede ser muy beneficiosa para el posicionamiento de la profesión, convirtiendo a los gestores de documentos en fiscales o auditores. Para ello, hay que ser capaces de crear un nuevo perfil con formación actualizada.

El participante 2 cree que uno de los principales beneficios es eliminar el concepto de “fe” que las personas tienen en los documentos por el mero hecho de existir. Aplicar la gestión de riesgos al diseño y la implantación de sistemas de gestión documental es una oportunidad para repensar la profesión de una manera más transversal, una oportunidad de posicionamiento estratégico en las organizaciones.

El participante 4 cree que es positivo para la profesión y que abre un campo de trabajo, porque trabajar la gestión de riesgos documentales debe conseguir cambiar la visión de los profesionales de gestión documental, ya que no solamente hay que tener presente aquello relacionado directamente con la metodología archivística, sino que se debe ir más allá. Las fronteras entre profesionales quedan ligeramente desdibujadas y los gestores de documentos pueden aprovecharlo para posicionarse en las organizaciones, salir de su zona de confort y aprovechar la oportunidad para aportar nuevas soluciones desde la gestión de riesgos.

Se observa que los beneficios que identifican los participantes en el debate no se relacionan tanto con la gestión documental en sí, sino que se asocian los beneficios a nivel de la profesión. Todos los participantes visualizan la gestión de riesgos documentales como una gran oportunidad que mejoraría el posicionamiento de los gestores de documentos tanto en las organizaciones públicas como privadas.

6. ¿Creéis que la gestión de riesgos documentales puede tener alguna repercusión en el proceso de rendición de cuentas de las administraciones públicas? ¿Cuál?

Todos los participantes están de acuerdo en que la gestión de riesgos documentales puede afectar a los procesos de rendición de cuentas.

El participante 2 afirma que sí, que tiene una clara repercusión. Lo relaciona nuevamente con el concepto de

“fe” en el documento. Según su punto de vista, sin gestión de riesgos no se controla la honestidad y eso repercute directamente en la confianza de los ciudadanos en las instituciones.

El participante 5 añade que la gestión de riesgos debe ser una parte importante de la gestión de documentos, entendiendo la gestión de riesgos desde la gestión documental para la rendición de cuentas. Diferencia entre diversos actores que rinden cuentas, como los tecnólogos sobre aspectos de seguridad o los gestores de documentos sobre aspectos procedimentales. Cada rol con sus responsabilidades.

El participante 3 añade que un buen sistema de gestión documental es aquel que no se percibe. Aquel que funciona de manera correcta, transparente. Un sistema que previene los riesgos y las situaciones negativas, que no llegan a ocurrir, y por tanto el usuario no llega a percibir la inseguridad. Este participante explica que rendir cuentas, muchas veces, se vincula a actuaciones extraordinarias, situaciones que rompen con la honestidad de la administración. La normalidad es rendir cuentas sin que haya escándalos o sin que sea noticable. A este argumento, el participante 5 añade que, muchas veces, lo que percibe el usuario no se corresponde con la arquitectura tecnológica que sustenta el sistema y que esta no es tan segura como puede parecer.

El participante 1 añade que no gestionar los riesgos documentales, además, provoca retrasos en la tramitación y el ciudadano queda perjudicado. El cumplimiento del propio negocio de la administración (en el que se enmarca la rendición de cuentas) queda, de este modo, afectado por la mala gestión documental.

7. ¿En qué momento/fase del proceso creéis que debería llevarse a cabo la identificación y análisis de riesgos documentales?⁶⁴

El participante 4 afirma que, desde el inicio, en el momento de diseñar el sistema. Según su punto de vista, el sistema de negocio debe tener identificados los riesgos y, desde los responsables de gestión documental, se deben conocer también los riesgos documentales.

El participante 3 está de acuerdo en realizarlo desde el inicio, pero como un proceso iterativo, de manera continua y teniendo en cuenta cualquier pequeño cambio, para llevar a cabo de nuevo la identificación de riesgos.

El participante 5 añade que incluso debe hacerse la identificación de riesgos antes del inicio, en el momento de plantearse el proyecto de implantación del sistema de gestión documental, ya que existen riesgos inherentes al planteamiento de la implantación. Por ejemplo, falta de compromiso de las personas del equipo o no disponer de los perfiles profesionales necesarios para llevar a cabo el proyecto de implantación.

⁶⁴ – El participante 1 se excusó y abandonó el debate por un compromiso laboral. Se continuó con el resto de participantes.

El participante 3 se manifiesta de acuerdo con el participante 5 en cuanto a la realización cíclica o continua de la identificación de los riesgos.

Finalmente, todos están de acuerdo en realizar el proceso de manera cíclica, teniendo siempre en cuenta los cambios (por pequeños que sean) y siempre incluyendo la identificación de riesgos desde el inicio de cualquier implantación de sistemas de gestión documental. Cuanto antes se realice, mejores resultados se obtienen.

8. De lo hablado anteriormente, ¿qué consideráis que es lo más importante?

Para el participante 3, lo más importante es la formación de los profesionales de la gestión documental en lo que él considera un nuevo perfil, de gestor de riesgos documentales. Formar a las personas que deben acompañar este cambio en las organizaciones.

Para el participante 5, lo más importante es contar con el apoyo sin fisuras de la dirección dentro de la organización.

Para el participante 3, lo más importante son los cambios políticos, que no dejan trabajar a medio y largo plazo en las administraciones públicas. El resto de participantes se manifiesta totalmente de acuerdo con esta realidad. El participante 4 comenta que no se separan los proyectos políticos de los proyectos de la organización y esto impide avanzar con una línea estratégica clara que ayude a prevenir riesgos (con formación, con la adquisición de aplicaciones con visión a largo plazo, con políticas de preservación, entre otros).

El participante 2 añade que conviven en un mundo hipernormativizado (estándares internacionales, normas técnicas estatales, normas técnicas autonómicas) y esto hace que muchas veces no se tenga claro con qué instrumento es más adecuado trabajar en cada organización. Para él, falta un marco de referencia claro. El participante 4, en línea con lo expuesto por el participante 2, añade que un riesgo importante en su contexto es la terminología. Dentro de la propia profesión hay definiciones distintas de los mismos términos y esto crea una confusión que conlleva un riesgo importante a la hora de trabajar.

9. ¿La sensación al finalizar el debate es positiva o negativa?

Todos los participantes manifiestan haber acabado el debate con una sensación positiva y apuntan a seguir trabajando en esta línea, a incluir la gestión de riesgos en el día a día de la profesión archivística como un aspecto clave de la evolución de la profesión.

Conclusiones del debate

Cabe destacar que las palabras más mencionadas durante el debate son “seguridad” y “documentos esenciales”, seguidas por “inconsciencia”, “integridad” y “normalización”. Esto nos da una idea general de que para los archiveros que han participado en este debate la gestión de riesgos se relaciona mayoritariamente con la seguridad. Pese a que todos dejan claro, en varios puntos de la conversación, que no se trata exclusivamente de seguridad, lo cierto es que, ya sea de forma consciente o inconsciente, se relacionan ambos conceptos a lo largo del debate.

Otro punto importante es la necesidad de tener identificados y controlados especialmente los documentos esenciales de la organización, como medida preventiva, así como para asegurar la continuidad del negocio en caso de desastre. Los participantes constatan que muchas administraciones públicas no los tienen identificados y ni siquiera son conscientes de su importancia.

Un aspecto a destacar se relaciona con las respuestas de los participantes a la pregunta 5, donde identifican y dan más importancia a los beneficios de la gestión de riesgos para la profesión, en lugar de identificar los beneficios que esta puede tener en la propia gestión de documentos (objetivo de la pregunta). Quizás se debió insistir más desde la moderación para obtener una respuesta alineada a la pregunta, aunque esta desviación se considera positiva y una aportación al debate que, en principio, no estaba prevista. Los participantes están convencidos de que incluir la gestión de riesgos documentales en su práctica diaria tan solo puede aportar beneficios y esto es algo a destacar y a tener en cuenta en los resultados obtenidos del *Focus Group*. Por otro lado, estas respuestas se pueden relacionar con una falta de experiencia real con la metodología, que no permite realizar analogías, sean positivas o negativas, con los resultados que pueden llegar a obtenerse. Esto concuerda con la manifestación de todos los participantes del grupo A con relación a que no están trabajando con este método en su día a día.

En cualquier caso, se destaca que, para los participantes, la gestión de riesgos documentales es un elemento de empoderamiento para la gestión documental, para los gestores de documentos y para los archiveros. Esto es así porque les posiciona de un modo estratégico en la organización, debido a que se entiende la gestión de riesgos documentales como un modo de prevenir riesgos mayores en la organización, que pueden derivar en pérdidas económicas importantes, pérdida de prestigio o de clientes, entre otras consecuencias destacables.

Otro aspecto a recalcar es la inclusión en el debate de aspectos éticos y morales. Se menciona en pocas ocasiones, aunque se considera de vital importancia en la profesión, precisamente en línea con los objetivos de transparencia y rendición de cuentas. Sin una praxis basada en la ética es posible que muchos de los objetivos planteados no puedan alcanzarse. Este aspecto lo destaca sobre todo el participante 2, que lo relaciona con la honestidad. Se cree importante destacar esta cuestión y relacionarla con lo que se indica en el Preámbulo del Código Deontológico de los Archiveros Catalanes⁶⁵, en el que se afirma que “*en el ejercicio profesional, la toma de decisiones plantea frecuentemente dilemas éticos a los propios archiveros y, a veces, puede provocar conflictos de intereses entre los profesionales, y entre estos y la sociedad*”. No debe olvidarse que muchas veces quien gestiona información, está en una posición “privilegiada”, que en ocasiones puede llegar a generar dudas.

⁶⁵ – Tal y como se recoge en sus Disposiciones generales, “*el Código deontológico de los archiveros catalanes asume el Código de Ética profesional aprobado por la Asamblea General del Consejo Internacional de Archivos en la 13a sesión celebrada en Beijing (China) el 6 de septiembre de 1996, a la vez que lo desarrolla y lo adecúa a la realidad archivística y social de Cataluña.*”

Con relación a la identificación de riesgos, antes de nada, cabe mencionar que los participantes tienen la percepción de una mayor existencia de riesgos en entornos electrónicos que en entornos clásicos o en papel.

Destaca, también, que uno de los riesgos identificados sea precisamente la inexistencia de sistemas de gestión documental en las organizaciones. Es una situación que se da en algunas administraciones, así como también la de no contar con profesionales expertos en gestión documental, tal y como apuntan los participantes. Es algo destacable, puesto que implica la no disposición de una base desde la que trabajar. En cualquier caso, también puede ser positivo, en el sentido de que se puede empezar el diseño del sistema partiendo de cero y esto permite la inclusión de la metodología de gestión de riesgos en dicho sistema, complementándolo.

Esta reflexión debe relacionarse con la conformidad mostrada por todos los participantes acerca de que la gestión de riesgos documentales puede afectar de alguna manera a los procesos de rendición de cuentas. En esta reflexión se mencionan tanto aspectos positivos como negativos. Por ejemplo, se habla de confianza, transparencia y normalidad y, en contraposición, de inseguridad, retrasos en la tramitación o perjuicios para el administrado. Existe, por tanto, según los participantes, una afectación doble.

Es destacable que todos los participantes hayan oído hablar del tema y manifiesten la gran importancia de incluir la gestión de riesgos en la gestión documental en línea con la seguridad y la continuidad del negocio, pero, en cambio, que ninguno de ellos disponga de la metodología implantada en la organización en la que trabaja. Es una cuestión que merece una mayor reflexión y que se debe contrastar con los resultados y conclusiones del grupo B.

Es importante, también, la consideración de los participantes de que la gestión de riesgos documentales puede incorporarse en cualquiera de las fases de la implantación de un sistema de gestión documental. Eso sí, siendo preferente su aparición ya desde la fase del diseño, pero destacando que debe ser una acción cíclica que se debe realizar de manera periódica para obtener resultados.

Por último, se destaca la importancia que dan los participantes al trabajo en equipo y a disponer de equipos de trabajo multidisciplinares en las administraciones

4.4.2 Análisis del debate – Grupo B

Duración

El debate se realiza el 13 de junio de 2017 y tiene una duración total de 100 minutos, 10 minutos más que el *Focus Group* del Grupo A.

Asistentes

Del listado inicial de participantes, en el momento de realizar el debate no puede asistir el especialista en Prevención de Riesgos Laborales por indisposición. Esto da una participación del 83,33 %, quedando en la lista final cinco participantes, con los siguientes perfiles:

1. Un consultor experto en Gestión Documental (participante 1).
2. Un experto en Derecho Administrativo y Administración Electrónica (participante 2).
3. Un experto en Tecnologías (participante 3).
4. Un experto en Procesos (participante 4).
5. Un experto en Archivística y Gestión Documental (participante 5).

Descripción del debate

Nº PARTICIPANTE	PERFIL PROFESIONAL
1	consultor en gestión documental
2	experto en derecho administrativo y administración electrónica
3	experto en teconologías
4	experto en procesos
5	experto en archivística y gestión documental

Figura 28 - Participantes del Grupo B (elaboración propia).

Para llevar a cabo el análisis se sigue el mismo método explicado para el Grupo A.

Para dar comienzo se explica el tema de debate, los objetivos del *Focus Group* de manera general, así como la dinámica a seguir. Se da paso a los participantes para que respondan a la pregunta número 1.

1. Nombre y campo de experiencia, para el grupo B

Los participantes realizan, cada uno, su presentación de manera individual, indicando su nombre, su campo de experiencia y su actual lugar de trabajo. Cabe destacar que todos ellos se conocen previamente y todos están relacionados de manera directa o indirecta con la gestión de documentos a nivel profesional. Esto facilita la fluidez en el debate desde el inicio, proporcionando un marco de conversación cómodo.

2. ¿Habéis oído hablar alguna vez de la gestión de riesgos documentales? ¿En qué contexto?

Todos los participantes han oído hablar de la gestión de riesgos documentales. Cada uno de ellos comenta su experiencia profesional al respecto.

El experto del área de archivo (en adelante, participante 5) comenta que en la política de gestión de documentos electrónicos con la que están trabajando en su organización se incluyen unos estándares de control interno. Dentro de estos, hay un estándar específico dedicado a la gestión de documentos, dentro del cual se enumeran una serie de riesgos relativos a incumplimientos. Este estándar específico se utiliza como argumento para forzar la aplicación de las reglas de gestión documental internas.

El experto del área de procesos (en adelante, participante 4) comenta que, desde su experiencia, el conocimiento de los riesgos documentales es bastante reciente. Explica que hasta hace poco asociaba el riesgo con el concepto de seguridad.

El experto en derecho administrativo y administración electrónica (en adelante, participante 2) comenta que, en su contexto, están vinculando la gestión de riesgos con la adecuación al Esquema Nacional de Seguridad (en adelante, ENS)⁶⁶ y que además lo trabajan en paralelo con la Ley Orgánica de Protección de Datos (en adelante, LOPD)⁶⁷. En su organización, cuando se aborda la implantación de un sistema de gestión documental, se hace tanto desde la gestión de los documentos como desde la gestión de la información, incluyendo el análisis de riesgos siguiendo el ENS: identifican los riesgos con relación a los activos (documentos e información) para aplicar las medidas de seguridad adecuadas. El participante 2 dice haber oído hablar de riesgos documentales a partir de la publicación del ENS.

El experto del área de tecnologías (en adelante, participante 3) comenta que, desde su experiencia en las ad-

⁶⁶ – Según el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica, la finalidad del ENS es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios. El ENS persigue fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar al conocimiento de personas no autorizadas.

⁶⁷ – Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

ministraciones con las que ha trabajado, se ha encontrado con una ausencia total de sensación de riesgo. Incluso cuando estas administraciones no disponen de políticas de documento electrónico, de firma electrónica o de preservación. Su percepción es que en las administraciones públicas no se realizan análisis de riesgos y que existe una gran inconsciencia sobre este tema. Cuando inician proyectos de transformación digital no se plantean estas cuestiones, poniendo en riesgo la gestión de documentos y el cumplimiento de los propios objetivos y obligaciones.

El experto en consultoría (en adelante, participante 1) comenta que oyó hablar de la gestión de riesgos aplicada a la gestión documental hace muchos años, a través de la normalización y de los estándares internacionales. Según su punto de vista, las administraciones públicas están muy centradas en la aplicación de las leyes y la gestión de riesgos no se contempla. Contrasta esta situación con la que se da en las empresas privadas, donde la gestión de riesgos es intrínseca a su razón de ser. Se manifiesta de acuerdo con la visión de los participantes 2 y 4, en cuanto a que se empieza a entender la gestión de riesgos documentales en las administraciones públicas como un aspecto de seguridad de la información y como una cuestión tecnológica. Aporta un punto de vista diferente al del resto de participantes con relación a la terminología, explicando que la palabra “riesgo” no solo tiene una connotación negativa, sino que esta se refiere, en general, a las incertidumbres que afectan al cumplimiento de un objetivo. Añade que para hablar de riesgos de gestión documental primero es necesario hablar de riesgos de gestión, en general. Desde esta perspectiva, afirma que la gestión de riesgos documentales no solo se refiere a aspectos de seguridad, sino que hay muchos más aspectos y cuestiones a considerar. En este sentido, según su opinión, cualquier sistema de gestión documental, en realidad, está hecho para evitar riesgos. Todo lo que se hace en gestión documental es para prevenir riesgos de la gestión. Explica, por ejemplo, que se conservan documentos para poder demostrar, mediante evidencias, las decisiones y acciones que se han llevado a cabo, para garantizar los derechos de los ciudadanos, entre otras cuestiones. Concluye afirmando que, en realidad, los gestores de documentos están haciendo gestión de riesgos sin saberlo.

3. ¿Podéis enumerar diferentes riesgos documentales (dos o tres principales) que afecten a la organización en la que trabajáis o con la que colaboráis?

El participante 4 identifica tres tipos de riesgos. Como primer riesgo, el traslado de la responsabilidad de la formación de expedientes en entorno electrónico a los propios usuarios. Como segundo riesgo, la falta de directrices claras en la formación del patrimonio documental municipal, que origina una gran variedad documental que va a dificultar la recuperación de la información en un futuro. Y como tercer riesgo, que se depende, en entornos electrónicos, de programas informáticos que no están cumpliendo la ley.

El participante 5 explica dos ejemplos basados en su experiencia. Uno de ellos se relaciona con la imposibilidad de rendir cuentas, aun sabiendo que ha habido irregularidades en las actuaciones llevadas a cabo por una organización. Esto es así debido a la inexistencia de directrices y protocolos sobre la creación y organización de los documentos en uno de los organismos que están investigando desde su organización, que conlleva la imposibilidad de recuperar la información de manera que se pueda exigir la rendición de cuentas en un juicio. Comenta que les ha resultado imposible encontrar la información necesaria para cumplir con sus obligaciones de exigencia de rendición de cuentas. El segundo ejemplo no es un riesgo, sino una medida de prevención. Introduce el concepto de documentos esenciales y explica cómo en una organización en la que trabajó, cada noche se realizaba una evacuación (tras-

lado) de este tipo de documentos del depósito en el que se custodiaban a otro lugar para asegurar su conservación.

El participante 3 identifica como un riesgo importante, y muy real, el hecho de que muchas veces se crean los documentos electrónicos sin tener la visión de que deberán ser preservados, accesibles y que se deberán conservar sus características para garantizar su validez jurídica. Otro riesgo que plantea, es la delegación de la responsabilidad sobre la gestión documental a informáticos, por el mero hecho de ser electrónica, sin que estos tengan los conocimientos suficientes o no estén capacitados para asumir dichas responsabilidades. También explica que en una organización con la que colabora los informáticos consideran que disponer de un único modelo normalizado de gestión electrónica de documentos es un riesgo, tomando la decisión de dispersar los repositorios virtuales y de conservar los documentos en las distintas aplicaciones que se utilizan en las áreas tramitadoras. Esto ocasiona una dispersión importante que dificulta el control y la preservación a largo plazo.

Para el participante 1, los principales riesgos son: no producir un documento cuando se necesita (documento entendido como una evidencia) y no encontrarlo cuando se necesita. Explica que son riesgos diferentes, pero con consecuencias similares. Este participante considera que todo lo que se lleva a cabo en relación con la gestión documental va enfocado a evitar estas dos situaciones. Considera que estos riesgos son generales y también son matizables y dependen del tipo de documentos. Introduce aquí el concepto de los documentos esenciales, como prioridad en la prevención. Añade como riesgo, además, que las personas que trabajan dentro del sistema de gestión documental puedan encontrar lo que denomina como “caminos alternativos”, es decir, trabajar fuera del sistema definido.

El participante 2 comparte lo mencionado por el resto de participantes. Añade y destaca los riesgos vinculados con el derecho de acceso a la información, que conllevan la adopción de medidas de prevención como la anonimización⁶⁸ o la pseudonimización⁶⁹ de la información que se hace accesible. Este participante añade también riesgos relacionados con la interoperabilidad, con relación a cómo se construyen los documentos y los expedientes electrónicos para poder ponerlos a disposición de un tercero cuando así se requiera. Para ello, se necesita disponer de un sistema y de un modelo de datos y documentos que esté estructurado, a día de hoy una gran carencia de las administraciones públicas y, por tanto, un riesgo.

Además, el participante 3 opina que el entorno electrónico bien gestionado es más seguro que el entorno papel. El participante 5 opina que, una vez se resuelve el problema de la preservación digital a largo plazo, es mejor. El participante 1 no se pronuncia, pero sí opina que la documentación electrónica necesita de metodologías adecuadas para ser sistematizada, como la gestión de riesgos. El participante 4 considera que la clave es la sistematización, tal y como apunta el participante 1.

⁶⁸ – Anonimizar se define como expresar un dato relativo a entidades o personas, eliminando la referencia a su identidad. En la legislación española, pese a que no se incluye la palabra “anonimización”, sí se reconoce el dato disociado como aquel que no permite la identificación de un afectado o interesado. El artículo 3.f de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal define el procedimiento de disociación como todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a una persona identificada o identificable.

⁶⁹ – La pseudonimización se encuentra definida en el artículo 4.5 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, como la información que, sin incluir los datos denominativos de un sujeto afectado es decir, aquéllos que lo pueden identificar de manera directa, sí que potencialmente permiten, a través de la asociación con información adicional, determinar quién es el individuo que está detrás de los datos pseudonimizados.

4. ¿Cómo definiríais la gestión de riesgos documentales?

Para el participante 1, una gestión sistemática de riesgos supone que se documente esta gestión como un proceso más. Esto incluye documentar también la identificación de los riesgos, su análisis y las medidas que se establecen para mitigar cada riesgo. Considera que es necesario documentarlo todo para poder evaluar, al cabo de un tiempo, si la gestión de riesgos ha funcionado o si se deben adoptar nuevas medidas.

El participante 3 se manifiesta de acuerdo con lo apuntado por el participante 1. Añade que la norma internacional ISO 27001 y también el ENS, precisamente, contemplan lo explicado por el participante 1, en el sentido de documentarlo todo. En su opinión, para una adecuada gestión de riesgos se deben tener identificados los activos de gestión documental y se deben definir y documentar las medidas de prevención.

El participante 2 se manifiesta totalmente de acuerdo con lo comentado por los participantes 1 y 3. Añade una dimensión que considera importante: la gobernanza del sistema de garantía de riesgos. En su organización entienden la seguridad a nivel integral y trabajan el ENS, el Esquema Nacional de Interoperabilidad (en adelante, ENI)⁷⁰ y la LOPD de manera integral. Para ello, se han dotado de una estructura de organización para gobernar estas cuestiones con el fin de garantizar la minimización de riesgos. Han creado una Comisión y una Subcomisión de Seguridad, compuesta por profesionales con perfiles distintos, que se reúnen mensualmente para analizar las diferentes incidencias que se producen en materia de seguridad, desde todos los puntos de vista, por ejemplo, desde el punto de vista informático o jurídico o de gestión de documentos. Esto les ayuda a solucionar y prevenir incidencias, así como también comenta que han aprendido y están aprendiendo mucho de esta experiencia.

El participante 5 se manifiesta de acuerdo con los demás participantes. Considera fundamental documentar y justificar las medidas que se toman, así como reaccionar cuando estas medidas no son suficientes. También opina que la legislación española es muy ambiciosa y a la vez difícil de cumplir, que la normativa española es de las más avanzadas, pero poco realista. Explica que en otros países se adopta una estrategia quizás menos completa, pero más práctica. Con relación a este comentario, el participante 1 se manifiesta totalmente de acuerdo, porque considera que este es otro de los riesgos a los que enfrentarse.

Además, el participante 1 añade que los riesgos documentales no son solo los relacionados con la seguridad y que un factor de riesgo importante a considerar son las personas, así como también el contexto legislativo, tal y como menciona el participante 5. Menciona, como referente, la norma internacional ISO 18128 para identificar los riesgos sobre estos ámbitos.

⁷⁰ – Según el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica (ENI), el ENI comprende el conjunto de criterios y recomendaciones en materia de seguridad, conservación y normalización que deberán ser tenidos en cuenta por las Administraciones públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad, entre éstas y con los ciudadanos. La finalidad del ENI es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas, que permita el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunde en beneficio de la eficacia y la eficiencia.

5. ¿Cuáles creéis que pueden ser los beneficios de la gestión de riesgos documentales para el correcto funcionamiento de un SGD?

Los participantes manifiestan la importancia de la pregunta y se toman unos segundos para pensar sus respuestas.

El participante 5, según su experiencia, considera la gestión de riesgos documentales como un elemento de *marketing*, en el buen sentido, y que “vende” la gestión documental como algo positivo hacia la dirección de las organizaciones y hacia quien toma las decisiones.

El participante 3 espera, como beneficio, que la gestión de riesgos documentales genere tranquilidad a la hora de trabajar, quizás después de generar previamente la intranquilidad en la organización, al identificar los riesgos. Lo argumenta explicando que, si se conocen los riesgos y debilidades del sistema, se dispondrá de acciones de prevención y actuación cuando sea necesario, y eso es lo que genera la tranquilidad. Según su opinión, las personas tienden a los extremos, es decir, a estar totalmente preocupadas por algo o a estar totalmente seguras. En este sentido, la gestión de riesgos puede situar a las personas en un término medio, con conciencia y conocimiento de la situación, que beneficia a la organización.

El participante 4 ve el beneficio más importante en la idea de centrar la esencia en la gestión documental y no en la seguridad, es decir, vincular la gestión de riesgos con los instrumentos de gestión documental. Desenfocar el análisis de riesgos en sistemas informáticos para focalizarlo en la gestión documental. Otro beneficio que puede derivarse, según él, es el de corresponsabilizar a los productores de documentos, a las unidades tramitadoras.

El participante 2 comparte lo dicho por el resto de participantes. Para él, el beneficio debe repercutir en la ciudadanía. Debe permitir simplificar los procesos, lo que de manera indirecta beneficia al ciudadano (menor tiempo de resolución de trámites, mayor eficacia en la recuperación de la información, etc.).

El participante 1 opina que trabajando la gestión de riesgos se pueden enfocar mejor las medidas. Con relación a lo mencionado por el participante 3, considera que, haciendo una gestión de riesgos sistematizada, probablemente se puede discriminar sobre qué medidas se debe aplicar, sobre qué tipos de documentos, sin extremos y de una manera racional. Según este participante, este modo de trabajar gusta a quien debe tomar decisiones y a quien debe invertir recursos, ya que focaliza las acciones a llevar a cabo. El participante 4 se manifiesta totalmente de acuerdo y añade la opción de la priorización de las actuaciones a partir del análisis de los riesgos. El resto de participantes se manifiesta de acuerdo.

6. ¿Creéis que la gestión de riesgos documentales puede tener alguna repercusión en el proceso de rendición de cuentas de las administraciones públicas? ¿Cuál?

Para el participante 4 es evidente que hay una repercusión. Para que haya rendición de cuentas se debe tener documentada la actividad pública y ponerla al acceso de la ciudadanía. Si no se controlan los riesgos que pueden afectar a estos objetivos, la ciudadanía se ve perjudicada.

El participante 1 explica que, si se habla de la rendición de cuentas como una idea, sí que puede haber repercusión, pero que, con la legislación actual, en que la rendición de cuentas está muy reglada, no lo ve posible. Considera que, si no se produce un cambio en la legislación, incluyendo la gestión de riesgos documentales dentro de los procesos de rendición de cuentas, esto no es más que una idea. En cambio, afirma que para las empresas privadas sí es un factor muy importante a tener en cuenta.

El participante 3 explica que el ENS exige a las empresas proveedoras de servicios o productos de las administraciones públicas que dichos productos o servicios tengan un nivel de calidad determinado. Esto está ocasionando que los proveedores realicen un análisis de riesgos de sus productos o servicios, lo que posteriormente da lugar a una certificación por un tercero. El objetivo de los proveedores es poder vender a las administraciones públicas. Explica esta situación como un ejemplo de éxito que puede ser extrapolable a la gestión documental si se modificase la legislación, con relación a lo que ha comentado el participante 1 sobre que se exija, por ley, la gestión de riesgos. También ve muy complicado que la gestión de riesgos documentales pueda, realmente, afectar en los procesos de rendición de cuentas, como apunta el participante 1. El participante 4 manifiesta su disconformidad con estos argumentos.

El participante 5 considera que puede ser un elemento importante para mejorar la rendición de cuentas, pero advierte que hay que estar alerta para que no se quede en nada.

El participante 2 cree que sí puede ayudar. Opina que seguramente se está actuando mal, que las personas intervienen demasiado en la apertura de la administración. Según su punto de vista, la información que permite la rendición de cuentas debe publicarse directamente desde los sistemas de gestión documental, sin mediación humana o intermediarios, para mostrar la actividad de la administración. Comenta que, quizás no hay una relación directa entre la gestión de riesgos documentales y la rendición de cuentas, pero que sí la hay indirecta y que puede reportar beneficios.

El participante 1 responde al participante 2 afirmando que la publicación directa se puede hacer con o sin gestión de riesgos. El participante 2 se reafirma en que la relación no es directa, sino indirecta y que, por tanto, sí puede ayudar. El participante 1 se manifiesta de acuerdo con esta afirmación. El participante 4 insiste en que él sí ve claramente la relación de beneficio.

7. ¿En qué momento/fase del proceso creéis que debería llevarse a cabo la identificación y análisis de riesgos documentales?

Todos los participantes coinciden en que debe realizarse al principio, en la fase de diseño de los procesos. En cualquier caso, también coinciden en que, si no es posible realizarlo al inicio, hay que realizarlo en el momento en que se pueda. El participante 2 añade que, como en todo buen sistema, debe ser algo continuo e integrado en la forma de trabajar.

8. De lo hablado anteriormente, ¿qué consideráis que es lo más importante?

Para el participante 4, lo más importante es poder disponer de una metodología que pueda mejorar la socialización de la gestión documental en toda la organización. Afirma que no ha trabajado con esta metodología y que ahora dispone de un recurso más.

Para el participante 1 es un gran descubrimiento un apunte hecho por el participante 4 durante el debate de la pregunta 6: la realización de un análisis de riesgos antes de llevar a cabo la implantación de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. Lo considera una oportunidad estupenda para empezar a trabajar con la gestión de riesgos.

Para el participante 3, lo más importante es disponer de una metodología normalizada para aplicar en la organización. Concretamente, que la gestión de riesgos sea una metodología corporativa y homogénea para la toma de decisiones. El participante 2 añade que la gestión de riesgos debe ser multidisciplinar, con un liderazgo claro, pero con diferentes perfiles: organización, tecnologías, archivos, compromiso político, entre otros. El participante 5 añade que la gestión de riesgos les proporciona un elemento para poder comunicarse con todos estos perfiles.

El participante 2 también destaca la toma de conciencia sobre cómo está la situación en las administraciones actualmente: habla de falta de recursos y de falta de perfiles profesionales adaptados, entre otros. Considera que hay un gran número de temas que deben abordarse para la transformación digital, pero no hay conciencia del cambio tan transcendental que se está viviendo.

9. ¿La sensación al finalizar el debate es positiva o negativa?

Todos los participantes manifiestan haber acabado el debate con una sensación positiva.

El participante 3 añade que se queda con una doble sensación: que no está haciendo las cosas todo lo bien que podría, y que se pueden hacer mucho mejor. También opina que se deben incorporar nuevos parámetros en el día a día. Globalmente, lo considera positivo.

El participante 4 añade que se tiene que socializar esta metodología de trabajo en las administraciones en general, no solo en una organización aislada, sino como un recurso más con el que trabajar. Comenta que quizás se puede aprender de la sistemática en gestión de riesgos de las organizaciones privadas.

El participante 1 también coincide en la sensación positiva, sobre todo porque al hablar de esta metodología, cada vez se van viendo más aplicaciones prácticas. También opina que es una asignatura pendiente, pero considera que hablar de ello es una manera de empezar.

El participante 5 se manifiesta de acuerdo con las intervenciones anteriores. Considera que la gestión de riesgos es un elemento a incorporar a la implantación de sistemas de gestión documental.

Conclusiones del debate

Para continuar con el análisis, se explican a continuación las conclusiones del debate llevado a cabo por el Grupo B.

Se destacan, en este segundo debate, como palabras más mencionadas “seguridad” y “gestión sistemática”, seguidas por “documentos esenciales”, “inconsciencia” y “normalización”. Se aprecia la coincidencia de la mayoría de términos con el grupo A. Nuevamente, se da un mayor protagonismo a la seguridad en relación con la gestión de riesgos, pese a haber manifestado los participantes que dicha gestión no se relaciona tan solo con la seguridad.

Todos los participantes del grupo B manifiestan conocer la gestión de riesgos documentales y dos de ellos la están aplicando a través de mecanismos de control interno o de mecanismos de seguridad. De ello se deduce que no realizan la gestión de riesgos documentales desde la identificación de las incertidumbres que pueden afectar propiamente a los documentos o a la gestión de los mismos. Los tres participantes restantes indican que no están trabajando con esta metodología en sus organizaciones. Por tanto, se constata que mayoritariamente esta metodología todavía no está instaurada como un instrumento más de la gestión de documentos en las administraciones públicas.

Con relación a la identificación de riesgos documentales, destaca que la práctica totalidad de ellos se enmarcan en entornos electrónicos. Pese a esta situación, el grupo manifiesta que un entorno electrónico bien gestionado y sistemático es más seguro que un entorno papel, lo que puede llevar a deducir que son afirmaciones contradictorias. Es posible que se refieran, en realidad, a que en entornos electrónicos bien gestionados se da un menor porcentaje de incidencias detectadas, y no a que exista un menor número de riesgos.

Destaca la diferencia de opiniones entre los participantes en la pregunta 6. Dos de ellos se muestran escépticos (perfil tecnológico y consultor) sobre la posible incidencia de la gestión de riesgos en los procesos de rendición de cuentas, y los otros tres participantes afirman que sí puede tener una afectación positiva sobre dichos procesos. Ambos “bandos” se muestran muy convencidos de su punto de vista, lo que ocasiona debate entre los participantes, finalizando todos con la misma opinión que al inicio de la discusión. En cualquier caso, todos los participantes consideran que es beneficioso disponer de una metodología normalizada en gestión de riesgos para aplicar en su día a día.

Se remarca la importancia que se da a la normalización en la metodología, ya que se trata de un aspecto que destacan los participantes. Del mismo modo, también recalcan la necesidad de disponer de equipos multidisciplinares en dicha metodología, para la obtención de resultados aplicables y funcionales. La aproximación a la gestión de riesgos documentales no debe hacerse desde un único profesional, sino que es más beneficioso para el proceso trabajar en equipo.

Finalmente, se destaca el comentario del participante 1 al responder a la pregunta 2, cuando afirma, en primer lugar, que en realidad cualquier sistema de gestión documental sirve para prevenir riesgos y, en segundo lugar, que los gestores de documentos están haciendo gestión de riesgos sin saberlo. Son dos afirmaciones complementarias que dan a entender que, en realidad, la gestión documental puede servir como una herramienta de prevención de riesgos en las organizaciones. Además, incluye una falta de consciencia entre los profesionales del sector con relación a los beneficios de su trabajo, como puede ser la prevención de riesgos. Ser consciente de ello puede dar lugar a un

mejor posicionamiento interno en las organizaciones, y a una orientación distinta de la gestión documental, vista como un puntal estratégico para la consecución de objetivos.

4.4.3 Análisis comparativo entre los grupos A y B

En la planificación de los *Focus Groups* se fijaron una serie de objetivos que se han alcanzado con éxito. Para demostrarlo, se finaliza el análisis de respuestas y resultados de ambos debates de manera comparada.

La visión que los participantes de ambos grupos tienen sobre la gestión de riesgos documentales es similar, aunque con matices importantes. Todos ellos manifiestan conocer la metodología, aunque los participantes del grupo A no la aplican mientras que algunos del grupo B sí han trabajado con ella. Globalmente, coinciden en los beneficios y efectos positivos que tendría en su día a día, pero cabe destacar que en el grupo B se tiene un mayor conocimiento, así como una visión más operativa de la gestión de riesgos documentales.

Se deduce de las afirmaciones de los participantes que, mayoritariamente, la gestión de riesgos documentales se relaciona, a día de hoy, con aspectos de seguridad. Prácticamente todos ellos afirman que cuando hablan de riesgos documentales no solo se refieren al control de la seguridad de los documentos, la información y los sistemas. Eso sí, al analizar las palabras más nombradas en ambos debates, se evidencia una fuerte presencia de “seguridad” por delante de cualquier otro término. Dentro de esta visión compartida sobre qué significa o qué implica esta metodología, los participantes de ambos grupos manifiestan la importancia de tener identificados y controlados de manera especial los documentos esenciales como un método preventivo de gestión. Esta coincidencia de términos es destacable en tanto que los profesionales que han participado en los *Focus Groups* provienen de diferentes tipos de archivos, con trayectorias diferentes, así como también de distintas disciplinas y campos de experiencia. Se deduce, por tanto, que el control de los documentos vitales y la seguridad son dos aspectos clave, a día de hoy, en lo que los profesionales entienden por gestión de riesgos documentales.

Otro aspecto interesante es la repetición de la misma situación en el grupo A y B, o muy similar, al responder la pregunta 5. En el grupo B, los participantes no se centran en responder de un modo preciso a lo que se les pregunta, sino que amplían la identificación de beneficios, en este caso no solo a la profesión (como los participantes del grupo A) sino también incluso a la ciudadanía. Adicionalmente a las respuestas del grupo A, en el grupo B sí se explican algunos ejemplos de beneficios sobre la gestión documental, aunque de forma indirecta, como la mejora en la toma de decisiones sobre las acciones preventivas. De esto se interpreta que, pese a que el grupo B sí ha empezado a trabajar la gestión de riesgos documentales, todavía no se cuenta con experiencias suficientes para poder identificar beneficios directos de esta metodología.

Otro de los puntos en común entre ambos grupos es la opinión compartida sobre los grandes beneficios que esta metodología puede aportar a la profesión. Se mencionan aspectos como: la mejora del posicionamiento de la profesión, que convierte a los gestores de documentos en fiscales o auditores; la oportunidad para repensar la profesión de una manera más transversal; la apertura de un campo de trabajo para no tener presente solamente aquello relacionado con la metodología archivística, sino ir más allá y salir de la zona de confort; el aprovechar la oportunidad; la visión de la gestión de riesgos como un elemento de marketing sobre la profesión, para ayudar a

socializar la gestión documental en las organizaciones; el generar confianza y tranquilidad; e incluso, la repercusión en la ciudadanía. Se deduce de estas palabras una visión muy positiva sobre lo que implicaría incluir la gestión de riesgos documentales en los sistemas de gestión documental. Se destaca la percepción como oportunidad y como reposicionamiento profesional, siempre desde la propuesta de soluciones en las organizaciones. Además, añadiendo esta metodología se consigue disponer de mayor información objetiva sobre el funcionamiento de la gestión diaria, consiguiendo mejorar la toma de decisiones, tal y como se apunta en ambos debates.

Por tanto, los beneficios deben partir de la base de aportar soluciones funcionales desde la apreciación del riesgo.

En línea con lo apuntado en la reflexión anterior, cabe destacar que los participantes también mencionan la importancia de la formación para poder realizar este cambio de visión. Se habla de formación actualizada para el “nuevo perfil”, para “las personas que deben acompañar este cambio en las organizaciones”. Pese a ello, quizás no sea necesario un nuevo perfil con nueva formación, sino capacitar a los profesionales de la gestión documental en esta metodología para que puedan disponer de un instrumento más con el que trabajar. También es necesario, en esta misma línea, incluir formación sobre la gestión de riesgos documentales en los cursos de formación reglada y de especialización de la profesión ya existentes, como por ejemplo el Máster universitario en Archivística y Gestión de Documentos⁷¹ y el Máster universitario en Gestión Documental, Transparencia y Acceso a la Información⁷² de la Escuela Superior de Archivística y Gestión de Documentos de la Universidad Autónoma de Barcelona⁷³, o el Máster en Archivística⁷⁴ de la Universidad Carlos III de Madrid. Tampoco cabe descartar el diseño y puesta en marcha de cursos monográficos sobre esta metodología para aquellos profesionales que quieran especializarse.

A la hora de identificar riesgos documentales, los participantes de ambos grupos, mayoritariamente, lo hacen refiriéndose a entornos electrónicos, pese a que los riesgos identificados pueden extrapolarse a entornos que trabajan en papel. Esto puede corresponderse con la realidad actual de transformación digital de las administraciones públicas, que están trabajando en la implantación de modelos y sistemas de gestión de documentos electrónicos. Una opinión discordante entre los grupos es la distinta visión sobre qué entorno puede generar más riesgos. Para el Grupo A en el entorno electrónico se dan más riesgos, con diferencia. Todos los participantes se muestran de acuerdo con este punto de vista. En cambio, en el Grupo B se afirma justo lo contrario, el entorno de trabajo es más seguro, siempre y cuando la gestión de documentos en entorno electrónico sea la adecuada.

Un punto de encuentro lo hallamos en el apunte que se hace en ambos grupos sobre la importancia de identificar los documentos vitales. Todos los participantes creen en la necesidad de identificar y controlar de manera espe-

⁷¹ – Se puede consultar el Plan de estudios siguiendo el enlace a la página web del programa: <http://www.uab.cat/web/estudiar/la-oferta-de-masteres-oficiales/plan-de-estudios/plan-de-estudios-1096480309783.html?param1=1267601207452> (consultado el 03/03/2018).

⁷² – Se puede consultar el Plan de estudios siguiendo el enlace a la página web del programa: <http://www.uab.cat/web/estudiar/la-oferta-de-masteres-oficiales/plan-de-estudios/plan-de-estudios-1096480309783.html?param1=1345679261925> (consultado el 01/08/2018).

⁷³ – Se puede consultar su oferta formativa siguiendo el enlace a su página web: <http://www.uab.cat/web/escuela-superior-de-archivistica-y-gestion-de-documentos-esaged-1345737665780.html> (consultado el 01/08/2018).

⁷⁴ – Se puede consultar el Plan de estudios siguiendo el enlace a la página web del programa: http://www.uc3m.es/ss/Satellite/Postgrado/es/Detalle/Estudio_C/1371209380359/1371219633369/Master_en_Archivistica#programa (consultado el 19/07/2017).

cial estos documentos para la continuidad del negocio, como una medida preventiva. Solamente uno de los participantes del Grupo A añade que dar un especial tratamiento a estos documentos, o tenerlos claramente identificados, puede también implicar riesgos, al estar especialmente expuestos. En cualquier caso, se constata la importancia que dan todos los participantes a esta cuestión, sean del ámbito de especialización que sean.

Con relación a la identificación de riesgos, para el Grupo A estos se relacionan más con aspectos de contexto y gestión que propiamente con los documentos. Se menciona el trabajo en equipo, la disposición de expertos en gestión documental, la formación, los recursos para el mantenimiento del sistema de gestión, entre otros aspectos. En cambio, el Grupo B da mayor importancia a cuestiones relacionadas con los objetivos de la administración como, por ejemplo, la rendición de cuentas, la publicación de documentación confidencial, la imposibilidad de recuperar información o la interoperabilidad, entre otros.

Es destacable la identificación como un riesgo de la inexistencia de sistemas de gestión documental, apuntado por el Grupo A. Los propios archiveros son conscientes de que, sin un sistema de trabajo centrado en los documentos y la información, la organización está expuesta a múltiples amenazas. Esto encaja perfectamente con una afirmación hecha por uno de los participantes del Grupo B, que se refiere a que, en realidad, los gestores de documentos están haciendo gestión de riesgos. También se alinea perfectamente con uno de los puntos de partida de la ISO 15489, actualizada el año 2016, en el que se afirma que dicha norma se ha desarrollado partiendo de diferentes ideas, entre ellas la gestión de documentos como una estrategia de gestión de riesgos en sí misma (AENOR 2016, p. 5). Este punto de partida, incluido en una norma internacional, refuerza claramente el valor añadido que tendría la inclusión de estrategias de gestión de riesgos en los sistemas de gestión documental, contribuyendo a una gestión integral del riesgo en las organizaciones. La gestión de documentos pasaría, por tanto, de ser una parte meramente instrumental y relegada, en muchas ocasiones, a ser un proceso finalista, para posicionarse en un nivel estratégico. De este modo, seguramente se conseguiría repositionar a los gestores de documentos en las organizaciones, tal como apuntan los participantes del Grupo A al hablar de los beneficios que supondría incluir esta metodología en su día a día.

Con relación a la pregunta sobre la posible afectación que la inclusión de la metodología de gestión de riesgos en la gestión documental puede tener sobre los procesos de rendición de cuentas en las administraciones públicas, un 70 % de los participantes afirma que sí puede existir afectación, ya sea esta positiva o negativa. Un 20 % se muestra escéptico y no ve clara la relación directa entre ambas cuestiones, a no ser que se dé un cambio en la legislación actual. El 10 % no se manifiesta ni a favor ni en contra, por no estar presente en el momento de la pregunta⁷⁵. Cabe destacar que el 20 % escéptico proviene completamente del Grupo B, el equipo multidisciplinar, y concretamente de los perfiles de consultoría y tecnológico. El Grupo A, de archiveros, se manifiesta 100 % de acuerdo con la existencia de una relación entre la metodología aplicada de gestión del riesgo y el objetivo de rendir cuentas.

Un apunte del Grupo B es la puntualización de que la relación puede no ser directa, sino indirecta. De hecho, una de las hipótesis de esta investigación es que la gestión de riesgos documentales no modificaría por sí sola los procesos de rendición de cuentas de manera directa, sino que la finalidad principal es la de mejorar la gestión

⁷⁵ – Cabe recordar que el participante 1 del Grupo A tuvo que abandonar el debate pasados 40 minutos.

documental. De este modo se conseguirían procesos más eficaces y más fácilmente sistematizables, precisamente con el objetivo de facilitar el cumplimiento de las obligaciones relacionadas con la publicación de información en portales de transparencia o con facilitar el derecho de acceso a la información pública. Un valor añadido de incluir la metodología de gestión de riesgos es el aumento de la confianza en esa información, precisamente partiendo de la base de que se ha llevado a cabo un proceso de apreciación de los riesgos que pueden afectar a las características de autenticidad, fiabilidad, integridad y usabilidad de los documentos que contienen dicha información. Por tanto, el hecho de que los participantes indiquen que la relación es indirecta se alinea, perfectamente, con esta hipótesis planteada en la investigación.

De estos datos, se puede deducir que mayoritariamente los participantes consideran posible la influencia sobre los procesos de rendición de cuentas. Sobre qué tipo de repercusiones, se dan algunos ejemplos durante el debate en ambos grupos. Se menciona, sobre todo, el aumento de la confianza de los ciudadanos en la información proporcionada. También, la mejora en el cumplimiento de los objetivos de la administración, dentro de los que se enmarca precisamente la rendición de cuentas o el acceso a la información.

Se concluye este análisis tal y como se concluyeron ambos debates, con la percepción de los participantes al finalizar. El 100% de ellos manifestó acabar el debate con una sensación positiva, con ganas de poner en práctica esta metodología en su día a día, y convencidos de que les aportaría beneficios así como de que es un instrumento realmente útil y funcional para las organizaciones. Es destacable esta visión positiva compartida en ambos grupos, con perfiles distintos y entornos de trabajo muy alejados en algunos casos (por ejemplo, trabajadores de archivos con documentación histórica y expertos en administración electrónica).

Capítulo 5.

La gestión de riesgos documentales en una administración pública: metodología, aplicación y resultados.

Un estudio de caso básico engloba el análisis intensivo y detallado de un único caso (Bryman 2012, p. 66). Su característica principal es la profundidad y el foco en el objeto de investigación, tanto si este es un individuo, un grupo, una organización, una cultura, un incidente o una situación (Ghauri 2004, p. 110), así como también que dicho objeto debe tener unos límites bien definidos (Pickard 2013, p. 101). El uso más común del término “caso” asocia el estudio de caso con una localización, como una comunidad o una organización (Bryman 2012, p. 67). Concretamente, este estudio de caso se centra en un organismo público municipal situado en una localidad de la provincia de Barcelona.

Esta investigación se realiza sobre un único caso y se fijan dos requisitos a la hora de seleccionar la organización objeto de estudio. En primer lugar, que tenga la obligatoriedad de rendir cuentas y, en segundo lugar, que cuente con un sistema de gestión documental implementado y funcionando.

En cuanto a la primera premisa, todas las administraciones públicas están obligadas a rendir cuentas, por lo que se optó por seleccionar un organismo público. Se propuso una administración pública municipal, concretamente un ayuntamiento, por ser el tipo más numeroso de administración pública existente, y por ese motivo se puede facilitar la aplicación y la extrapolación del estudio a organizaciones similares a corto y medio plazo.

En cuanto a la segunda premisa, se selecciona un ayuntamiento con un sistema de gestión documental implantado, tal y como se explicará más adelante en el análisis del contexto.

Una de las finalidades principales de este estudio de caso es la de aplicar la metodología de gestión del riesgo a la gestión de documentos, así como también relacionar dicha metodología con el proceso de rendición de cuentas a que está obligado cualquier organismo público, como es el caso de la administración municipal. Se parte de la hipótesis de que la metodología de gestión de riesgos puede aplicarse a la gestión de documentos, aportando beneficios, y uno de ellos es la mejora del proceso de rendición de cuentas de las administraciones públicas. En este sentido, lo que se pretende es centrarse en la importancia de disponer de documentos auténticos, íntegros, fiables y accesibles para poder llevar a cabo, cuando sea necesario, los procesos de rendición de cuentas de manera fiable. Se pretende, también, analizar cómo puede afectar la inclusión de la gestión del riesgo en la gestión documental a la hora de disponer de documentos con estas características a lo largo del tiempo. Para ello, se fijan dos grandes objetivos en este estudio de caso:

Objetivo 1: Aplicar el proceso de gestión del riesgo a la metodología de gestión documental de la organización. Este objetivo tiene dos finalidades. En primer lugar, incluir un análisis para conocer si existe y si se pone en prácti-

ca una metodología o proceso específico de gestión del riesgo en dicha organización. En segundo lugar, identificar, analizar y evaluar los riesgos documentales del organismo estudiado, así como proponer diferentes acciones de tratamiento y prevención para la mejora de la gestión documental.

Objetivo 2: Analizar cómo puede afectar la inclusión de la gestión del riesgo en la gestión documental a los procesos de rendición de cuentas de la organización.

Este estudio debe entenderse como un punto de partida para demostrar que es posible la inclusión de esta metodología, como un valor añadido, en el día a día de los gestores de documentos.

Cabe destacar que este estudio de caso se presenta de manera anónima a petición de la organización objeto de estudio. Esta organización entendía que su reputación podía quedar dañada debido a las situaciones de riesgo identificadas, así como a las causas de las que se derivan, que también quedan recogidas en este análisis. De acuerdo a esta petición, la organización que nos ocupa manifiesta su conformidad ante la propuesta de denominarla, de ahora en adelante, “Organización X”.

5.1 Metodología

Para el estudio de caso, se parte de la metodología de gestión del riesgo propuesta en los estándares internacionales. El marco general metodológico que se sigue es el definido en la norma ISO 31000. Además de esta metodología, se emplean otros estándares en la aplicación concreta para el ámbito de la gestión documental, como es el informe técnico ISO/TR 18128, empleado para el subproceso de apreciación del riesgo. También, la norma ISO/IEC 31010 para la selección de las técnicas más apropiadas al estudio de caso realizado.

La metodología enmarcada en estándares o normas ISO goza del consenso de distintos sectores profesionales y académicos a nivel internacional. La organización ISO destaca, de entre otras organizaciones internacionales de normalización, por ser una de las más activas en el desarrollo y publicación de estándares internacionales en distintos ámbitos, para dar soluciones que armonicen los requerimientos de sectores de negocio y necesidades de la sociedad (Grupo de Difusión del CTN 50-SC1 2012, p. 175).

A continuación, se enumeran las metodologías y técnicas que se seleccionan para este estudio de caso, siguiendo la estructura de las fases a través de las que se desarrolla el proceso de gestión del riesgo:

- Comunicación: en esta primera fase el objetivo es informar a todas las personas involucradas en el estudio de caso sobre el proceso que se va a seguir, qué se espera de ellas y un calendario aproximado con la duración del proyecto. Es fundamental que todo el personal esté siempre informado para evitar posibles rechazos y conseguir complicidades.
- Análisis del contexto: para poder realizar un estudio detallado de la situación de la Organización X es

necesario realizar un análisis previo de situación. El objetivo es conocer si existe o no una metodología de gestión del riesgo (no necesariamente de riesgos documentales) y qué conocimiento de ella tienen los trabajadores. Además, se estudia la organización a nivel interno con relación a su estructura, directrices existentes, instrumentos de gestión documental desarrollados, entre otros aspectos relevantes para el estudio de caso. Para ello, se emplea principalmente la técnica de las entrevistas semi-estructuradas, y se complementa con la observación directa y la consulta de documentación de la organización. El uso de tres fuentes de información distintas permite un mejor y un mayor conocimiento de la organización.

- **Identificación de riesgos:** es una de las etapas más importantes del estudio de caso, ya que de ella derivan el resto de fases posteriores. Es, por tanto, una fase crucial y por ello es necesario utilizar todas las fuentes de información posibles: entrevistas semi-estructuradas, análisis del contexto, recopilación de información a partir de documentos y observación directa del funcionamiento de la gestión. En primer lugar, se realiza la identificación de riesgos documentales a partir de las amenazas, en función de la información obtenida de las entrevistas al personal seleccionado. En segundo lugar, se realiza una nueva identificación a través del análisis del cumplimiento de los requisitos de gestión documental partiendo de la norma ISO 30301, que incluye los requisitos que debe cumplir cualquier sistema de gestión para los documentos para poder obtener una certificación internacional. Emplear dos enfoques distintos permite contrastar y comparar los resultados obtenidos para conseguir una mayor precisión en la identificación de riesgos.
- **Análisis de riesgos:** el objetivo principal es profundizar en las causas, las probabilidades y las consecuencias potenciales de cada uno de los riesgos identificados. Para ello, en esta fase se emplean dos técnicas de análisis de riesgos distintas, con el objetivo de comprender mejor los riesgos documentales identificados en la fase anterior. Se realiza un primer análisis a partir de la matriz de consecuencia y probabilidad, lo que permite una categorización o clasificación de los riesgos. En segundo lugar, se emplea la técnica del análisis de pajarita, que permite analizar las trayectorias de un riesgo desde sus causas hasta sus consecuencias. Emplear dos técnicas distintas permite contrastar los resultados y obtener información más detallada del proceso de análisis, con la finalidad de ajustar mejor la evaluación en el siguiente paso del estudio.
- **Evaluación de riesgos:** esta fase permite la toma de decisiones informada, a partir de los resultados del análisis de la fase anterior. Se emplea la técnica semicuantitativa de los índices de riesgo. Para ello se definen una serie de factores a evaluar y comparar, basados en los datos obtenidos en las fases previas, con la finalidad de obtener resultados con relación a la prioridad de tratamiento que se debe dar a cada riesgo identificado. Los resultados obtenidos en esta etapa sirven de apoyo en la fase del tratamiento de riesgos.
- **Propuestas de tratamiento:** en este caso se parte de la metodología establecida por la organización, que define diferentes tipologías de acciones preventivas. A partir de esta, se desarrollan actuaciones concretas para el tratamiento de cada uno de los riesgos. A partir de la información recopilada en las fases anteriores, se puede decidir mejor entre distintos tratamientos y se puede establecer un cronograma aproximado de implantación para la Organización X. Los tratamientos no siempre deben actuar sobre los mismos aspectos, sino que en función de los resultados de las fases anteriores se ajustan las propuestas a las necesidades reales de prevención.
- **Propuesta de seguimiento:** en esta fase, el objetivo principal es que la Organización X no se olvide de controlar y revisar, de manera periódica, el grado de adecuación y eficacia de los tratamientos propuestos en la fase anterior. Es fundamental asegurar la implantación de la dinámica de gestión del riesgo en la organización para que esta pueda alcanzar el éxito en dicho proceso. Esto implica una reducción de los riesgos documentales y una mejora sustancial del sistema de gestión documental, que debe redundar en una mayor fiabilidad de los procesos de rendición de cuentas.

- Documentación del proceso: aún situando esta cuestión en el último lugar, cabe destacar que es una de las más importantes a lo largo de todo el proceso y desde el inicio. Es un aspecto fundamental de la metodología y debe realizarse de manera continua, ya que la documentación del proceso proporciona la base para la mejora de los métodos y las herramientas, así como del proceso en su conjunto. Es necesario ir documentando todas las acciones que se realizan, los resultados de las distintas técnicas empleadas o las decisiones tomadas a lo largo del estudio de caso. De igual modo, en cualquier proceso de gestión del riesgo siempre deben documentarse todos los pasos para disponer de las evidencias necesarias para continuar el proceso y mejorarlo a lo largo del tiempo. En este caso, se desarrollan unas fichas para cada riesgo, con los campos de información necesarios para su gestión.

Estos pasos están alineados con el proceso de gestión del riesgo descrito en la norma internacional ISO 31000, así como también con el proceso de apreciación del riesgo descrito en el informe técnico ISO/TR 18128.

Además de los métodos y técnicas explicados anteriormente, para la realización de estudios de caso es recomendable la recopilación de información a través de múltiples fuentes, como informes verbales, entrevistas personales, observación e informes escritos (Ghauri 2004, p. 109). Para el caso concreto de este estudio, la recopilación de información se realiza a partir de entrevistas semi-estructuradas, observación y el estudio de la documentación producida por la organización con relación a las directrices internas de gestión documental. De este modo, se dispone de tres fuentes distintas de información, siguiendo la metodología de la triangulación. Este método se refiere a la recopilación de datos a través de distintos métodos e incluso distintos tipos de datos sobre el mismo fenómeno. La principal ventaja de la triangulación es que puede producir una imagen más completa, holística y contextual del objeto de estudio reduciendo, además, la posibilidad de malinterpretaciones (Ghauri 2004, p. 115). La recopilación de datos desde distintas fuentes sirve, además, como complemento (Pickard 2013, p. 102). Por último, se incluye la retroalimentación de las personas de la Organización X implicadas en el estudio de caso, cuando se considera necesario para ampliar información, matizarla o corroborarla.

El estudio de caso se desarrolla entre los meses de septiembre del año 2016 y abril del año 2018.

Para poder iniciar el estudio de caso sobre una organización real se realizaron contactos a través de los responsables de dos áreas concretas de la Organización X, con las que se había colaborado anteriormente en otro proyecto: el área de Gestión documental y archivos, y el área de Organización y proyectos de mejora. De hecho, una de las ventajas percibidas a la hora de poder conseguir una respuesta positiva a la realización del proyecto de investigación aplicada es el conocimiento previo de la organización.

Se realiza, en primer lugar, un contacto informal para proponer el proyecto y explicar los objetivos de manera general a las personas responsables de estas dos áreas. Hecho esto, se realiza un contacto formal para solicitar los permisos y autorización necesarios para el desarrollo del estudio de caso. Posteriormente, se convoca una reunión con las personas responsables de las dos áreas mencionadas con la finalidad de realizar una presentación en la que exponer los objetivos, la metodología a seguir, los posibles roles con los que se espera poder contactar para el estudio, el calendario aproximado, los beneficios que aportaría este estudio en la Organización X y los documentos que se van a entregar, con los resultados, a lo largo del desarrollo del proyecto. Esta presentación se realiza también, de manera abreviada, a todas las personas con las que se realizan encuentros y entrevistas a lo largo de la investigación.

Para la comunicación se elabora un documento informativo breve (ver Anexo B). En este caso, no se trata únicamente de buscar el compromiso en el ámbito corporativo sino, además, su colaboración voluntaria con el desarrollo de un estudio de caso, dentro de una investigación enmarcada en el desarrollo de una tesis doctoral. En el documento se introduce el objetivo general del estudio, se explica el alcance definido, así como la necesidad de contar con la participación de cada una de las áreas a las que se ha seleccionado. Por último, se pone a su disposición un nombre y dirección de correo electrónico de contacto por si alguna de las partes interesadas tuviera, en algún momento, la necesidad de contactar.

Se decide realizar el envío del documento de comunicación a través de la persona responsable de una de las áreas seleccionadas para el estudio, el área de Organización y proyectos de mejora, por ser un departamento de gestión relacionado con el resto de áreas enmarcadas en el alcance definido. La persona responsable de este departamento envía el documento de comunicación por correo electrónico a las partes interesadas, haciendo de mediadora. Se decide de esta manera por parte del personal interno involucrado de la Organización X, con la finalidad de facilitar el primer contacto y por considerar que un proyecto de estas características necesita contar, desde el principio, con el apoyo de un departamento clave.

Esta comunicación se realiza de manera satisfactoria, quedando todas las partes interesadas debidamente informadas. Se consigue su compromiso para el resto de etapas del proceso en que van a ser necesarias y se mantiene un contacto fluido durante el desarrollo del estudio.

El siguiente paso consiste en fijar las fechas para la realización de las entrevistas. En esta comunicación se adjunta el listado con las preguntas que se van a realizar para que pudiesen preparar el encuentro con tiempo y plantear dudas. Ninguno de los entrevistados plantea dudas respecto a las preguntas formuladas antes de los encuentros.

En uno de estos encuentros, concretamente con el responsable de tecnologías, se plantea por primera vez la posibilidad de que se realice de manera anónima, ya que el estudio de caso, y la inclusión de los resultados en una tesis doctoral de acceso público, se perciben como una amenaza a la reputación de la organización, como una fuente de conocimiento sobre sus debilidades, y eso puede hacerles más vulnerables. Es por ello que, después de hablarlo también con otras personas de la Organización X involucradas en el proyecto, se decide anonimizar todo el estudio.

Por último, para el estudio de caso se define un alcance limitado para la aplicación de la metodología estudiada, lo que implica contar con las siguientes partes interesadas internas: área de Gestión documental y archivo, área de Prevención de riesgos laborales, área de Informática, área de Atención ciudadana y, por último, área de Organización y proyectos de mejora. Estas áreas son seleccionadas debido a su implicación directa en la gestión de documentos dentro de la Organización X, así como por su relación con la gestión de riesgos. Para este estudio de caso no se identifican partes interesadas externas.

A continuación, se explican las distintas fases del estudio de caso, en el orden en que se han llevado a cabo, incluyendo la metodología empleada.

5.2 Fase 1. Contexto

La mayoría de metodologías de gestión del riesgo, incluyendo la metodología ARMA y la metodología ISO, explicadas en el capítulo 2, recomiendan llevar a cabo un análisis del contexto de la organización al iniciar el proceso de apreciación del riesgo. Esto implica realizar un estudio en profundidad del contexto y del entorno en que se encuentra la actividad de la organización. Mediante el establecimiento del contexto, la organización articula sus objetivos, define los parámetros externos e internos a tener en cuenta en la gestión del riesgos, y establece el alcance y los criterios de riesgo para el proceso restante (AENOR 2010, p. 21).

La metodología empleada se basa, principalmente, en la observación y en el análisis del funcionamiento de la organización, así como también en la realización de una serie de entrevistas a los responsables de departamentos seleccionados, que se relacionan directamente con la gestión documental o con la gestión de riesgos.

Es fundamental poder observar cómo se trabaja, en la organización, con relación a la gestión de riesgos y a la gestión de documentos. Esta observación se lleva a cabo en paralelo a la consulta y análisis de aquellos instrumentos existentes para la gestión y prevención de riesgos. Una vez realizado este análisis preliminar, se realiza un estudio del contexto de la organización, tal y como se propone en la normativa internacional ISO.

5.2.1 Análisis preliminar: Entrevistas

Para la comprensión del contexto, es importante poder acceder a la información que disponen aquellas personas que son responsables de gestionar documentos y de gestionar riesgos en la organización. Para ello, se decide emplear la técnica de las entrevistas estructuradas o semi-estructuradas, contemplada en la norma ISO 31010 como una técnica de apreciación del riesgo (AENOR 2011a, p. 26).

En una entrevista estructurada se plantea al entrevistado una serie de preguntas, previamente preparadas, que pretenden que este mire o se acerque a una situación desde una perspectiva distinta a la habitual y, a partir de ahí, identifique los riesgos. Este método es útil cuando resulta complicado reunir a un grupo de gente para hacer una sesión de lluvia de ideas o en los casos en que una discusión en grupo no es apropiada por la situación o por las personas implicadas (AENOR 2011a, p. 32). Es por ello que se decide realizar este tipo de entrevistas, con el objetivo final de obtener diferentes puntos de vista sobre la materia. Además, mediante las entrevistas estructuradas se realizan las mismas preguntas a personas con perfiles y trayectorias diferentes, así como con distintos roles dentro de la organización, que permiten la comparación de respuestas y de perspectivas.

Para ello, se necesita definir una serie de entradas para desarrollar el proceso y obtener los resultados esperados. Las entradas incluyen una lista de personas a entrevistar, una clara definición de los objetivos de la entrevista, y una lista de preguntas.

Para la selección de las personas se realiza un muestreo, seleccionando algunos de los responsables de distintas áreas de la organización, que se relacionan directamente con la toma de decisiones sobre gestión de documentos o sobre gestión de riesgos. Los interlocutores seleccionados son:

1. Responsable del Servicio de Atención Ciudadana. Es la puerta de entrada de documentos en cualquier administración pública, como es el caso de la Organización X. Es por ello que se considera necesario incluir a su responsable como interlocutor en la medida en que los documentos que se reciben en el desarrollo de las funciones de la organización entran por este canal.
2. Responsable del Servicio de Prevención de Riesgos Laborales. Es el departamento que establece e implanta la metodología de gestión de riesgos en la organización, con lo que resulta de vital importancia conocer su perspectiva para este estudio.
3. Responsable del Servicio de Informática. En un momento de transición hacia la administración electrónica, los responsables de nuevas tecnologías de cualquier organización resultan imprescindibles para el desarrollo, aprobación e implantación de metodologías.
4. Responsable del Servicio de Gestión Documental y Archivo. Es el departamento responsable de establecer políticas y definir instrumentos para la gestión de los documentos en la organización, junto con otros departamentos como el de Tecnologías o el de Organización. Se trata del puntal de la Organización X en lo que respecta a la gestión de documentos, fuese en entorno electrónico o en entorno papel.
5. Responsable del Servicio de Organización y Proyectos de Mejora. Es el departamento responsable de normalizar y simplificar procesos y procedimientos de trabajo en la Organización X. Además, la persona responsable de esta área es también la responsable en materia de transparencia dentro del organismo estudiado. Es por ello que, debido a estas dos grandes funciones, se considera necesario incluirla como interlocutora.

Es necesario disponer de una serie de preguntas, a ser posible no concluyentes, para guiar la entrevista. Preguntas sencillas, formuladas en un lenguaje apropiado y que traten un solo tema cada vez. También es recomendable preparar subpreguntas para aclarar posibles respuestas. A la hora de formular las preguntas a los entrevistados se vigila para no guiar la entrevista en uno u otro sentido y es importante realizar las preguntas en el mismo orden cada vez. Eso facilita la posterior comparación entre perspectivas de los entrevistados.

Los objetivos de la realización de entrevistas son:

1. Conocer el grado de conocimiento que los responsables de las áreas involucradas tienen sobre los riesgos documentales.
2. Saber si se conoce alguna metodología de gestión de riesgos en la organización.
3. Conocer si en los diferentes departamentos seleccionados se lleva a cabo algún tipo de control sobre posibles amenazas o riesgos.
4. Conocer el punto de vista de los entrevistados sobre los entornos electrónico y papel, con relación a la existencia de riesgos documentales.
5. Identificar riesgos documentales a los que está expuesta la Organización X.

Para conseguir respuestas sobre todos los objetivos, se definen las preguntas que se enumeran a continuación:

1. ¿Qué es para ti un riesgo? ¿Y un riesgo documental o riesgo de gestión documental?
2. ¿A qué áreas de la organización crees que pueden afectar los riesgos documentales?
3. ¿Crees que tu trabajo puede estar afectado por algún tipo de riesgo documental? ¿Puedes poner algún ejemplo?
4. ¿Sabes si en la organización existe alguna metodología para prevenir o tratar los riesgos? ¿Se te ha explicado alguna vez dicha metodología?
5. En caso de que la respuesta anterior sea afirmativa, ¿te parece adecuada también para el control de los documentos que generas y gestionas en tu día a día?
6. ¿En tu departamento lleváis a cabo algún control sobre los posibles riesgos documentales? ¿Consideras que sería necesario?
7. ¿Consideras que existe un mayor riesgo al trabajar con documentos electrónicos? ¿Por qué sí/no?

En la siguiente figura se puede ver la relación entre las preguntas y los objetivos planteados (ver Figura 29).

OBJETIVOS	PREGUNTAS						
	1	2	3	4	5	6	7
1	X	X	X				
2				X	X	X	
3				X	X	X	
4		X	X				X
5	X	X	X		X	X	X

Figura 29 – Correlación entre objetivos y preguntas de las entrevistas estructuradas (elaboración propia).

Cabe destacar que con esta entrevista no se pretende evaluar los conocimientos técnicos ni evaluar a las personas implicadas, sino conocer el estado de la cuestión dentro de la Organización X. El resultado obtenido (ver Anexo C para la transcripción no literal de las entrevistas) es la visión de cada uno de los entrevistados sobre las problemáticas o cuestiones tratadas en la entrevista.

Como todos los métodos y técnicas de investigación, las entrevistas estructuradas tienen fortalezas y debilidades a considerar.

Las fortalezas incluyen:

- Las entrevistas estructuradas permiten a las personas considerar con tiempo sus ideas sobre una determinada cuestión.
- La comunicación en privado puede permitir una mayor profundización sobre las cuestiones tratadas.
- Permiten la participación de un amplio número de personas.

Las debilidades incluyen:

- Conlleva mucho tiempo para el investigador obtener las respuestas.
- El sesgo se tolera y no se elimina a través de una discusión de grupo.

Se realizan cinco entrevistas. El 80 % de las entrevistas se realizan en persona y el 20 % restante mediante videoconferencia, debido a la falta de disponibilidad del entrevistado. Se acuerda previamente un calendario para la realización de las entrevistas (ver Anexo C). A continuación, se presentan las conclusiones a las que se llega a partir de la información obtenida de las entrevistas.

Conclusiones de las entrevistas

Todos los entrevistados son capaces de dar una definición de riesgo documental. De esto se deduce que, ya sea de manera consciente o inconsciente, todos identifican alguna situación de riesgo en la gestión de los documentos en su día a día. De hecho, la práctica totalidad de los entrevistados incluye, a la hora de dar una definición, el mismo ejemplo de no poder localizar un documento en el momento en que se necesita. Este ejemplo lo contextualizan en su actividad diaria y cada uno de ellos afirma haber vivido dicha situación en más de una ocasión.

Los entrevistados, al contestar a la pregunta 1, mayoritariamente consideran los riesgos como algo negativo o que implica consecuencias negativas para la organización. De esta visión se desmarca claramente el responsable de informática, que afirma que tener los riesgos identificados es algo positivo, puesto que pueden controlarse y prevenirse. Esta percepción mayoritariamente negativa contrasta con las respuestas que dan a la pregunta 6; acerca de la metodología de gestión de riesgos, los entrevistados cambian su percepción, y consideran que es algo muy positivo para su día a día. Es decir, la visión cambia en función de si se habla de riesgos con relación a una definición o a una metodología.

Otra cuestión en la que los entrevistados se muestran de acuerdo es en la posible afectación de riesgos documentales sobre todas las áreas de la organización. Explican que, en la medida en que todas generan y gestionan documentos, todas pueden estar expuestas a riesgos documentales. El responsable de Atención Ciudadana destaca

como áreas críticas los departamentos de Urbanismo y de Seguridad Ciudadana, debido al gran volumen de documentación que gestionan. Por parte del responsable de Informática, se destacan como críticas el área de Gestión Documental y Archivo y la propia área de Informática, debido a sus responsabilidades a la hora de garantizar el control y la gestión adecuada de la información y la documentación.

En cuanto a metodología, a partir de las respuestas de los entrevistados, se deduce que existen, al menos, dos métodos para la prevención de riesgos. El primero, y más conocido, es el relacionado con la prevención de riesgos laborales. El segundo se basa en la aplicación del ENS. Resulta destacable que el 60 % de los entrevistados manifieste no haber recibido formación sobre la prevención de riesgos laborales, ni conocer la metodología. El 40 % restante sí que la conoce y manifiesta haber recibido capacitación al respecto.

Con relación a la posible aplicación de las metodologías de gestión del riesgo existentes en la Organización X a la gestión de sus documentos, se cuenta con las respuestas de las dos personas expertas en riesgos laborales y en seguridad de la información. Ambos entrevistados afirman que la metodología que utilizan es perfectamente aplicable a la gestión de documentos y que esto es positivo para la organización. El resto de entrevistados manifiesta su desconocimiento al respecto.

El 60 % de los entrevistados afirma que en su departamento se lleva a cabo algún control sobre posibles amenazas o riesgos documentales. Concretamente, el área de Informática sigue la metodología del ENS para garantizar la protección adecuada de la información y los servicios que proporcionan a la organización. El área de Gestión Documental y Archivo no dispone de una metodología establecida, pero afirma actuar en función de las necesidades y las incidencias que se detecten, por tanto, se deduce que su gestión es más correctiva que preventiva. Por otro lado, el área de Organización y Proyectos de Mejora afirma que se llevan a cabo acciones de concienciación y formación como método preventivo, aunque no disponen de un protocolo o metodología implantada y aprobada. El 40 % restante afirma no llevar a cabo ningún control sobre los riesgos documentales en sus departamentos respectivos.

El 100 % de los entrevistados considera necesario disponer de una metodología de gestión de riesgos documentales. Algunos de ellos, además, lo consideran de vital importancia para el correcto funcionamiento de la organización. Se deduce que, pese a la inexistencia de protocolos establecidos, sí existe conciencia de la necesidad de gestionar y prevenir las situaciones de riesgo documental en la Organización X. En algunas áreas, de hecho, se ha intentado dar respuesta a estas situaciones desde el desconocimiento y la buena voluntad, trabajando en función de las necesidades y las urgencias detectadas pese a no disponer de pautas claras sobre cómo proceder. La formación y la concienciación son instrumentos de prevención adecuados, pero no suficientes.

La percepción de los entrevistados sobre si existe un mayor riesgo en entornos electrónicos o en papel no coincide. Un 40 % de los entrevistados opina que existe mayor riesgo en el entorno en papel. De este porcentaje, cabe diferenciar entre la opinión del responsable de Informática y la del responsable de Atención Ciudadana, basadas en contextos distintos. El primero basa su percepción en la experiencia y el conocimiento en profundidad de los entornos tecnológicos y en el uso del ENS como medida de control y prevención en dichos entornos, mientras que el segundo basa su percepción en diferentes situaciones de riesgo documental a las que debe enfrentarse, como el traslado descontrolado de documentos o la deficiencia en los depósitos de archivo, que puede ocasionar la pérdida de información en soporte papel. En cualquier caso, cabe añadir que este último afirma que el entorno electrónico es más seguro, siempre y cuando se gestione de manera adecuada.

Por otro lado, un 20 % de los entrevistados opina que existe un mayor riesgo en entornos electrónicos. Esta es la opinión del responsable de prevención de riesgos laborales, que basa su percepción en el desconocimiento del funcionamiento de las nuevas aplicaciones con las que debe trabajar debido, según manifiesta, a una falta de formación y a lo que él considera una mala gestión del cambio.

El 40 % restante manifiesta que no hay mayor o menor riesgo según el entorno, sino que lo que se dan son diferentes tipos de riesgos y el modo de abordar su prevención y corrección varía en función de este. Esta es la opinión compartida del responsable de Gestión Documental y Archivo y del responsable de Organización y Proyectos de Mejora, ambos perfiles relacionados directamente con la gestión de documentos dentro de la Organización X, así como también con las políticas de transparencia y publicidad activa.

Existe, por tanto, una división de criterios en función del ámbito de trabajo y especialización de los entrevistados, así como en función de su experiencia personal con situaciones de riesgo. Cabe destacar la percepción del responsable de prevención de riesgos laborales con relación a la gestión del cambio en la organización, así como sobre la falta de formación acerca de la transición a la administración electrónica. Para este, es fundamental informar, formar y concienciar sobre esta transformación a todos los trabajadores para conseguir su compromiso e implicación, además de para evitar y prevenir fallos e incidencias que puedan derivar en situaciones de riesgo. Por tanto, es necesario desarrollar una estrategia adecuada de gestión del cambio.

En línea con esta falta de formación manifestada por el responsable de Riesgos Laborales, él mismo identifica como un riesgo la falta de directrices claras sobre la gestión documental, tanto en entorno papel como en electrónico. A esto puede añadirse el riesgo que identifica el responsable de Gestión Documental sobre la falta de formación de los trabajadores en materia de procedimiento administrativo. Sumando estos dos factores pueden identificarse numerosos riesgos susceptibles de afectar a los documentos en las diferentes etapas del ciclo de vida. De hecho, todos los entrevistados identifican diferentes riesgos que se pueden relacionar directamente con la falta de formación, como son: descontrol de la documentación durante la tramitación, pérdida de documentos en los traslados entre departamentos, eliminaciones no autorizadas, incumplimiento de los procedimientos de transferencia y préstamo, no documentación de trámites administrativos, entre otros.

Una situación de riesgo que identifica el 60 % de los entrevistados es la de las malas condiciones de los depósitos de archivo, lo que puede ocasionar pérdidas o deterioro de los documentos, en este caso en papel. Los entrevistados mencionan problemas de humedades, goteras, presencia de insectos, entre otros. Además, en muchas ocasiones no hay controles de acceso a dichos depósitos con las posibles consecuencias de pérdidas, robos, accesos indebidos o eliminaciones no autorizadas, entre otras. Con relación a este último riesgo, el responsable del área de Organización y Proyectos de Mejora menciona también la falta de criterios sobre el acceso a los documentos. Lo relaciona con las solicitudes de acceso a información pública que pueden tramitar los ciudadanos, si bien en esta línea también se menciona por otros entrevistados la falta de control en el acceso a la documentación. De esto se deduce que no existen directrices claras al respecto en la Organización X.

Cabe destacar la falta de recursos que menciona el responsable de Gestión Documental. Más que un riesgo, se puede considerar como la causa de otras carencias que no permiten planificar una formación completa en la organización, llevar el control de las transferencias o asegurar el cumplimiento del calendario de transferencias, entre otras cuestiones planteadas por este entrevistado.

5.2.2 Descripción de la Organización X

El estudio del contexto se realiza de acuerdo con la información recopilada a través de documentos, instrumentos, directrices y otros materiales que explican la estructura organizativa de la organización, haciendo especial énfasis en todo lo relacionado con la gestión documental. También se emplea la información obtenida de las entrevistas realizadas al personal y de la observación directa en las visitas a las instalaciones.

El análisis del contexto se centra especialmente, por tanto, en los aspectos relacionados con la gestión de documentos en la Organización X, debido a que el objetivo es llevar a cabo el proceso de gestión del riesgo aplicado a la gestión de documentos. Para realizar dicho análisis, se sigue lo indicado en el informe técnico internacional ISO/TR 18128, en sus apartados 5.2 y 5.3. Esto implica considerar, para el contexto externo, los entornos político-social, macroeconómico, tecnológico, físico y de infraestructura, así como amenazas de seguridad externas, y para el contexto interno, los cambios en la organización o en los recursos económicos y materiales.

La Organización X es una administración pública municipal situada en la provincia de Barcelona. Cuenta con una población de más de 100.000 habitantes. Con relación al contexto político-social, las últimas elecciones municipales del año 2015 no supusieron un gran cambio en el municipio, puesto que se mantiene el mismo partido político y el mismo alcalde que en las elecciones municipales anteriores, del año 2011. Esto proporciona estabilidad a la organización.

Con relación al contexto social y económico, durante los últimos años la población vivió una crisis económica, iniciada en 2007, que generó un descenso demográfico substancial, alcanzando su máximo el año 2014 con una disminución del 5 % de la población extranjera, situando los niveles en cifras inferiores a las del año 2005. La recuperación económica de los últimos dos años ha permitido una ligera recuperación al alza. Cabe remarcar que el grupo de edad que más ha crecido durante los últimos cinco años son las personas mayores de 65 años. Este envejecimiento de la población responde a la estructura poblacional, así como al aumento de la esperanza de vida.

Desde el año 2007, el impacto de la crisis económica disparó el número de personas usuarias de los servicios sociales de la ciudad, repercutiendo esto en la actividad y el incremento de los presupuestos del ayuntamiento destinados a los servicios sociales para atender a las demandas de la ciudadanía. Cabe destacar que el análisis de la evolución del mercado que el propio ayuntamiento realiza de manera periódica es optimista y revela una tendencia a la baja en el paro, así como una recuperación del mercado de trabajo en el municipio. En el ámbito empresarial, el municipio no solo ha conseguido mantener la estabilidad durante estos últimos años, sino que se ha experimentado un pequeño crecimiento, según las estadísticas municipales, sobre todo de las pequeñas y medianas empresas y el sector servicios.

En el ámbito tecnológico, organizativo y legal, la aprobación de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y de la Ley 40/2015, de 1 de octubre, de Régimen

Jurídico del Sector Público⁷⁶ supone una aceleración en la transformación digital de las administraciones públicas. Esto conlleva una mayor inversión en nuevas tecnologías y cambios en algunos procesos de trabajo, con el fin de sistematizarlos y automatizarlos, en aras de conseguir una administración electrónica real. Esta transformación afecta de manera directa a la gestión de documentos de la Organización X. De hecho, uno de los objetivos principales de estas leyes es la eliminación del papel, y basa el funcionamiento de las administraciones públicas en un entorno íntegramente electrónico. Esta transformación no puede producirse en un periodo corto de tiempo, sino que implica grandes cambios, no solamente con relación a los procesos o los nuevos dispositivos, sino con respecto al nivel cultural de los trabajadores.

La Organización X está inmersa, por tanto, en un proceso de transformación digital hacia la administración electrónica dentro de este contexto. La aprobación del *Proyecto de diseño e implementación del sistema de gestión documental*, por parte de dicha organización en el año 2013, señala el primer paso hacia la progresiva normalización de la gestión de documentos. A este proyecto le sigue la aprobación del *Plan Director del Documento Electrónico* y el desarrollo del *Modelo de gestión del documento y expediente electrónicos*, este último actualmente en revisión y pendiente de aprobación formal. El Plan Director pretende dar cumplimiento a las obligaciones establecidas por la legislación vigente y dar continuidad a los proyectos de administración electrónica que ya se habían ejecutado, fijando un criterio corporativo homogéneo para explotar al máximo las ventajas del nuevo modelo de gestión electrónica. En este plan se describen las acciones a realizar por la Organización X a corto, medio y largo plazo para su adaptación a la administración electrónica. Además de estos dos instrumentos, la organización cuenta con una *Ordenanza reguladora de la administración electrónica* del año 2010, aunque este documento ha quedado desactualizado con las nuevas leyes de procedimiento administrativo aprobadas el año 2015. Tenía como objetivo la regulación de la utilización de las herramientas de la sociedad de la información y el conocimiento en las relaciones jurídico-administrativas entre los ciudadanos y el conjunto de la administración municipal. Establecía el régimen jurídico básico de la administración electrónica en la administración municipal y, sobre esto, las disposiciones para una implantación progresiva de la administración electrónica.

Uno de los propósitos contemplados en el Plan Director es disponer de un gestor documental único, donde todas las herramientas de tramitación almacenen documentos electrónicos. Actualmente, se está trabajando en la integración de la herramienta *Alfresco*⁷⁷ con *eArchivo*⁷⁸ como gestor documental y gestor de expedientes, y con

⁷⁶ – La aprobación de las leyes 39/2015 y 40/2015 configura un escenario en el que la tramitación electrónica debe constituir la actuación habitual de las administraciones en sus múltiples vertientes de gestión interna, de relación con los ciudadanos y de relación de aquellas entre sí. En la Ley 39/2015 se establecen cuestiones tales como que los actos administrativos se producirán por escrito a través de medios electrónicos y que los documentos administrativos se emitirán igualmente por escrito a través de medios electrónicos; mientras que la Ley 40/2015 establece que las administraciones públicas se relacionarán entre sí y con sus órganos a través de medios electrónicos.

⁷⁷ – *Alfresco* es un sistema de administración de contenidos de código fuente libre, desarrollado en Java, basado en estándares abiertos y de escala empresarial para sistemas operativos tipo Windows, Unix Solaris y algunas versiones de Linux. Se puede consultar más información en su página web: https://www.alfresco.com/es/?sl_redirect=1 (consultado el 08/08/2017).

⁷⁸ – Es una solución de la empresa Tecsidel. *eArchivo* dispone de los elementos necesarios para dar soporte al modelo de gestión documental definido por la organización cliente. Se trata, según la empresa, de una solución corporativa para el almacenamiento y preservación de cualquier documento, tanto en electrónico como en papel. Se puede consultar más información sobre las funcionalidades en su página web: <http://www.tecsidel.com/es/productos/eadmin/earchivo#1-funcionalidades> (consultado el 08/08/2017).

*iArxiu*⁷⁹ para el objetivo de preservación a largo plazo de los documentos y expedientes electrónicos. Se contempla con estas herramientas todo el ciclo de vida del documento.

Además, la Organización X trabaja, actualmente, con más de 15 aplicaciones (propias o externas) para distintas funcionalidades, que mayoritariamente tienen en cuenta la gestión de documentos en soporte papel. Esto dificulta la gestión de documentos integrada en las plataformas mencionadas, tanto por la complejidad de adaptación del conjunto de aplicaciones a un entorno de documento electrónico como por la dispersión de metodologías.

Con respecto a las amenazas de seguridad externas, la organización trabaja de acuerdo al ENS, realizando auditorías periódicas en materia de vulnerabilidades y amenazas que se relacionen con la tecnología con la que se trabaja. También se tiene en cuenta el estándar internacional ISO 27001, de Sistema de Gestión de Seguridad de la Información (SGSI). La organización no está certificada con esta norma ISO, pero sigue sus lineamientos. En cualquier caso, las vulnerabilidades están identificadas y se trabaja desde el área de Informática para su control y prevención en el día a día.

Cabe mencionar que uno de los cuatro objetivos de ciudad del Plan de Actuación Municipal para el periodo 2016-2019 se centra en el gobierno abierto, con la intención de profundizar en la transparencia de la acción de gobierno y en la participación ciudadana. Este objetivo se relaciona directamente con la rendición de cuentas y el control de la actividad municipal. Se menciona, también, en este documento el impulso de la administración electrónica y la simplificación administrativa dentro de la necesidad de actualizar la relación de la administración con los ciudadanos. Estos objetivos se enmarcan dentro del cambio legislativo comentado, que hace necesaria una inversión económica en el análisis y actualización del funcionamiento administrativo de la organización, incluyendo su gestión de documentos y de información.

⁷⁹ – *iArxiu* es un servicio, prestado por el Consorcio de Administración Abierta de Cataluña, de preservación y archivo electrónico que garantiza que los expedientes/documentos que genera o recibe una organización en el ejercicio de sus funciones se mantengan íntegros, fiables, auténticos y accesibles a lo largo de su ciclo de vida. Es un servicio dirigido a todas las administraciones públicas catalanas que deban preservar documentos electrónicos a largo plazo y que necesiten garantizar la autenticidad y la integridad de sus contenidos, así como la accesibilidad, la disponibilidad y su legalidad. Se puede consultar más información en su página web: <https://www.aoc.cat/serveis-aoc/i-arxiu/> (consultado el 08/08/2017).

5.2.3 Estructura organizativa

En el ámbito organizativo, la gestión de la administración municipal se divide en seis grandes áreas y subáreas, que se enumeran a continuación:

- Área de Alcaldía – Presidencia
 - Concejalía de Gobierno de Participación Ciudadana
- Área de Coordinación, Planificación, Desarrollo Económico y Ocupación
 - Concejalía de Gobierno y Turismo y Desarrollo Económico
 - Concejalía de Gobierno de Comercio y Derechos de los Consumidores
 - Concejalía de Gobierno de Innovación Social
- Área de Seguridad, Convivencia y Civismo
- Área de Bienestar y Derechos Sociales
 - Concejalía de Gobierno de Bienestar Social
 - Concejalía de Gobierno de Educación
 - Concejalía de Gobierno de Cultura
 - Concejalía de Gobierno de Igualdad y Personas Mayores
 - Concejalía adjunta de Sanidad y Salubridad Pública
- Área de Espacio Público, Vivienda, Urbanismo y Sostenibilidad
 - Concejalía adjunta de Medio Ambiente y Sostenibilidad
- Área de Hacienda y Servicios Centrales

Las funciones asignadas a cada una de las áreas, así como las dependencias y relaciones entre ellas, están aprobadas mediante decreto de alcaldía. A continuación, se describen de manera general su composición y sus funciones por áreas.

- Área de Alcaldía – Presidencia: en esta área se encuentran diferentes subáreas, como son el Gabinete de Alcaldía, la Gerencia Municipal, la Participación, la Asesoría Jurídica, la Secretaría Técnica de la Junta de Gobierno Local y el Tribunal económico administrativo de la organización. Dentro de las funciones del Gabinete de Alcaldía se encuentran la asistencia a la alcaldía y a los grupos políticos municipales, las relaciones externas e institucionales, aspectos de comunicación e imagen corporativa, así como también el análisis y prospectiva de lo relacionado con el *Open Data*. La Gerencia Municipal se encarga de la dirección ejecutiva superior del Ayuntamiento y del establecimiento de los mecanismos para desarrollar sus tareas de coordinación con el resto de los órganos directivos. Para ello, tiene asignadas las funciones de impulso y seguimiento ejecutivo de la actuación municipal, la organización y desarrollo de proyectos de desarrollo

del modelo de gestión corporativa, administración electrónica, archivo y sistema de gestión documental municipales, así como coordinación de la comunicación interna, la elaboración y seguimiento del Plan de Actuación Municipal y la responsabilidad sobre el objetivo y las obligaciones de transparencia. La subárea de Participación lleva a cabo el diseño, elaboración e impulso de los programas en materia de participación. Asesoría Jurídica se encarga, entre otras funciones, de la asistencia jurídica a la Alcaldía y a la Junta de Gobierno Local, así como a los órganos directivos con relación a sus funciones y competencias. Por su parte, la Secretaría técnica de la Junta de Gobierno Local tiene como función principal la asistencia al Concejal Secretario de la Junta de Gobierno Local, así como la gestión de dichas juntas, el archivo y custodia de la documentación y el resto de funciones contempladas en la Ley 7/1985, de 2 de abril, reguladora de las bases de régimen local. A la Secretaría general del Pleno se le atribuyen funciones con relación a la Presidencia del Pleno, las Comisiones, Junta de Portavoces, entre otras. Por último, al Tribunal económico administrativo de la Organización X se le atribuyen las funciones relativas a la resolución de las reclamaciones económico administrativas de conformidad con el Reglamento Orgánico del Tribunal Económico Administrativo vigente en la organización desde el año 2012.

- Área de Coordinación, Planificación, Desarrollo Económico y Ocupación: en esta área se encuentran distintas subáreas de las que se explican, de manera general, sus funciones y competencias. Gestión general del área se encarga de la coordinación de la actuación de las concejalías de gobierno delegadas, la resolución de procedimientos y el seguimiento de las subvenciones obtenidas en materias que se gestionan desde el área. Coordinación lleva la iniciativa y coordina la elaboración de la normativa orgánica municipal, las actividades relacionadas con los procesos electorales y las subvenciones relacionadas con fondos de otras administraciones públicas nacionales o internacionales, entre otras funciones. Planificación se encarga de la coordinación y la elaboración de las directrices necesarias para la actuación municipal, el diseño e impulso de los planes estratégicos del municipio, proyectos de ciudad y la dirección del Plan de Actuación Municipal (PAM). Por su parte, la Agencia de Desarrollo Urbano es un órgano especial sin personalidad jurídica que desarrolla las funciones de desarrollo y alta dirección del conjunto de políticas estratégicas de carácter urbanístico. También el estudio, análisis e implantación de las estrategias de desarrollo urbanístico, así como la búsqueda de medidas para dicho desarrollo, la tramitación de procedimientos administrativos relacionados, entre otras competencias. La subárea de Innovación social lleva a cabo el diseño e implantación de las políticas de nuevas tecnologías como una herramienta de interacción entre los ciudadanos y el Ayuntamiento, estrategias de innovación y búsqueda de fórmulas de colaboración interadministrativa. Formación y Ocupación se encargan del impulso a distintos programas y proyectos para el fomento de la ocupación y la formación ocupacional, relaciones con otras instituciones para la dinamización económica, tramitación de convenios, procedimientos o programas con distintas finalidades con relación a la formación y la ocupación. Turismo gestiona el diseño e implantación de las estrategias de políticas públicas de promoción turística de la ciudad, así como otros programas de desarrollo turístico. Desarrollo económico, entre otras responsabilidades, se encarga del diseño de políticas públicas transversales destinadas a la mejora del tejido económico municipal y las sinergias entre la administración y la empresa, así como el desarrollo de instrumentos para la potenciación del desarrollo económico de la ciudad, la promoción de formas para el emprendimiento y la empresa o la participación municipal en los proyectos empresariales. Comercio gestiona y tramita los programas para el desarrollo y promoción en coordinación con otros agentes comerciales, como entidades asociativas en materia de comercio, y lleva a cabo la tramitación de procedimientos relativos a la otorgación de ayudas, subvenciones u otras medidas. Mercados se encarga de la coordinación, gestión, inspección, control e intervención de los Mercados Municipales, así como también

de la regulación de los Mercados no sedentarios. Consumo, por su parte, consta de dos subáreas. Por un lado, la Oficina Municipal de Información al Consumidor (OMIC), que lleva a cabo actuaciones dirigidas a la defensa de los consumidores y usuarios. Por otro lado, la Junta Arbitral de Consumo, que se encarga de tramitar aquellos procedimientos que las partes litigantes en conflicto someten a este órgano de conformidad, la regulación de quejas o reclamaciones tanto de consumidores como de empresarios. Finalmente, la subárea de Cooperación y Solidaridad asume el diseño de las políticas y los programas de cooperación y solidaridad, así como la elaboración, control y ejecución de dichos programas.

- Área de Seguridad, Convivencia y Civismo: esta área engloba temas de movilidad y transporte, ocupación de la vía pública, guardia urbana, protección civil, así como sanciones de tráfico y una subárea de convivencia y civismo. Existe también un departamento de Servicios Generales que se encarga de la dirección, planificación, control y coordinación de los servicios del Área, la coordinación del Plan Local de Seguridad y de la Junta Local de Seguridad, así como otras funciones de coordinación. Por su parte, Convivencia y Civismo gestionan las situaciones e incidencias con relación a la convivencia que se puedan producir, elaboran y proponen programas para la promoción y la defensa de políticas relacionadas con el civismo y la convivencia, así como otras actividades relacionadas.

- Área de Bienestar y Derechos Sociales: cuenta con una subárea de gestión general que se encarga de la coordinación de la actuación de las concejalías de gobierno delegadas en las materias del área, así como de la coordinación y gestión de los programas de voluntariado vinculados a dicha área. También cuenta con Servicios Sociales, Infancia y Adolescencia, Dependencia y Discapacidad, LGTBI, Ciudadanía e Integración, Salud, Personas Mayores, Igualdad, Educación, Cultura, Deportes, y Juventud. Se trata de un área con mucha diversificación. Diseña la política en materia de servicios sociales y se encarga de la realización de los estudios necesarios para el correcto desarrollo de los programas y servicios del área, así como también otras gestiones como el comedor social o el servicio residencial de estancia limitada, entre otras. Infancia y Adolescencia diseña las políticas y desarrolla los programas con relación a la infancia y la adolescencia para la ciudad, en especial para aquella en riesgo de desventaja social. Dependencia y Discapacidad elabora y gestiona los programas de atención a las personas con discapacidad física, psíquica y/o sensorial, así como también los programas de atención a la dependencia, la gestión del servicio de teleasistencia o de ayuda al domicilio, entre otras funciones. La subárea LGTBI impulsa políticas contra la homofobia y la transfobia, coordina acciones de sensibilización y visualización en materias de LGTBI, así como en defensa de los derechos y libertades de las personas de este colectivo. Por su parte, Ciudadanía e Integración define y gestiona programas dirigidos a la integración de las personas extranjeras, la información y asesoramiento a los nuevos empadronados, así como el seguimiento de estas acciones. Salud tiene asignadas las competencias conforme a la Ley General de Sanidad, la Ley de Bases de Régimen Local y la Ley 18/2009, de 22 de octubre, de Salud Pública de Cataluña. Personas Mayores diseña las políticas encaminadas a la defensa y protección de este colectivo, así como planes y programas, subvenciones y prestación de servicios en los hogares para personas mayores. Educación, a través de la Oficina Municipal de Escolarización, participa en los procesos de matriculación de los centros públicos; llevan a cabo estudios sobre la escolarización en función del censo de población, diseñan el mapa escolar, participan en el diseño de la oferta educativa de ámbito municipal y realizan tareas de coordinación, organización y gestión de diferentes entidades formativas, como por ejemplo la Escuela Municipal de Música o el Centro de Normalización Lingüística del municipio, entre otros. Cultura gestiona las competencias municipales en materia de cultura en sus diversos ámbitos

sectoriales, como son el patrimonio histórico y cultural, la cultura popular y tradicional, el fomento de la lectura pública, la creación, y la formación y difusión artística. La subárea de Deportes tiene como funciones el establecimiento de las necesidades, el régimen de utilización y la iniciativa en la determinación de la forma de gestión de las instalaciones deportivas de propiedad municipal; también tramita los procedimientos de contratación de la gestión de instalaciones deportivas que son propiedad municipal, se encarga de promocionar el deporte, organizar competiciones, gestionar subvenciones, el control y seguimiento de concesiones sobre instalaciones deportivas de titularidad municipal, entre otras responsabilidades. Por último, Juventud establece, gestiona y coordina las políticas públicas en materia de juventud y los recursos destinados a dichas políticas; gestiona la Oficina Joven de Emancipación, colabora con entidades y asociaciones juveniles, gestiona subvenciones y tramita los procedimientos administrativos para el ejercicio de las actividades, los programas y los servicios en materia de juventud que lleve a cabo el Ayuntamiento.

- Área de Espacio Público, Vivienda, Urbanismo y Sostenibilidad: en esta área se enmarcan cuestiones como medio ambiente, urbanismo, parques y jardines o servicios funerarios y cementerio. Existe una subárea de gestión general que se encarga de la planificación, dirección y control de los servicios, proyectos y las actuaciones dirigidas a la consecución de los objetivos fijados por el área en materia de urbanismo, obras públicas, actividades, creación y mantenimiento de las infraestructuras urbanas y las zonas verdes municipales, así como la limpieza del espacio público y la eliminación de residuos. Medio Ambiente y Sostenibilidad impulsa, coordina y supervisa la ejecución de los programas, proyectos y estudios municipales con relación a los aspectos medioambientales y de protección de la naturaleza, promueve la participación ciudadana en estas cuestiones y tramita los procedimientos necesarios para llevarlas a cabo. Proyectos de Obras redacta o supervisa la redacción de los proyectos y la dirección de la ejecución o su supervisión de los anteproyectos y de los proyectos ejecutivos de conservación, remodelación y nueva construcción de las obras relativas a la infraestructura urbana, la urbanización, alcantarillado, alumbrado público y la ejecución de la instalación de la red de semáforos, la red de comunicaciones de la ciudad, así como los proyectos de urbanización y remodelación del espacio público. Por su parte, Obras y Mantenimiento de los Edificios Públicos coordina y dirige la fase de redacción del proyecto y la de ejecución, de las obras de reforma o remodelación, derribo, rehabilitación, ampliación y nueva construcción de los edificios municipales. Infraestructuras Urbanas y Espacio Público se encarga de la planificación, supervisión y coordinación de las obras de construcción y las instalaciones destinadas a la renovación y el mantenimiento del alcantarillado, alumbrado público, obras de urbanización y, en general, de las relativas a la infraestructura urbana. Por su parte, Urbanismo y Actividades tramita los expedientes en materia urbanística a iniciativa de la Agencia de Desarrollo Urbano, para otorgar licencias, autorizaciones, permisos, comunicaciones previas y declaraciones responsables sometidas a la normativa urbanística; gestiona el nomenclátor de la ciudad; también se encarga del control de la legalidad urbanística, incluyendo todos los trámites asociados a dicho control. Vivienda gestiona la Oficina Municipal de Vivienda, asesora a la ciudadanía en materias relacionadas con vivienda, concesiones de ayudas para la rehabilitación de viviendas, alquiler social y, en general, cualquier otro procedimiento o actividad relacionado con el acceso a la vivienda que lleve a cabo el Ayuntamiento. La subárea de Limpieza Viaria, Saneamiento y Mantenimiento de Parques y Jardines planifica, dirige y supervisa los servicios de limpieza viaria, de recogida de residuos municipales, conservación de zonas verdes, mantenimiento del arbolado y de los elementos de ocio en el espacio público. Sistemas de Información Geográfica y Cartografía coordina y gestiona el servicio de cartografía de la ciudad, definiendo el estándar de la plataforma gráfica del municipio y el mantenimiento gráfico de las modificaciones producidas en la ciudad y su digitalización definitiva; se coordina con el resto de áreas del ayuntamiento para unificar las bases de datos del Sistema

de Información Geográfica y Territorial (SIGT), realiza tareas topográficas, actualiza la red topográfica de la ciudad y sus bases de datos, y se encarga de la confección y mantenimiento de nomenclátor vigente. Servicios Funerarios y Cementerio gestiona, controla y mantiene el cementerio, así como también realiza los trámites para la gestión administrativa de los derechos funerarios, prestación del servicio y las actividades de inhumaciones, exhumaciones, traslados y otras actividades propias del cementerio municipal. Por último, la subárea de Apoyo al Territorio lleva a cabo la actividad de apoyo común a los servicios del área y a los distritos para la comprobación de las incidencias que se producen en el territorio con relación a todo lo que hace referencia al mantenimiento del espacio público, la limpieza de la ciudad, la recogida de residuos y las infraestructuras para la realización de actos.

- Área de Hacienda y Servicios Centrales: se compone de distintas subáreas, tal como se explica a continuación. La primera de ellas es Intervención General Municipal, a la cual corresponden las funciones de control y fiscalización interna de la gestión económico financiera y presupuestaria en la triple acepción de función interventora, función de control financiero y función de control de eficacia con plena independencia. La subárea de Contabilidad, por su parte, lleva y desarrolla la contabilidad financiera y la ejecución del presupuesto, así como también el registro de facturas, la coordinación de las funciones o actividades contables del Ayuntamiento y otras funciones contables. Tesorería Municipal tiene asignadas las funciones que los artículos 194 y siguientes del Real Decreto Legislativo 2/2004, que aprueba la Ley Reguladora de las Haciendas Locales le atribuye, como, por ejemplo, la elaboración de la planificación financiera y el plan de disposición de fondos del Ayuntamiento, el presupuesto de la tesorería y la gestión de los pagos de la hacienda municipal, entre otras funciones. Programación y Presupuestos organiza y coordina las funciones relativas a la preparación y elaboración de los presupuestos del Ayuntamiento, elabora los planes de saneamiento financiero, el análisis y evaluación de los programas de ingresos y de gastos que integran el presupuesto, así como otras funciones relacionadas. Gestión Tributaria determina las directrices generales en materia de imposición, gestión e inspección de los tributos y precios públicos locales. Patrimonio y Seguros gestiona el Inventario de Bienes y Derechos Municipales, el Inventario del Patrimonio Municipal del Suelo y la Vivienda, y realiza las tramitaciones de los procedimientos necesarios para su mantenimiento. Contratación tramita los procedimientos de contratación de obras, concesión de obra pública, gestión de servicios públicos, suministro, servicios, contratos administrativos especiales y contratos privados, así como los contratos sometidos a la legislación patrimonial sea cual sea la cuantía y su ejecución legal, teniendo en cuenta que la iniciativa corresponde a las áreas y subáreas en atención a las materias, actividades y servicios que gestionan. Servicios Centrales se encarga de la adquisición centralizada y la distribución de materiales y suministros para atender las necesidades comunes de todos los servicios, centros y dependencias del Ayuntamiento (que no estén atribuidos a ninguna otra área o subárea) así como la adquisición y mantenimiento de los vehículos oficiales, el control de los suministros de agua, gas y electricidad, entre otras funciones. Recursos Humanos tramita los procedimientos para la organización de la estructura administrativa del personal y el catálogo de puestos de trabajo, en coordinación y colaboración con las diferentes áreas de gestión del Ayuntamiento, también gestiona los expedientes relativos a la plantilla de personal, relación de puestos de trabajo, selección, perfeccionamiento y promoción del personal, gestiona las relaciones laborales o los expedientes disciplinarios, entre otros. Tecnologías de Información y Sistemas gestiona el sistema de informática municipal y da soporte a la interrelación de los procesos y sistemas con otras administraciones públicas, gestiona la intranet y la página web municipal, gestiona los procedimientos dirigidos al cumplimiento de la normativa sobre protección de datos de carácter personal, elabora los protocolos y políticas de auditoría de seguridad de acuerdo con el Esquema Nacional de Seguridad, diseña las plataformas y las

tecnologías de base municipal, atiende las incidencias que puedan darse y en general se encarga del resto de actuaciones destinadas a la gestión del sistema informático municipal que no se encuentren asignadas a otras áreas o subáreas. Población gestiona el Padrón Municipal de Habitantes, coordina el Censo Electoral del municipio junto con la Oficina del Censo Electoral, notifica las designaciones de las Mesas Electorales y tramita los procedimientos previstos en la legislación para el mantenimiento y revisión del Padrón Municipal de Habitantes. Por último, Atención Ciudadana proporciona información al ciudadano sobre los trámites y servicios que presta el Ayuntamiento o sobre la ciudad, gestiona la Oficina de Atención Ciudadana, gestiona y coordina todos los puntos municipales de atención e información al ciudadano, así como los sistemas de información telefónica municipales.

5.2.4 Descripción de las metodologías de gestión de riesgos existentes en la Organización X

En la Organización X existe un procedimiento para la evaluación de riesgos laborales desarrollado y aprobado formalmente en el año 2010. Este se basa en la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales. En su introducción expone que la prevención de riesgos laborales debe integrarse en el sistema general de gestión de la organización. Considera el proceso como cíclico, en la medida en que debe realizarse la evaluación de riesgos de manera periódica y dinámica. La metodología empleada en la Organización X sigue las siguientes fases:

1. Identificación de los riesgos: realizada a partir de la información obtenida sobre la organización, características y complejidad de trabajo, sobre las materias primas, los equipos de trabajo y el estado de salud de los trabajadores.
2. Valoración y análisis de los riesgos: en función de los criterios objetivos de valoración que se hubiesen fijado previamente por la organización. El método empleado para el análisis se basa en la matriz de consecuencia/probabilidad, estableciendo tres niveles de consecuencia y tres niveles de probabilidad.
3. Planificación de las actividades preventivas: en caso de que se considere necesario a partir de la valoración, se debe realizar una planificación de la actividad preventiva que incluya las actividades de prevención que garanticen un mayor nivel de protección de la seguridad y salud de los trabajadores.
4. Control periódico: una vez finalizada la valoración de los riesgos y adoptadas las medidas preventivas pertinentes, se debe realizar el seguimiento necesario para cada una de las actuaciones.

Cabe añadir que, pese a que no queda incluido en las fases que se describen en el procedimiento de la Organización X, sí se menciona la importancia de conocer el contexto al explicar la metodología de trabajo. Se puede apreciar, por tanto, una clara correspondencia con la metodología de gestión del riesgo de las normas ISO, que se visualiza en la siguiente figura (ver Figura 30).



Figura 30 – Correlación entre la metodología de gestión del riesgo ISO y la metodología de prevención de riesgos laborales empleada por la Organización X (elaboración propia).

La metodología seguida por la Organización X con relación a los riesgos laborales, por tanto, es prácticamente la misma que la que se contempla en las normas ISO de gestión del riesgo (incluyendo la gestión de riesgos documentales). Esto conlleva la posibilidad de integrar en un solo procedimiento la gestión de riesgos laborales y documentales, sin que esto suponga un cambio importante en el modo de trabajar de la organización. Simplemente, se debe realizar una ampliación del alcance en la identificación de riesgos para incluir aquellos relacionados con la gestión de documentos.

Con relación a la metodología seguida por el área de Informática, se cuenta con un *Plan de adecuación al Esquema Nacional de Seguridad*, del año 2012, en el que se realiza una identificación de riesgos de seguridad de la información, algunos de ellos relacionados con la gestión de documentos. En este documento se pone de manifiesto que la Organización X no dispone de un “proceso documentado, sistemático, repetible y eficiente de análisis y gestión de riesgos sobre sus activos críticos”⁸⁰ y se recomienda, como base para futuros análisis, utilizar la metodología de análisis de riesgo empleada para la realización de dicho plan de adecuación. Esta metodología sigue los siguientes pasos:

1. Identificar los activos: en primer lugar, se realiza la identificación y valoración de activos de información de la Organización X, es decir, lo que se debe proteger.
2. Identificar los riesgos: se identifican las amenazas dentro de las que enmarca cualquier evento que pueda producir una violación de la seguridad de los activos y/o de los recursos de información, ocasionando daños materiales o pérdidas inmateriales en el organismo. Se realiza una relación entre activos y amenazas y se valora la frecuencia de ocurrencia (probabilidad) de estas últimas.

⁸⁰ – Información extraída del Plan de adecuación al Esquema Nacional de Seguridad (ENS) de la Organización X.

3. Identificar los controles existentes: se realiza tanto la identificación como el grado de implantación o madurez de cada control en la Organización X. De este modo se puede obtener una información más ajustada a la realidad sobre la probabilidad y el impacto de los riesgos en la seguridad de la información.
4. Interpretar los resultados: a partir de las consecuencias, la prioridad, y la clasificación (siguiendo el catálogo de amenazas de la metodología MAGERIT⁸¹).

Se observa que la metodología empleada se basa en la identificación de los riesgos y en su análisis, sin establecer acciones de prevención o tratamiento ni acciones para el seguimiento y revisión. En la Figura 31 se puede apreciar la correlación de esta metodología con la planteada por las normas ISO.



Figura 31 – Correlación entre la metodología de gestión del riesgo ISO y la metodología de gestión del riesgo según el Plan de adecuación al Esquema Nacional de Seguridad empleada por la Organización X (elaboración propia).

Se puede considerar, por tanto, que la metodología empleada es incompleta, tanto si se compara con la explicada en la normativa internacional ISO, como si se compara con la definida en el procedimiento de prevención de riesgos laborales. No se contempla la fase de comunicación, no se establece el contexto en el que se va a llevar a cabo la gestión del riesgo ni tampoco se establecen medidas de prevención o tratamiento, ni de seguimiento y revisión de dichas medidas. Por tanto, se considera que esta metodología por sí sola no puede garantizar la prevención de riesgos, sino que deben desarrollarse planes de actuación en función de los resultados obtenidos de las fases de identificación y análisis.

⁸¹ – MAGERIT es una metodología de análisis y gestión de riesgos, elaborada por el Consejo Superior de Administración Electrónica, que estima que la gestión de los riesgos es una piedra angular en las guías de buen gobierno. MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información. MAGERIT tipifica las amenazas en cuatro grupos: desastres naturales, de origen industrial, errores y fallos no intencionados, y ataques deliberados.

En este caso, el método empleado para el análisis de riesgos se basa en la matriz de consecuencia/probabilidad, estableciendo cuatro niveles de consecuencia o severidad y cinco niveles de probabilidad. Esta técnica coincide con la empleada por el área de prevención de riesgos laborales, aunque los niveles establecidos sean distintos.

Si comparamos las dos metodologías de gestión del riesgo empleadas en la Organización X, se aprecia la falta de correlación entre ambas, pese a tener objetivos similares. Coinciden en las fases de identificación y valoración, pese a que esta última se enfoca desde distintas perspectivas en cada una de las metodologías. No coinciden a la hora de establecer acciones preventivas, de implementar controles periódicos o de interpretar resultados del análisis (ver Figura 32). Se puede afirmar que la metodología seguida para el cumplimiento con el ENS se centra tan solo en la identificación y análisis de riesgos, obviando el resto del proceso de gestión de riesgos.



Figura 32 – Correlación entre las metodología de gestión del riesgo empleadas por la Organización X (elaboración propia).

Se considera necesario ampliar el alcance de la metodología del área de Informática para adecuarla lo máximo posible a la empleada en el área de Prevención de Riesgos Laborales. Es necesario, tal y como se expone en el procedimiento de esta última, integrar la gestión del riesgo en el sistema general de gestión de la organización, con la finalidad de evitar que se trate de un método de trabajo aislado y empleado tan solo por dos o tres áreas. Es fundamental concienciar a todas las áreas de la organización para que trabajen siguiendo esta metodología en su día a día, incluyendo la prevención de todos aquellos riesgos que les afecten, siempre desde el liderazgo claro de la Dirección.

5.2.5 Sistema de Gestión Documental

Dentro de la estructura general de la organización, el análisis de este apartado se centra en aquellas áreas o subáreas relacionadas directamente con la gestión de documentos.

La subárea de Gestión Documental y Archivo depende directamente de Gerencia, que a su vez depende de Alcaldía. Se encuentra en el mismo grupo y al mismo nivel que las subáreas de Administración Electrónica y de Transparencia. Otro aspecto importante es que está situada también al mismo nivel que Organización y Proyecto de Desarrollo del Modelo de Gestión Corporativo, dentro del cual sería conveniente incluir la gestión de riesgos documentales como un aspecto nuclear en la gestión corporativa, tal y como se apunta tanto en la normativa internacional ISO como en el modelo MAGERIT. Este modelo afirma que la gestión de los riesgos⁸² es una piedra angular en las guías de buen gobierno público o privado, donde se considera un principio fundamental que las decisiones de gobierno se fundamenten en el conocimiento de los riesgos que implican (Amutio Gómez *et al.* 2012, p. 6).

Cabe destacar que la Organización X no dispone de política de gestión documental, instrumento considerado clave para el correcto funcionamiento de un sistema de gestión documental en cualquier organización. En cambio, sí dispone de una serie de instrumentos internos, metodologías y procedimientos de gestión documental que se ajustan a sus necesidades en la materia, como por ejemplo el vocabulario de metadatos, el cuadro de clasificación o el reglamento de archivo.

En el instrumento de Reglamento de Archivo es donde queda patente el objetivo de impulsar la gestión y garantizar la preservación de la documentación de la organización de acuerdo a sus valores, así como el objetivo de regular su gestión de manera integrada. En él se definen los elementos constitutivos del sistema de gestión documental corporativo, que se enumeran a continuación:

- Subsistema de identificación: que debe integrarse por el cuadro de clasificación, el manual de uso del cuadro de clasificación y los criterios para la codificación de documentos.
- Subsistema de descripción: que debe integrarse por el plan descriptivo y por los instrumentos de descripción definidos.
- Subsistema de conservación: que debe integrarse por el calendario de conservación, el plan de conservación preventiva y el registro de eliminaciones.
- Subsistema de transferencia: que debe integrarse por el calendario de transferencias, el manual de procedimiento y por las instrucciones aplicables a soportes o formatos específicos.
- Subsistema de acceso: que debe integrarse por el cuadro y calendario de acceso, así como por las normas y procedimientos de consulta y préstamo de documentos.

⁸² – Se entiende en este contexto la gestión de riesgos generales de la organización, esta afirmación no se refiere a la gestión de riesgos documentales específicamente.

Estos subsistemas dibujan el sistema de gestión documental de la organización, delimitando diferentes espacios dentro de los cuales se ha desarrollado y deben desarrollarse normativa, procedimientos, instrucciones de trabajo y otros instrumentos con la finalidad de cumplir con los objetivos fijados por el área y por la organización, en línea con los principios de gestión documental.

De los instrumentos previstos en el Reglamento de Archivo, se desarrollan algunos que no han sido aprobados formalmente, por lo que no son de cumplimiento obligatorio para los trabajadores. Estos instrumentos son:

- El “Calendario de Conservación”, realizado a partir de las Tablas de Valoración Documental⁸³ aprobadas por la Comisión Nacional de Acceso, Valoración y Selección Documental (CNAADT⁸⁴, por sus siglas en catalán).
- La “Instrucción sobre la valoración, selección y eliminación de documentos”, desarrollada de acuerdo con la legislación vigente sobre la materia. En este instrumento se explican conceptos relevantes para llevar a cabo estos procesos, las responsabilidades en materia de valoración, el procedimiento para la elaboración de propuestas de valoración documental, el procedimiento para la selección documental y el de eliminación.
- La “Instrucción de transferencia de documentos al Archivo Municipal” en la que consta la descripción del procedimiento, roles, normativa aplicable y otra información relacionada con las transferencias. Se dispone también de un documento con recomendaciones sobre transferencias en la intranet del Ayuntamiento.
- La “Guía metodológica – Modelo de registro de expedientes: conceptos, aplicación e instrucciones de gestión”. En este instrumento se explica el marco corporativo del registro de expedientes, su aplicación, así como también una serie de instrucciones de gestión. Se aprovecha para introducir aspectos de gestión documental básicos para los usuarios del registro con la finalidad de que puedan entender mejor el objetivo y la importancia de trabajar de acuerdo a esta guía metodológica. Cabe destacar que, a partir de la puesta en marcha del registro de expedientes, los trabajadores de la organización empiezan a ser más conscientes de la importancia de seguir unas directrices normalizadas para poder recuperar la información de manera más eficaz y sin incidencias.
- La “Instrucción sobre el préstamo ordinario y consulta de documentos”, donde se describe el proceso a seguir para poder consultar los documentos custodiados en los depósitos de archivo.

Puede apreciarse que los instrumentos desarrollados y no aprobados son herramientas necesarias para garantizar el correcto funcionamiento de un sistema de gestión documental, que deberían formar parte del mismo de manera formal, tal y como se especifica en el Reglamento de Archivo.

⁸³ –Las Tablas de Valoración Documental son unas disposiciones normativas que definen el periodo de conservación de los documentos de las administraciones públicas de Cataluña y su régimen general de acceso.

⁸⁴ –La CNAADT es un órgano colegiado de carácter técnico, adscrito a la Dirección General de Archivos, Bibliotecas, Museos y Patrimonio de la Generalitat de Catalunya, que desarrolla las competencias en las materias de valoración y selección de la documentación, y acceso, que le atribuye la Ley 10/2001, de archivos y gestión de documentos y está regulada por el Decreto 13/2008, de 22 de enero, sobre acceso, valoración y selección de documentos.

Es importante tener en cuenta que la documentación de la Organización X está mayoritariamente en soporte papel, excepto alguna documentación electrónica derivada de los trámites que ya pueden hacerse de manera electrónica. Respecto a esta última, se conserva en un repositorio interno del área de Informática, de manera provisional, con el objetivo a corto plazo de poder introducirla en el gestor documental. Respecto a la documentación en papel, está custodiada en diferentes depósitos que son de propiedad municipal y, por tanto, la custodia no está externalizada. El año 2015 se calculó un volumen de documentación de 8859 metros lineales custodiados en el Archivo Municipal, aunque se debe tener presente que existe un volumen indeterminado de documentación en las oficinas tramitadoras. Este volumen no queda reflejado en este cálculo. No se dispone de información acerca del volumen documental actual.

Existe, tal y como se ha explicado anteriormente, una instrucción sobre el préstamo ordinario de documentos siguiendo lo consignado por el reglamento. Además de este instrumento, se ha desarrollado una instrucción más extensa donde consta mucha más información al respecto. Por tanto, se constata que la organización dispone de diferentes herramientas con información similar sobre un mismo procedimiento, lo que puede ocasionar confusión.

No se han definido indicadores para el control de los procesos de gestión documental, si bien se tiene previsto. El área de Archivo y Gestión Documental junto con el área de Organización y Proyectos de Mejora están trabajando en la definición de indicadores sobre los procedimientos de administración electrónica que se vayan implantando en la organización. El objetivo es realizar un seguimiento y llevar un control sobre las posibles incidencias y desviaciones que se puedan producir.

A partir de lo expuesto, se puede afirmar que la organización, pese a la madurez de algunas cuestiones, carece de algunos de los instrumentos básicos para una gestión documental eficaz como, por ejemplo, la política de gestión documental. Dispone, por tanto, de un sistema de gestión documental incompleto, y eso puede repercutir en la consecución de sus objetivos, así como también en la calidad del servicio a los ciudadanos.

El personal es consciente de la importancia de la gestión documental en su día a día, así como de disponer de metodología para la gestión y prevención de los riesgos. En este sentido, las metodologías existentes no trabajan de acuerdo a los mismos parámetros, lo que dificulta la gestión integral del riesgo en la Organización X. Esto puede suponer un problema a la hora de incluir la gestión de riesgos documentales.

5.3 Fase 2. Apreciación del riesgo

Según la norma internacional ISO 31000, la apreciación del riesgo es el proceso global que comprende la identificación, el análisis y la evaluación del riesgo (AENOR 2010, p. 23). En este apartado, por tanto, se ha previsto la inclusión de estos tres subprocesos de la gestión del riesgo, detallando para cada uno de ellos la metodología que se ha empleado y las conclusiones halladas.

5.3.1 Identificación de riesgos documentales

Se siguen dos técnicas distintas para llevar a cabo la identificación de riesgos explicadas en el capítulo 2, con el objetivo final de poder comparar los procesos y los resultados obtenidos. Estas técnicas son:

- Enfoque basado en amenazas, considerado como la técnica tradicional de identificación de riesgos, que determina un hecho o una amenaza desencadenante que puede afectar de algún modo a una organización.
- Enfoque basado en requisitos, que analiza el cumplimiento de los requisitos aplicables a la organización estudiada para identificar los riesgos.

Para llevar a cabo el proceso de identificación de riesgos documentales se parte de la información recopilada y analizada de las entrevistas estructuradas (ver Anexo C para la transcripción no literal de las entrevistas), así como también de la observación directa en las visitas a la organización durante el proceso. En primer lugar, se efectúa una primera identificación de riesgos documentales a través de las amenazas descritas por los entrevistados, así como por aquellas situaciones de riesgo identificadas mediante el análisis del contexto y la observación directa. En segundo lugar, se efectúa otra identificación de riesgos documentales a través del análisis del cumplimiento de los requisitos que el sistema de gestión documental debería cumplir según los estándares internacionales. En tercer lugar, se comparan los resultados obtenidos con el objetivo final de conseguir una identificación de riesgos documentales lo más pertinente y ajustada a la realidad posible.

Identificación de riesgos basada en amenazas (Técnica A)

En primer lugar, a través de la información recopilada, se identifican nueve amenazas o situaciones de riesgo, que se enumeran a continuación:

1. Falta de control en la realización de traslados de documentación: en las entrevistas se pone de manifiesto la inexistencia de controles en los traslados de documentación entre departamentos y entre edificios. El personal que realiza estas operaciones no es consciente de la importancia de la documentación que traslada ni de las consecuencias que puede suponer no realizar el traslado con garantías.

2. No documentación de los trámites administrativos: se evidencia una falta de definición de los procedimientos en la organización que, en algunos casos, deriva en una falta de evidencias documentales sobre las decisiones o acciones llevadas a cabo.
3. Falta de controles y criterios sobre el acceso a los depósitos: no se han definido directrices de acceso y consulta de la documentación en los espacios de archivo.
4. Malas condiciones de los depósitos de archivo: se evidencian malas condiciones de los espacios destinados a conservar la documentación de la organización, sobre todo problemas de goteras, humedades no controladas y presencia de insectos.
5. Falta de control en la eliminación de documentos: hay departamentos que realizan destrucciones documentales sin la autorización previa del responsable de gestión documental. Además, estas eliminaciones no se llevan a cabo siguiendo la normativa y legislación existentes.
6. Incumplimiento del procedimiento de préstamo y consulta: al realizar peticiones de información internas, no se siguen los canales ni los plazos establecidos. En ocasiones no se devuelve la documentación a tiempo o se entregan expedientes ya cerrados con nuevos documentos, entre otras casuísticas.
7. Incumplimiento del procedimiento de transferencias: en la mayoría de ocasiones, por falta de recursos, no se verifican las transferencias.
8. Falta de formación de los trabajadores en materia de gestión documental: se detecta una falta de formación general en cuestiones relacionadas con la gestión de documentos: eliminaciones, transferencias, traslados o acceso a la información, entre otras.
9. Falta de directrices claras sobre la gestión de documentos: pese a la existencia de procedimientos normalizados, se detecta su falta de conocimiento por parte del personal. No se dispone de normas claras y conocidas.

A partir de estas nueve amenazas se realiza la identificación de riesgos documentales que afectan a la Organización X (ver Figura 33) según la técnica tradicional basada en amenazas (en adelante, técnica A) como base para identificar los riesgos.

N	AMENAZA	IDENTIFICACIÓN DE RIESGOS DOCUMENTALES
1	Falta de control a la hora de realizar traslados de documentación	<ul style="list-style-type: none"> - Pérdida de información/documentación - Falta de garantías de integridad
2	No documentación de los trámites administrativos	<ul style="list-style-type: none"> - Pérdida de documentos esenciales - No creación de evidencias documentales - No recuperación de información/documentación - Falta de garantías de integridad
3	Falta de controles y criterios sobre el acceso a los depósitos	<ul style="list-style-type: none"> - Accesos indebidos a información - Eliminación indebida de documentos - Sustracción o robo de documentos - Falta de garantías de integridad - Manipulación no autorizada de documentos
4	Malas condiciones de los depósitos de archivo	<ul style="list-style-type: none"> - Pérdida de información/documentación - Falta de garantías de accesibilidad - Falta de garantías de usabilidad
5	Falta de control en la eliminación de documentos	<ul style="list-style-type: none"> - Eliminación indebida de documentos - No eliminación de documentos - Falta de garantías de integridad
6	Incumplimiento del procedimiento de préstamo y consulta	<ul style="list-style-type: none"> - Accesos indebidos a información - Eliminación indebida de documentos - Sustracción o robo de documentos - Falta de garantías de integridad - Manipulación no autorizada de documentos
7	Incumplimiento del procedimiento de transferencias	<ul style="list-style-type: none"> - Ubicación errónea o indebida de documentos - No recuperación de información/documentación - Falta de garantías de integridad
8	Falta de formación de los trabajadores en materia de gestión documental	<ul style="list-style-type: none"> - Pérdida de documentos esenciales - No creación de evidencias documentales - No recuperación de información/documentación - Falta de garantías de autenticidad - Eliminación indebida de documentos - Duplicidad documental - Creación innecesaria de documentos
9	Falta de directrices claras sobre la gestión de documentos	<ul style="list-style-type: none"> - Pérdida de documentos esenciales - No creación de evidencias documentales - No recuperación de información/documentación - Falta de garantías de autenticidad - Falta de garantías de accesibilidad - Falta de garantías de fiabilidad - Falta de garantías de integridad - Falta de garantías de trazabilidad - Eliminación indebida de documentos - No eliminación de documentos - Duplicidad documental - Creación innecesaria de documentos - Duplicación de instrumentos de gestión documental - Accesos indebidos a información - Manipulación no autorizada de documentos

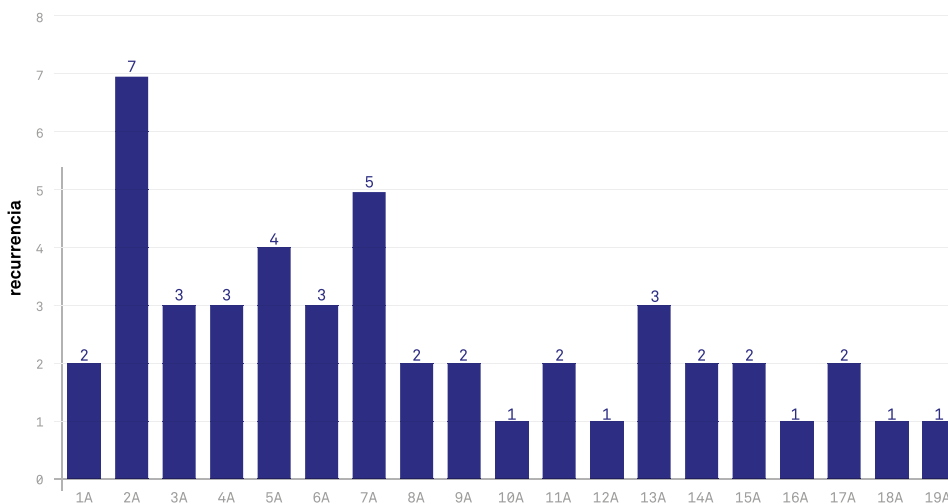
Figura 33 – Identificación de riesgos documentales de la Organización X siguiendo la Técnica A (elaboración propia).

A continuación, se incluye la definición de cada uno de los riesgos identificados según la Técnica A:

1. Pérdida de información/documentación: extravío o desaparición de información o documentación generada o recibida por la organización en el ejercicio de sus funciones.
2. Falta de garantías de integridad: documentos y/o expedientes de los que no puede certificarse o asegurarse su completitud o inalterabilidad a lo largo del tiempo en que deben ser conservados.
3. Pérdida de documentos esenciales: falta de generación o pérdida de evidencias documentales consideradas fundamentales para la gestión de las funciones de la organización.
4. No creación de evidencias documentales: falta de generación de documentos considerados necesarios para la gestión de las funciones y actividades de la organización.
5. No recuperación de información/documentación: incapacidad para localizar o acceder a información o documentación generada o recibida por la organización en el ejercicio de sus funciones.
6. Accesos indebidos a información: entrada a o lectura de información, sin disponer de permiso o autorización para ello.
7. Eliminación indebida de documentos: destrucción de información o documentación sin disponer del permiso o autorización para ello, o por error.
8. Sustracción o robo de documentos: hurto de documentación o información.
9. Falta de garantías de accesibilidad: documentación de la que no puede certificarse o asegurarse su localización, recuperación y acceso a lo largo del tiempo en que debe ser conservada.
10. Falta de garantías de usabilidad: incapacidad para asegurar la localización, recuperación, presentación, interpretación y uso de un documento a lo largo del tiempo en que debe ser conservado.
11. No eliminación de documentos: conservación innecesaria de documentación, pese a estar establecida su eliminación en el calendario de conservación y en las directrices de disposición.
12. Ubicación errónea o indebida de documentos: falta de control y seguimiento en el almacenamiento de la documentación en los depósitos físicos y en los repositorios electrónicos.
13. Manipulación no autorizada de documentos: realización de cambios en el contenido o formato de los documentos sin consentimiento, aprobación o permiso previos.
14. Duplicidad documental: creación de varias copias idénticas de un mismo documento.
15. Creación innecesaria de documentos: generación de documentos, sean copias u originales, no requeridos para la gestión de la organización.
16. Duplicación de instrumentos de gestión documental: desarrollo de varios protocolos o directrices, internos, para un mismo proceso de gestión documental.
17. Falta de garantías de autenticidad: incapacidad para asegurar la legitimidad y veracidad de un documento a lo largo del tiempo en que debe ser conservado.
18. Falta de garantías de fiabilidad: incapacidad para asegurar la confiabilidad de un documento a lo largo del tiempo en que debe ser conservado.

19. Falta de garantías de trazabilidad: incapacidad para asegurar la creación, incorporación y conservación de información (que se incluye en forma de metadatos) sobre la gestión y uso de un documento a lo largo del tiempo en que este debe ser conservado.

Se identifican un total de 19 riesgos documentales, algunos de los cuales aparecen relacionados con más de una amenaza. En la siguiente tabla se visualiza la recurrencia de cada riesgo en el proceso de identificación.



N	RIESGO IDENTIFICADO
1A	Pérdida de información / documentación
2A	Falta de garantías de integridad
3A	Pérdida de documentos esenciales
4A	No creación de evidencias documentales
5A	No recuperación de información / documentación
6A	Accesos indebidos a información
7A	Eliminación indebida de documentos
8A	Sustracción o robo de documentos
9A	Falta de garantías de accesibilidad
10A	Falta de garantías de usabilidad
11A	No eliminación de documentos
12A	Ubicación errónea o indebida de documentos
13A	Manipulación no autorizada de documentos
14A	Duplicidad documental
15A	Creación innecesaria de documentos
16A	Duplicación de instrumentos de gestión documental
17A	Falta de garantías de autenticidad
18A	Falta de garantías de fiabilidad
19A	Falta de garantías de trazabilidad

Figura 34 – Número de apariciones de cada riesgo identificado según la Técnica A (elaboración propia).

Se aprecia claramente la falta de garantías de integridad como el riesgo que aparece en más ocasiones (con un valor de 7), duplicando y triplicando la mayoría del resto de valores de los riesgos identificados. En esta escala, le siguen el riesgo de eliminación indebida de documentos (con un valor de 5) y la no recuperación de información o documentación (con un valor de 4). Estos tres son los riesgos que más aparecen. Para los demás riesgos identificados, el número de apariciones es similar. De estos números se puede deducir que existen riesgos en la Organización X que pueden ocurrir con más frecuencia que otros.

Se observa que, a la hora de identificar riesgos, el número de los mismos aumenta o disminuye en función de la amenaza con la que se relacionan. La amenaza con mayor número de riesgos identificados es la número 9, consistente en la falta de directrices claras sobre gestión documental, con un total de 15 riesgos asociados. La amenaza con menos riesgos identificados es la número 1, que se corresponde con la falta de control a la hora de realizar traslados de documentación, con 2 riesgos asociados. El número de riesgos depende, por tanto, de la amenaza de la que se parte para llevar a cabo el proceso de identificación. En algunos casos, la diferencia resulta substancial.

Identificación de riesgos basada en requisitos (Técnica R)

En segundo lugar, se realiza nuevamente el proceso de identificación de riesgos documentales de la Organización X, en este caso a partir del análisis de los requisitos de gestión documental que la organización debe cumplir (en adelante, técnica R). Se trabaja de acuerdo a la norma internacional ISO 30301, que es una norma de requisitos para los sistemas de gestión para documentos aplicable a cualquier tipo de organización (ver capítulo 1). Concretamente, el proceso parte de los requisitos determinados en el Anexo A (normativo) del estándar. En él se fijan los requisitos que se relacionan directamente con los procesos de gestión documental. En la Figura 35 se enumeran los riesgos documentales identificados con esta técnica para la Organización X. Para ello, se mantiene el código dado en el Anexo A de la norma, incluido en la primera columna, y los procesos de gestión documental consignados en dicho anexo, siguiendo el mismo orden en el que aparecen, en la segunda columna.

El proceso seguido a la hora de identificar los riesgos parte del análisis del cumplimiento de los procesos de gestión documental del Anexo A por parte de la Organización X. Para cada proceso se realiza un análisis de los instrumentos existentes y del cumplimiento de los requisitos a partir de lo consignado en el anexo. Sobre la base de este análisis, se identifican los riesgos que se incluyen en la Figura 35.

N.	PROCESO DE GESTIÓN DOCUMENTAL	IDENTIFICACIÓN DE RIESGOS DOCUMENTALES
A.1	Creación	
A.1.1	Determinar qué documentos, cuándo y cómo deben ser creados y capturados en cada proceso de negocio	
A.1.1.1	Determinar la necesidad de información	<ul style="list-style-type: none"> - Pérdida de documentos esenciales - No creación de evidencias documentales - Duplicidad documental - Falta de garantías de integridad - Falta de garantías de trazabilidad - Creación innecesaria de documentos
A.1.1.2	Determinar los requisitos	<ul style="list-style-type: none"> - Pérdida de documentos esenciales - No creación de evidencias documentales - No recuperación de información/documentación - Falta de garantías de integridad - Creación innecesaria de documentos
A.1.1.3	Crear documentos fiables	<ul style="list-style-type: none"> - Falta de garantías de autenticidad - Falta de garantías de fiabilidad - Manipulación no autorizada de documentos
A.1.1.4	Determinar la conservación	<ul style="list-style-type: none"> - Eliminación indebida de documentos
A.1.1.5	Establecer calendarios de conservación	<ul style="list-style-type: none"> - Eliminación indebida de documentos - No eliminación de documentos - No recuperación de información/documentación
A.1.1.6	Determinar los métodos de captura	<ul style="list-style-type: none"> - Pérdida de documentos esenciales - No creación de evidencias documentales - Falta de garantías de fiabilidad - Manipulación no autorizada de documentos
A.1.2	Determinar la información sobre el contenido, contexto y control (metadatos) que debe incluirse en los documentos	
A.1.2.1	Identificar la información descriptiva y de contexto	<ul style="list-style-type: none"> - No recuperación de información/documentación - Errores en la descripción documental - Falta de garantías de integridad - Falta de garantías para la trazabilidad - Manipulación no autorizada de documentos
A.1.2.2	Identificar los momentos de captura	<ul style="list-style-type: none"> - Pérdida de documentos esenciales - No creación de evidencias documentales - Falta de garantías de fiabilidad - Errores en la descripción documental - No recuperación de información/documentación - Falta de garantías de integridad
A.1.3	Decidir en qué forma y estructura se deben crear y capturar los documentos	
A.1.3.1	Identificar los requisitos específicos	<ul style="list-style-type: none"> - Pérdida de documentos esenciales - No creación de evidencias documentales - Falta de garantías de usabilidad - No recuperación de información/documentación - Creación innecesaria de documentos
A.1.4	Determinar tecnologías apropiadas para crear y capturar documentos	
A.1.4.1	Seleccionar la tecnología	<ul style="list-style-type: none"> - Falta de garantías de usabilidad - No recuperación de información/documentación - Pérdida de información/documentación - Falta de garantías de accesibilidad

N.	PROCESO DE GESTIÓN DOCUMENTAL	IDENTIFICACIÓN DE RIESGOS DOCUMENTALES
A.2 Control		
A.2.1 Determinar qué información de control (metadatos) debe crearse en los procesos de gestión de documentos y cómo se vinculará con los documentos y se gestionará a lo largo del tiempo		
A.2.1.1	Registrar	<ul style="list-style-type: none"> - Falta de garantías de fiabilidad - Errores en la descripción documental - No recuperación de información/documentación - Falta de garantías de integridad - Falta de garantías de trazabilidad - Manipulación no autorizada de documentos
A.2.1.2	Clasificar	<ul style="list-style-type: none"> - No recuperación de información/documentación - Errores en la descripción documental - Accesos indebidos a información - Pérdida de información/documentación - Manipulación no autorizada de documentos
A.2.1.3	Clasificar	<ul style="list-style-type: none"> - No recuperación de información/documentación - Errores en la descripción documental - Accesos indebidos a información - Pérdida de información/documentación - Manipulación no autorizada de documentos
A.2.1.4	Seleccionar la información de control (elementos de metadatos)	<ul style="list-style-type: none"> - No recuperación de información/documentación - Errores en la descripción documental - Falta de garantías de trazabilidad - Falta de garantías de integridad - Falta de garantías de fiabilidad - Manipulación no autorizada de documentos
A.2.1.5	Determinar el historial de eventos	<ul style="list-style-type: none"> - Falta de garantías de trazabilidad - No recuperación de información/documentación - Falta de garantías de integridad - Falta de garantías de fiabilidad - Manipulación no autorizada de documentos
A.2.1.6	Control de los documentos en la organización	<ul style="list-style-type: none"> - Falta de garantías de trazabilidad - Errores en la descripción documental - No recuperación de información/documentación - Falta de garantías de integridad - Falta de garantías de fiabilidad - Manipulación no autorizada de documentos - Creación innecesaria de documentos
A.2.2 Establecer las reglas y condiciones para el uso de los documentos a lo largo del tiempo		
A.2.2.1	Desarrollar reglas de acceso	<ul style="list-style-type: none"> - No recuperación de información/documentación - Accesos indebidos a información - Eliminación indebida de documentos - Sustracción o robo de documentos - Manipulación no autorizada de documentos - Falta de garantías de integridad - Falta de garantías de fiabilidad - Falta de garantías de accesibilidad
A.2.2.2	Implementar reglas de acceso	<ul style="list-style-type: none"> - No recuperación de información/documentación - Accesos indebidos a información - Eliminación indebida de documentos - Manipulación no autorizada de documentos - Falta de garantías de integridad - Falta de garantías de fiabilidad - Falta de garantías de accesibilidad - Sustracción o robo de documentos
A.2.3 Mantener la usabilidad de los documentos a lo largo del tiempo		
A.2.3.1	Mantener la integridad y la autenticidad	<ul style="list-style-type: none"> - No recuperación de información/documentación - Accesos indebidos a información - Eliminación indebida de documentos - Falta de garantías de integridad - Falta de garantías de fiabilidad - Falta de garantías de accesibilidad - Sustracción o robo de documentos

N.	PROCESO DE GESTIÓN DOCUMENTAL	IDENTIFICACIÓN DE RIESGOS DOCUMENTALES
A.2.3.2	Mantener la usabilidad	<ul style="list-style-type: none"> - No recuperación de información/documentación - Falta de garantías de usabilidad - Falta de garantías de accesibilidad - Pérdida de información/documentación
A.2.3.3	Mantener la usabilidad	<ul style="list-style-type: none"> - No recuperación de información/documentación - Falta de garantías de integridad - Falta de garantías de usabilidad - Falta de garantías de accesibilidad - Pérdida de información/documentación
A.2.3.4	Limitar las restricciones	<ul style="list-style-type: none"> - No recuperación de información/documentación - Falta de garantías de accesibilidad
A.2.4 Implementar la disposición/eliminación autorizada de los documentos		
A.2.4.1	Implementar la disposición	<ul style="list-style-type: none"> - Eliminación indebida de documentos - No eliminación de documentos - No recuperación de información/documentación - Pérdida de información/documentación
A.2.4.2	Autorizar la disposición	<ul style="list-style-type: none"> - Eliminación indebida de documentos - No recuperación de información/documentación - Pérdida de información/documentación
A.2.4.3	Transferir	<ul style="list-style-type: none"> - Pérdida de información/documentación - No recuperación de información/documentación - Ubicación errónea o indebida de documentos - Falta de garantías de accesibilidad - Errores en la descripción documental - Falta de garantías de trazabilidad
A.2.4.4	Trasladar	<ul style="list-style-type: none"> - Pérdida de información/documentación - No recuperación de información/documentación - Ubicación errónea o indebida de documentos - Falta de garantías de accesibilidad - Errores en la descripción documental - Falta de garantías de trazabilidad
A.2.4.5	Destruir	<ul style="list-style-type: none"> - Eliminación indebida de documentos - No recuperación de información/documentación - Pérdida de información/documentación - Falta de garantías de trazabilidad
A.2.4.6	Mantener información sobre los documentos destruidos	<ul style="list-style-type: none"> - Eliminación indebida de documentos - No recuperación de información/documentación - Pérdida de información/documentación - Falta de garantías de trazabilidad
A.2.5 Establecer las condiciones de administración y mantenimiento de las aplicaciones de gestión de documentos		
A.2.5.1	Identificar las aplicaciones de gestión de documentos	<ul style="list-style-type: none"> - Desarrollo no controlado de aplicaciones - Falta de interoperabilidad - Falta de respuesta ante fallos del sistema - Duplicidad documental (en aplicaciones distintas)
A.2.5.2	Documentar las decisiones de implementación	<ul style="list-style-type: none"> - Desarrollo no controlado de aplicaciones - Falta de interoperabilidad - Falta de respuesta ante fallos del sistema - Infraestructura insuficiente
A.2.5.3	Acceder a las aplicaciones de gestión de documentos	<ul style="list-style-type: none"> - Pérdida de información/documentación - Falta de garantías de trazabilidad - Interrupción de la actividad - Falta de garantías de accesibilidad - Falta de respuesta ante fallos del sistema - Eliminación indebida de documentos - Manipulación no autorizada de documentos - No recuperación de información/documentación - Accesos indebidos a las aplicaciones de gestión de documentos
A.2.5.4	Asegurar la disponibilidad	<ul style="list-style-type: none"> - Interrupción de la actividad - Falta de garantías de accesibilidad - Falta de respuesta ante fallos del sistema - Incapacidad de acceder a las aplicaciones

N.	PROCESO DE GESTIÓN DOCUMENTAL	IDENTIFICACIÓN DE RIESGOS DOCUMENTALES
A.2.5.5	Garantizar la efectividad	<ul style="list-style-type: none"> - Pérdida de información/documentación - Falta de garantías de trazabilidad - Interrupción de la actividad - Falta de garantías de accesibilidad - Falta de garantías de usabilidad - Falta de respuesta ante fallos del sistema - No recuperación de información/documentación - Accesos indebidos a las aplicaciones de gestión de documentos
A.2.5.6	Garantizar la integridad	<ul style="list-style-type: none"> - Pérdida de información/documentación - Manipulación no autorizada de documentos - Falta de garantías de trazabilidad - Falta de garantías de accesibilidad - Falta de garantías de integridad - Falta de garantías de autenticidad - Falta de respuesta ante fallos del sistema - No recuperación de información/documentación
A.2.5.7	Administrar los cambios	<ul style="list-style-type: none"> - Pérdida de información/documentación - Falta de garantías de trazabilidad - Interrupción de la actividad - Falta de garantías de accesibilidad - Falta de garantías de usabilidad - Falta de garantías de integridad - Falta de garantías de fiabilidad - Falta de respuesta ante fallos del sistema - Eliminación indebida de documentos - Manipulación no autorizada de documentos - No recuperación de información/documentación - Accesos indebidos a las aplicaciones de gestión de documentos - Infraestructura insuficiente

Figura 35 – Identificación de riesgos documentales de la Organización X siguiendo la Técnica R (elaboración propia).

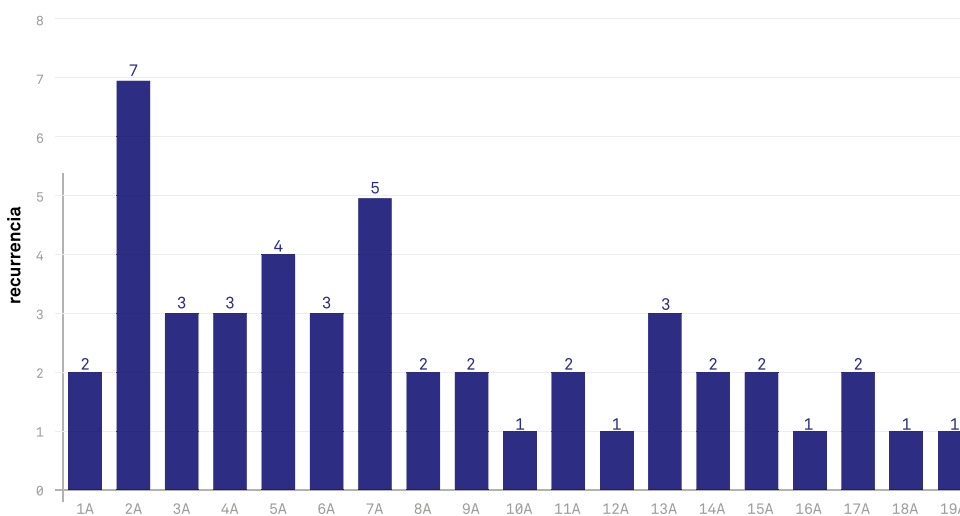
A continuación, se incluye la definición de cada uno de los riesgos identificados según la Técnica R:

1. Pérdida de documentos esenciales: falta de generación o pérdida de evidencias documentales consideradas fundamentales para la gestión de las funciones de la organización.
2. No creación de evidencias documentales: falta de generación de documentos considerados necesarios para la gestión de las funciones y actividades de la organización.
3. No recuperación de información/documentación: incapacidad para localizar o acceder a información o documentación generada o recibida por la organización en el ejercicio de sus funciones.
4. Duplicidad documental: creación de varias copias idénticas de un mismo documento.
5. Falta de garantías de integridad: documentos y/o expedientes de los que no puede certificarse o asegurarse su completitud o inalterabilidad a lo largo del tiempo en que deben ser conservados.
6. Falta de garantías de trazabilidad: incapacidad para asegurar la creación, incorporación y conservación de información (que se incluye en forma de metadatos) sobre la gestión y uso de un documento a lo largo del tiempo en que este debe ser conservado.
7. Falta de garantías de autenticidad: incapacidad para asegurar la legitimidad y veracidad de un documento a lo largo del tiempo en que debe ser conservado.
8. Falta de garantías de fiabilidad: incapacidad para asegurar la confiabilidad de un documento a lo largo del tiempo en que debe ser conservado.

9. Eliminación indebida de documentos: destrucción de información o documentación sin disponer del permiso o autorización para ello, o por error.
10. No eliminación de documentos: conservación innecesaria de documentación, pese a estar establecida su eliminación en el calendario de conservación y en las directrices de disposición.
11. Errores en la descripción documental: fallos e incidencias a la hora de incluir información sobre el contexto, contenido y estructura de los documentos.
12. Falta de garantías de usabilidad: incapacidad para asegurar la localización, recuperación, presentación, interpretación y uso de un documento a lo largo del tiempo en que debe ser conservado.
13. Pérdida de información/documentación: extravío o desaparición de información o documentación generada o recibida por la organización en el ejercicio de sus funciones.
14. Falta de garantías de accesibilidad: documentación de la que no puede certificarse o asegurarse su localización, recuperación y acceso a lo largo del tiempo en que debe ser conservada.
15. Accesos indebidos a información: entrada a o lectura de información, sin disponer de permiso o autorización para ello.
16. Sustracción o robo de documentos: hurto de documentación o información.
17. Ubicación errónea o indebida de documentos: falta de control y seguimiento en el almacenamiento de la documentación en los depósitos físicos y en los repositorios electrónicos.
18. Manipulación no autorizada de documentos: realización de cambios en el contenido o formato de los documentos sin consentimiento, aprobación o permiso previos.
19. Creación innecesaria de documentos: generación de documentos, sean copias u originales, no requeridos para la gestión de la organización.
20. Desarrollo no controlado de aplicaciones: creación de distintos aplicativos informáticos para realizar las mismas funciones o muy similares, con relación a la gestión de documentos.
21. Falta de interoperabilidad: incapacidad para compartir datos y posibilitar el intercambio de información entre departamentos o entre organizaciones.
22. Falta de respuesta ante fallos del sistema: incapacidad de la organización de actuar frente a incidencias en las aplicaciones informáticas de gestión documental.
23. Infraestructura insuficiente: no disponer de los elementos necesarios para el correcto desempeño de los procesos de gestión documental en la organización.
24. Interrupción de la actividad: suspensión temporal del funcionamiento de las aplicaciones que permiten la gestión de documentos en la organización.
25. Accesos indebidos a las aplicaciones: entrada a las aplicaciones de gestión documental sin disponer de permiso o autorización para ello.
26. Incapacidad para acceder a las aplicaciones: imposibilidad de entrada a las aplicaciones informáticas que permiten la gestión de documentos.

Siguiendo la Técnica R se identifican un total de 26 riesgos documentales. Cabe mencionar que en este proceso de identificación se incluyen aspectos relacionados con las aplicaciones de gestión documental, al estar estos integrados en los requisitos del Anexo A de la norma ISO 30301. Estos aspectos no se tienen en cuenta en la identificación realizada según la Técnica A, ya que no se han identificado amenazas con relación a las aplicaciones por parte de los entrevistados. Del total de los riesgos identificados según la Técnica R, el 73,08 % se relaciona directamente con la gestión de documentos, mientras que el 26,92 % restante se relaciona con las aplicaciones informáticas.

Tal y como ocurre en la identificación de riesgos según la Técnica A, siguiendo la Técnica R los riesgos aparecen de manera reiterada y relacionados, en este caso, con diversos requisitos. En la siguiente figura se visualiza la recurrencia de cada riesgo en el proceso de identificación (ver Figura 36).



N	RIESGO IDENTIFICADO
1R	Pérdida de documentos esenciales
2R	No creación de evidencias documentales
3R	No recuperación de información/documentación
4R	Duplicidad documental
5R	Falta de garantías de integridad
6R	Falta de garantías de trazabilidad
7R	Falta de garantías de autenticidad
8R	Falta de garantías de fiabilidad
9R	Eliminación indebida de documentos
10R	No eliminación de documentos
11R	Errores en la descripción documental
12R	Falta de garantías de usabilidad
13R	Pérdida de información/documentación

14R	Falta de garantías de accesibilidad
15R	Accesos indebidos a información
16R	Sustracción o robo de documentos
17R	Ubicación errónea o indebida de documentos
18R	Manipulación no autorizada de documentos
19R	Creación innecesaria de documentos
20R	Desarrollo no controlado de aplicaciones
21R	Falta de interoperabilidad
22R	Falta de respuesta ante fallos del sistema
23R	Infraestructura insuficiente
24R	Interrupción de la actividad
25R	Accesos indebidos a aplicaciones
26R	Incapacidad para acceder a las aplicaciones

Figura 36 - Número de apariciones de cada riesgo identificado según la Técnica R (elaboración propia).

Destaca el riesgo de no recuperación de la información como el que más aparece en el proceso de identificación (28 apariciones), con unos valores muy por encima de los del resto de riesgos identificados. Existe un segundo nivel de riesgos, con valores de 14 y 15 apariciones, como pérdida de información o documentación, falta de garantías de integridad o manipulación no autorizada de documentos, entre otros. El siguiente nivel de recurrencia se reduce a valores de entre 6 y 9, quedando el resto de riesgos identificados por debajo del valor 5 y destacando el valor 2 como predominante.

El número de apariciones de cada riesgo puede relacionarse de manera directa con las probabilidades de que este suceda. Esto es así debido a que las apariciones derivan, en esta técnica, de los requisitos de gestión documental que se deberían cumplir en la organización. En caso de que estos no se cumplieran o no se controlaran de manera adecuada, afloraría el riesgo. Si un riesgo se relaciona con un gran número de requisitos y procesos es más probable que llegue a suceder.

Observando los resultados del proceso de identificación siguiendo la Técnica R, el riesgo con mayor probabilidad de suceder es el número 3R, seguido de los riesgos 13R, 5R, 6R, 14R y 18R. De acuerdo con este criterio, el riesgo con menor probabilidad de suceder es el 26R, con un valor de 1, seguido de los riesgos 4R, 7R, 10R, 17R, 20R, 21R y 23R, con un valor de 2. Cabe recordar que el análisis de probabilidades por sí solo no implica dar una mayor prioridad al tratamiento de estos riesgos.

Análisis comparativo entre la Técnica A y la Técnica R

Se puede observar que los resultados obtenidos con ambas técnicas no coinciden totalmente. Por ejemplo, siguiendo la Técnica R, la identificación de riesgos da resultados más complejos y más completos, incluyendo aspectos que en la Técnica A no se tuvieron en cuenta, como por ejemplo los riesgos relacionados con la tecnología.

Para realizar una comparación entre la recurrencia de los riesgos identificados en ambas técnicas se seleccionan aquellos riesgos relacionados directamente con la gestión de documentos, concretamente 20 riesgos documentales. Por tanto, los riesgos identificados con relación a las aplicaciones informáticas siguiendo la Técnica R no se incluyen en este análisis.

Se realiza una comparación de proporciones sobre el número de aparición de cada riesgo siguiendo ambas técnicas (ver Figura 37). Los porcentajes se calculan a partir del valor total de la aparición de riesgos para cada técnica. El valor total de la Técnica A es 48 y el valor total del Técnica R es 166.

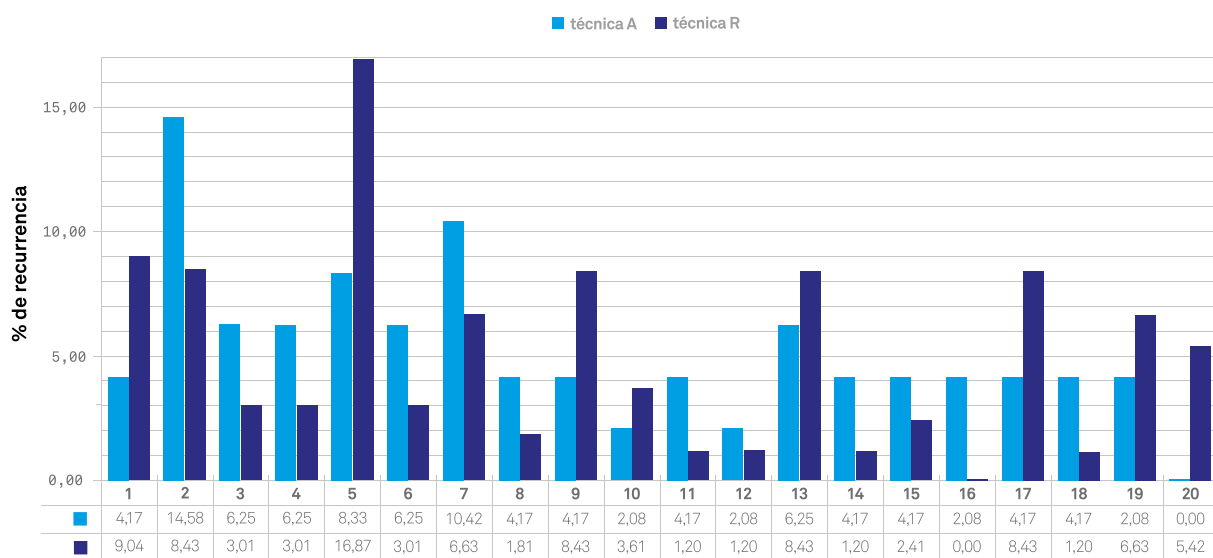


Figura 37 - Comparación de la recurrencia según la técnica empleada (elaboración propia).

Para complementar la Figura 37 se realiza la Figura 38 con la inclusión de los riesgos que aparecen en cada técnica (en la columna derecha). Estas dos figuras deben leerse en complementariedad para realizar el análisis comparativo.

N	RIESGO IDENTIFICADO	TÉCNICA A/R
1	Pérdida de información / documentación	A/R
2	Falta de garantías de integridad	A/R
3	Pérdida de documentos esenciales	A/R
4	No creación de evidencias documentales	A/R
5	No recuperación de información / documentación	A/R
6	Accesos indebidos a información	A/R
7	Eliminación indebida de documentos	A/R
8	Sustracción o robo de documentos	A/R
9	Falta de garantías de accesibilidad	A/R
10	Falta de garantías de usabilidad	A/R
11	No eliminación de documentos	A/R
12	Ubicación errónea o indebida de documentos	A/R
13	Manipulación no autorizada de documentos	A/R
14	Duplicidad documental	A/R
15	Creación innecesaria de documentos	A/R
16	Duplicación de instrumentos de gestión documental	A
17	Falta de garantías de trazabilidad	A/R
18	Falta de garantías de autenticidad	A/R
19	Falta de garantías de fiabilidad	A/R
20	Errores en la descripción documental	R

Figura 38 - Riesgos identificados y técnica empleada (elaboración propia).

Un dato que llama la atención es la baja correlación existente entre los valores de recurrencia de algunos de los riesgos identificados. Por ejemplo, el riesgo número 2, empleando la Técnica A tiene un porcentaje de aparición del 14,58 %, mientras que empleando la Técnica R el porcentaje queda reducido al 8,43 %. Lo mismo ocurre con el riesgo número 5, en este caso en sentido contrario, contando según la Técnica A con un porcentaje de recurrencia del 8,33 % mientras que según la Técnica R se eleva al 16,87 %. Estos son los casos más significativos, aunque también se pueden apreciar diferencias destacables en los riesgos 1, 9, 17 y 19.

Por otro lado, existe un alto grado de semejanza en otros de los riesgos identificados, como es el caso de los números 10 y 12, siendo la diferencia entre ellos inferior a 1 punto, del 0,88 %, en el 12, y ligeramente superior, de 1,53%, en el 10. No puede extraerse, por tanto, un patrón a la hora de establecer qué riesgos tienen mayor porcentaje de recurrencia en la Organización X a partir de la comparación de las dos técnicas empleadas.

En el siguiente gráfico se puede observar cómo, en algunos casos, la coincidencia es muy similar y, en cambio, en otros es prácticamente inexistente (ver Figura 39). Lo que sí puede apreciarse es que, mayoritariamente, si la recurrencia es más alta con una técnica, lo es también con la otra y viceversa. La diferencia son los valores finales, que no resultan coincidentes, además de algunos riesgos con picos muy altos o muy bajos.

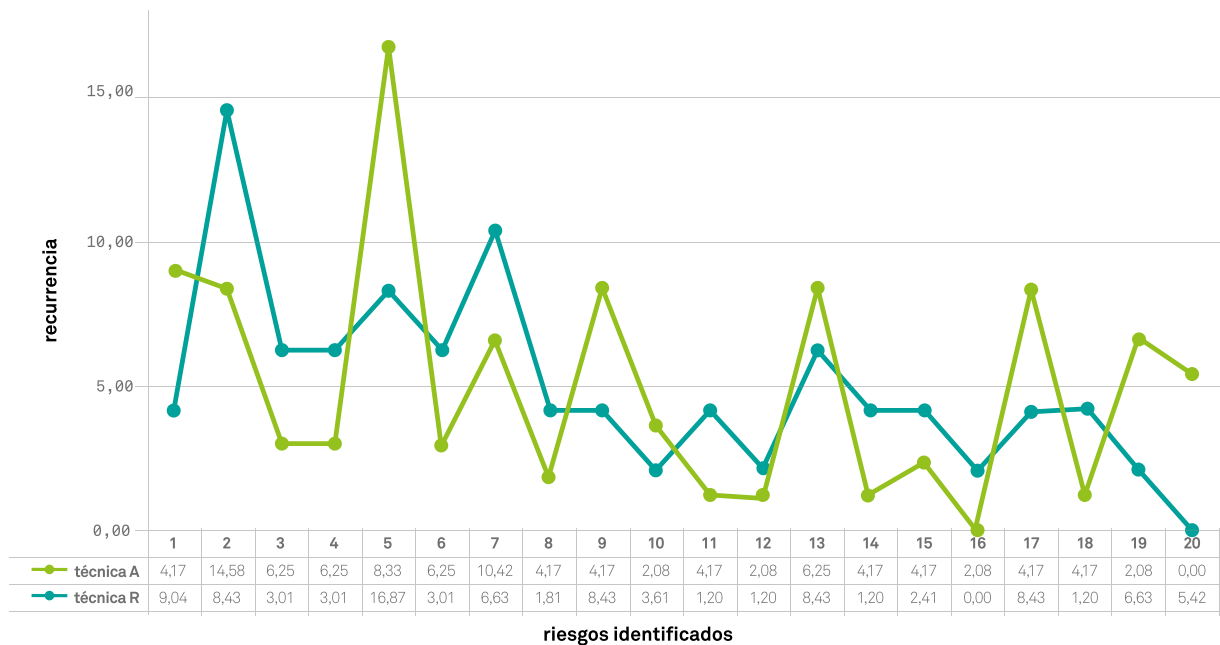


Figura 39 - Líneas de recurrencia en la identificación de riesgos según la técnica empleada (elaboración propia).

A partir de esta observación se realiza un estudio de la desviación entre ambas técnicas, calculando el valor de desviación típica y comparándolo con la desviación real de los valores absolutos entre ambas técnicas. La desviación real se calcula restando los valores para cada riesgo y, a partir del valor resultante se calcula la desviación típica. Para la obtención del valor de desviación típica se emplea la siguiente fórmula, donde s equivale a la variación típica.

$$s = \sqrt{\frac{\sum_{i=1}^n (x_i - \bar{x})^2}{n}}$$

Los resultados se pueden ver en la Figura 40.

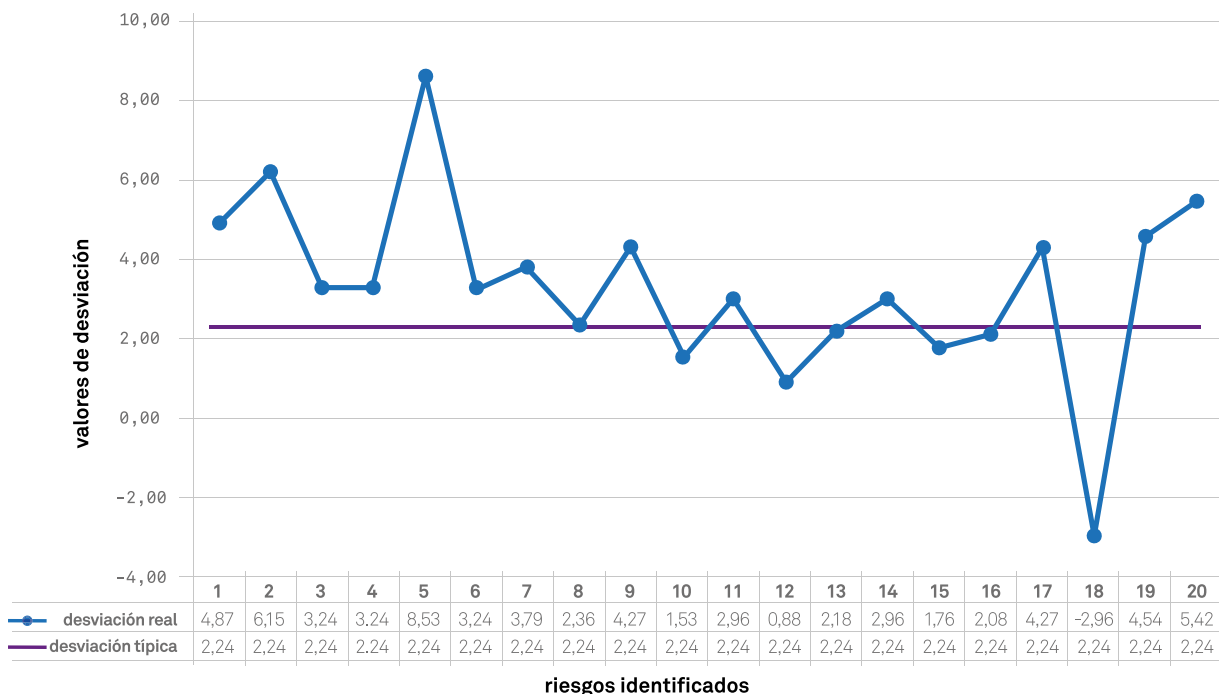


Figura 40 - Desviación típica y real entre las Técnicas A y R (elaboración propia).

El valor de desviación típica es de 2,24. De los valores de desviación real, destacan dos puntas que se sitúan muy por encima y muy por debajo de la desviación típica. Una corresponde al riesgo número 5, con una diferencia entre desviación real y típica de 6,29 puntos. La otra punta corresponde al riesgo 18, con una diferencia de 5,2 puntos. Existen otros 2 riesgos que, como mínimo, duplican el valor de la desviación típica. Estos son los riesgos 2 y 19.

De este gráfico se puede deducir que ambas técnicas no aportan resultados similares. La causa principal es, probablemente, la diferencia en el punto de partida o enfoque inicial del proceso. El punto de partida, más subjetivo, de la Técnica A proporciona una identificación de riesgos basada en situaciones y experiencias concretas. Es posible que aumentando la muestra de personas entrevistadas los resultados sean más amplios, aunque, en este caso, la inversión de tiempo y recursos para la realización del proceso de identificación de riesgos aumentaría considerablemente. Por su parte, cabe mencionar la importancia de una correcta selección de los requisitos que debe cumplir la organización como punto de partida de la Técnica R para una mayor precisión en los resultados de la identificación de riesgos.

Conclusiones

Lo primero que se aprecia es que no se identifica la totalidad de los riesgos siguiendo ambas técnicas, sino que existen algunos que tan solo se manifiestan empleando una de ellas.

Centrando el análisis en los riesgos documentales se puede observar que con ambas técnicas se identifica el mismo número de riesgos. En cambio, si se considera el total de riesgos identificados, incluyendo aquellos relacionados con las aplicaciones informáticas, el incremento es del 26,93 % (19 riesgos con la Técnica A y 26 riesgos con la Técnica R). Se deduce que esto es así debido a que los requisitos empleados para el proceso de identificación provienen de un estándar internacional de gestión documental completo y exhaustivo. Cabe mencionar que la efectividad de esta técnica depende, en gran medida, de los requisitos de base de los que se parta, pudiendo resultar los riesgos identificados diversos, en número y tipo, en función de este criterio. Por tanto, cuanto más completos y exhaustivos sean los requisitos de partida, más efectiva resultará la técnica.

En la Técnica A, se aprecia una mayor subjetividad a la hora de realizar el proceso de identificación. Se parte de una serie de entrevistas semi-estructuradas realizadas a una muestra de personas de la Organización X considerada significativa para la investigación. Se puede observar que los sujetos entrevistados basan la descripción de amenazas en su propia experiencia y en su propio conocimiento. Esto puede conllevar una identificación de riesgos parcial, pero a la vez muy realista, puesto que parte de una realidad concreta.

Se observa, por otro lado, que los riesgos identificados mediante la Técnica R pueden ser fácilmente extrapolables a organizaciones similares. Esto es así porque parten de un análisis pormenorizado de una serie de procesos y requisitos establecidos en un estándar internacional y que son aplicables a cualquier tipo de organización. Partiendo de esta base, es muy probable que una gran parte de las organizaciones se vean amenazadas por las mismas situaciones que la Organización X, haciendo este método extrapolable de manera relativamente sencilla. La diferencia radicará en el análisis y evaluación de dichos riesgos, ya que las variaciones aflorarán en la probabilidad de que ocurra el riesgo y en las consecuencias que puede tener para cada organización.

A través de los resultados obtenidos en este estudio de caso, se considera recomendable emplear ambas técnicas de manera complementaria. De este modo, se puede conseguir una identificación de riesgos conforme a requisitos normalizados, además de disponer de información sobre las experiencias y percepciones de los trabajadores de la organización. Esto puede arrojar resultados depurados sobre los riesgos y amenazas reales que pueden tener consecuencias sobre la organización.

Se considera de suma importancia poder contar en este proceso con el bagaje y experiencia de los trabajadores. Esto proporciona una identificación de riesgos contrastada y menos teórica, por tanto, mucho más realista y funcional.

Por otro lado, cabe destacar el desconocimiento de los requisitos de gestión documental de la organización por parte de las personas involucradas en el estudio. Se conocía la existencia del área de gestión documental y archivo, pero las distintas áreas de la organización, en algunos casos, desconocían cómo gestionar los documentos de su

día a día y qué directrices seguir. Esto puede ser debido a una falta de acciones de concienciación, comunicación y formación, debido al gran tamaño de la organización estudiada y a los pocos recursos de los que se manifiesta disponer. Con el objetivo de prevenir o mitigar los riesgos documentales identificados, una primera acción que debe plantearse la organización va en esta línea de concienciación básica en la materia. Más adelante, se presentan una serie de acciones para el tratamiento de los riesgos.

Otra conclusión de este proceso se corresponde con la poca madurez del sistema de gestión documental de la Organización X con relación a los requisitos de la norma ISO 30301. La identificación de riesgos documentales según la Técnica R, tal y como se ha explicado, parte de los requisitos incluidos en el Anexo A de dicha norma, lo que supone una buena parte de los requerimientos que debe cumplir cualquier organización que tenga el objetivo de certificarse según esta norma ISO. Se aprecia, a partir del proceso de identificación de riesgos, que la Organización X no está preparada para enfrentarse a un proceso de certificación de su sistema de gestión documental. El motivo principal es la inmadurez del mismo, que se hace patente a través de los riesgos documentales identificados, y que se relacionan directamente con incumplimientos de requisitos.

Por último, se detecta una cierta inconsciencia del personal sobre las situaciones de riesgo documental que se dan en la organización. Esta situación se puede considerar un riesgo en sí misma, ya que una de las premisas para la prevención de riesgos es precisamente la conciencia y el conocimiento de dichos riesgos. A esto se suma la inconsciencia sobre el tratamiento de los riesgos. En las entrevistas, el personal explicó algunas acciones que se llevan a cabo en distintas áreas con la finalidad de evitar situaciones negativas. Pese a que el personal de la Organización X no es consciente, en realidad, estas iniciativas son acciones de tratamiento o prevención de riesgos. Estas dos situaciones de desconocimiento, tanto de riesgos como de prevenciones, son sintomáticas de la inmadurez de la organización con relación a la cuestión de estudio.

5.3.2 Análisis de riesgos

Para el análisis de los riesgos se trabaja con dos técnicas distintas, seleccionadas de la norma internacional ISO/IEC 31010 y que son: la matriz de consecuencia y probabilidad, y el análisis de pajarita. Se explican a continuación.

Matriz de consecuencia/probabilidad

La matriz de consecuencia/probabilidad implica la combinación de clasificaciones cualitativas o semicuantitativas de consecuencias y de probabilidad para dar lugar a un nivel de riesgo o a una clasificación de los riesgos. El formato de la matriz y las definiciones aplicadas dependen del contexto en el que se usen. Es importante emplear un diseño adecuado a las circunstancias, en este caso, una administración pública municipal.

Este método se utiliza para jerarquizar o clasificar riesgos, fuentes de riesgo o tratamientos de riesgos basándose en el nivel de riesgo. Normalmente se utiliza como una herramienta de filtrado cuando se han identificado una gran cantidad de riesgos, por ejemplo, para definir cuáles necesitan mayor nivel de detalle en el análisis, cuáles necesitan ser tratados con prioridad o cuales necesitan consultarse con un nivel superior de mando. También resulta útil para seleccionar aquellos riesgos que no necesitan ser tratados de manera inmediata, en función de los criterios de riesgo establecidos por la organización. Esta matriz también se utiliza de manera generalizada para determinar si un riesgo es aceptable o no, con relación a su posición dentro de la matriz.

Por tanto, se obtiene información que ayuda, en la siguiente fase, a priorizar acciones de tratamiento y prevención de manera rápida y fiable.

Para llegar a cabo el proceso se necesita una serie de información. Las entradas del proceso consisten en escalas de consecuencia y de probabilidad, y en una matriz que combine ambas.

La escala de consecuencia o severidad debe cubrir el rango de los distintos tipos de consecuencias a considerar en la organización (por ejemplo, pérdidas financieras, seguridad, medio ambiente u otros parámetros en función del contexto) y debe abarcar desde la mayor consecuencia creíble hasta la mínima consecuencia. La escala puede tener varios niveles de puntuación. Las escalas suelen ser de 3, 4 o 5 puntos o niveles. La escala de probabilidad también puede tener varios niveles de puntuación.

Las definiciones de probabilidad y consecuencia necesitan elaborarse de manera que sean lo menos ambiguas posibles.

Para llevar a cabo el proceso, se debe dibujar una matriz con las consecuencias en un eje y las probabilidades en el otro eje (ver Figura 41). Los niveles de riesgo asignados a las celdas dependen de las definiciones que se hayan dado en las escalas de probabilidad y de consecuencia. Los niveles de riesgo pueden relacionarse con las reglas de decisión, como por ejemplo la prioridad de acción (tratamiento) sobre el riesgo.

CLASIFICACIÓN DE LA PROBABILIDAD	E	IV	III	II	I	I	I
	D	IV	III	III	II	I	I
	C	V	IV	III	II	II	I
	B	V	IV	III	III	II	I
	A	V	V	IV	III	II	II
		1	2	3	4	5	6
		CLASIFICACIÓN DE LA CONSECUENCIA					

Figura 41 - Ejemplo de una matriz de consecuencia/probabilidad (ISO/IEC 31010, B.29.3).

Para clasificar los riesgos, lo primero que se debe hacer es encontrar el descriptor de consecuencia que mejor encaje con la situación. Entonces se define la probabilidad con la que aquellas consecuencias pueden ocurrir. El nivel de riesgo se mide a partir de la matriz.

El resultado obtenido consiste en una clasificación de cada riesgo o una lista de riesgos con los niveles significativos definidos.

Como todos los métodos de análisis, la matriz de consecuencia/probabilidad tiene puntos fuertes y puntos débiles a tener en cuenta. Las fortalezas incluyen (AENOR 2011a, p. 94):

- Es relativamente fácil de utilizar.
- Proporciona una clasificación jerarquizada de los riesgos en diferentes niveles significativos, de manera rápida.

Las debilidades incluyen (AENOR 2011a, p. 95):

- La matriz debe diseñarse de manera que resulte apropiada a las circunstancias y, por tanto, puede resultar difícil disponer de un sistema común para aplicar en una gama de circunstancias relevantes dentro de una organización.
- Es difícil definir las escalas de manera inequívoca.
- El uso es subjetivo y tiende a darse una variación significativa según quien clasifica.
- Los riesgos no pueden sumarse (es decir, no se puede definir un grupo de riesgos de bajo nivel o un número de veces que se ha identificado un riesgo de bajo nivel como equivalente a un riesgo medio).
- Es difícil combinar o comparar el nivel de riesgo para diferentes categorías o consecuencias.

Siguiendo esta técnica, se debe analizar cada riesgo con relación a la combinación de la probabilidad de que ocurra y las consecuencias que pueden alcanzarse si realmente ocurre. Para ello se emplea un método semi-cuantitativo utilizando escalas numéricas para ambos parámetros. La probabilidad de que un riesgo ocurra se analiza de acuerdo al contexto y a la naturaleza de dicho riesgo, así como empleando aquellos datos de los que se dispone de las fases anteriores del proceso.

En la Organización X se trabaja con una matriz de 3 niveles de probabilidad y 3 niveles de severidad. Pese a ello, en este estudio de caso se opta por una definición de 5 niveles para cada uno de estos parámetros ya que es necesario un mayor nivel de detalle. Se definen, por tanto, cinco niveles de probabilidad, tal y como se determina en la siguiente figura (ver Figura 42).

PUNTUACIÓN DE PROBABILIDAD	INTERPRETACIÓN
1	Probabilidad muy baja, al menos una vez cada 2 años.
2	Probabilidad baja, al menos una vez al año.
3	Probabilidad media, al menos una vez cada 6 meses.
4	Probabilidad alta, al menos una vez al mes
5	Probabilidad muy alta, al menos una vez a la semana

Figura 42 - Niveles de probabilidad (elaboración propia).

Para el análisis de las consecuencias se definen cinco niveles, tal y como se determina en la siguiente figura (ver Figura 43).

PUNTUACIÓN DE CONSECUENCIA	INTERPRETACIÓN
1	Menor, afectará a un área con una duración inferior un día.
2	Moderada, afectará a unas o más áreas con una duración inferior a una semana.
3	Mayor, afectará a más de un área con una duración superior a una semana e inferior a un mes.
4	Severa, afectará a más de un área con una duración superior a un mes e inferior a un año.
5	Muy severa, afectará a más de un área con una duración superior a un año.

Figura 43 - Niveles de consecuencia (elaboración propia).

Para determinar el nivel de riesgo, se deben cruzar los resultados del análisis de probabilidades con los resultados del análisis de consecuencias. Para ello se determina la siguiente matriz (ver Figura 44).

		PROBABILIDAD				
		1	2	3	4	5
CONSECUENCIAS	1	I	II	III	IV	V
	2	II	III	IV	V	VI
	3	III	IV	V	VI	VII
	4	IV	V	VI	VII	VIII
	5	V	VI	VII	VIII	IX

Figura 44 - Matriz de consecuencia/probabilidad (elaboración propia basada en la norma ISO/IEC 31010).

Al cruzar los valores de la matriz de consecuencia/probabilidad se obtiene como resultado los siguientes niveles de riesgo (ver Figura 45):

VALOR DE LA MATRIZ	NIVEL DE RIESGO
I	Irrelevante
II	Extremadamente leve
III	Muy leve
IV	Leve
V	Moderado
VI	Considerable
VII	Importante
VIII	Severo
IX	Intolerable

Figura 45 - Niveles de riesgo (elaboración propia).

Los resultados del análisis se obtienen a partir de la información recopilada en las fases anteriores, así como de la observación directa. No existen en la organización instrumentos de medida e indicadores que faciliten el seguimiento y la obtención de datos para realizar este tipo de análisis, lo que supone una debilidad y puede resultar en

una valoración con un mayor grado de subjetividad que si se realizase de otro modo. Es conveniente poder desarrollar una serie de indicadores objetivos para medir aspectos de probabilidad y consecuencia, para poder arrojar resultados imparciales.

En la siguiente figura se pueden ver los resultados obtenidos del análisis de riesgos, siguiendo las variables definidas en las tablas anteriores, con la asignación del nivel de riesgo. (ver Figura 46).

N	RIESGO IDENTIFICADO	PROBABILIDAD	CONSECUENCIA	NIVEL
1	Pérdida de información/documentación	2	4	V
2	Falta de garantías de integridad	2	4	V
3	Pérdida de documentos esenciales	2	5	VI
4	No creación de evidencias documentales	3	2	IV
5	No recuperación de información/documentación	3	3	V
6	Accesos indebidos a información	3	3	V
7	Eliminación indebida de documentos	2	5	VI
8	Sustracción o robo de documentos	1	5	V
9	Falta de garantías de accesibilidad	2	4	V
10	Falta de garantías de usabilidad	1	4	IV
11	No eliminación de documentos	2	2	III
12	Ubicación errónea o indebida de documentos	3	4	VI
13	Manipulación no autorizada de documentos	2	4	V
14	Duplicidad documental	3	1	III
15	Creación innecesaria de documentos	3	1	III
16	Duplicación de instrumentos de gestión documental	1	4	IV
17	Falta de garantías de trazabilidad	3	5	VII
18	Falta de garantías de autenticidad	2	5	VI
19	Falta de garantías de fiabilidad	2	5	VI
20	Errores en la descripción documental	2	3	IV
21	Desarrollo no controlado de aplicaciones	1	4	IV
22	Falta de interoperabilidad	3	4	VI
23	Falta de respuesta ante fallos del sistema	1	2	II
24	Infraestructura insuficiente	1	4	IV
25	Interrupción de la actividad	1	2	II
26	Accesos indebidos a las aplicaciones	3	2	IV
27	Incapacidad para acceder a las aplicaciones	1	1	I

Figura 46 - Análisis de riesgos de la Organización X siguiendo la matriz de consecuencia/probabilidad (elaboración propia).

En la siguiente figura (ver Figura 47) se puede observar la distribución por niveles de los distintos riesgos documentales analizados.

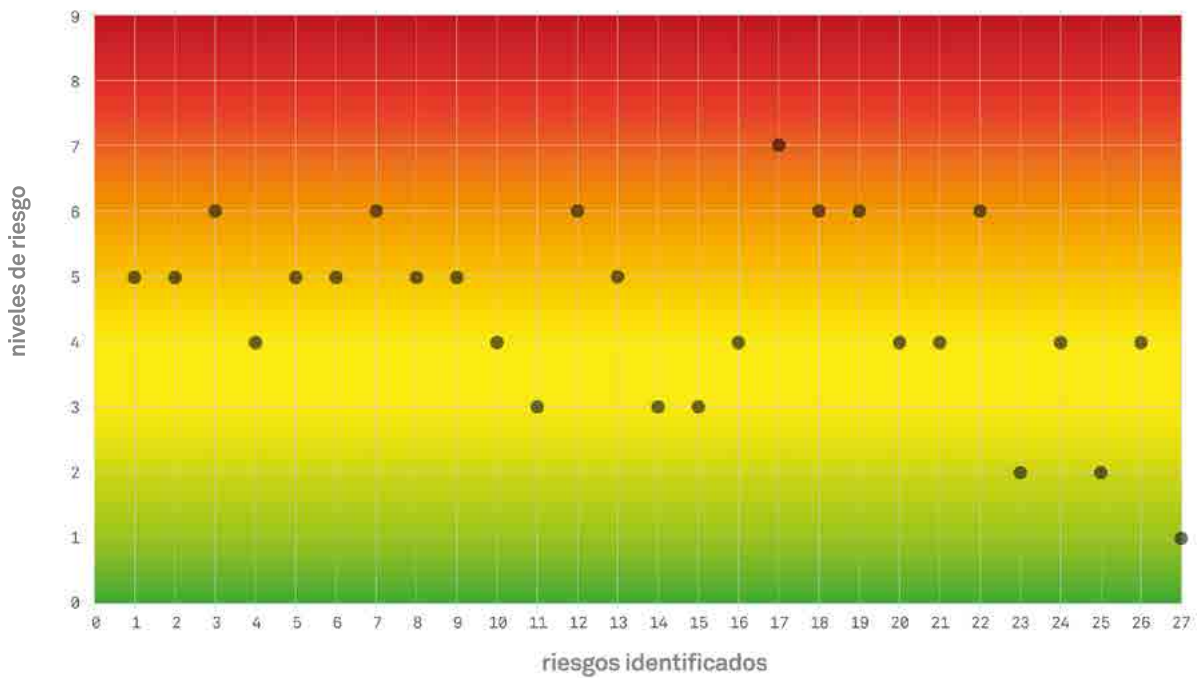


Figura 47 - Niveles de riesgo de la Organización X (elaboración propia).

Se observa que la mayoría de los riesgos tienen un nivel superior a 3, situándose igual o por debajo tan solo el 22,22 %. La mayoría de los riesgos se sitúa entre los niveles de 4 a 6, concretamente el 74,07 %. Por último, tan solo un riesgo se sitúa entre niveles de 7 a 9, que son los superiores, y se corresponde con el 3,7 % del total. No hay riesgos identificados con niveles superiores a 7. Por tanto, la mayoría de riesgos queda enmarcado entre niveles intermedios. En la siguiente figura se puede observar la distribución de porcentajes según el nivel de riesgo (ver Figura 48).

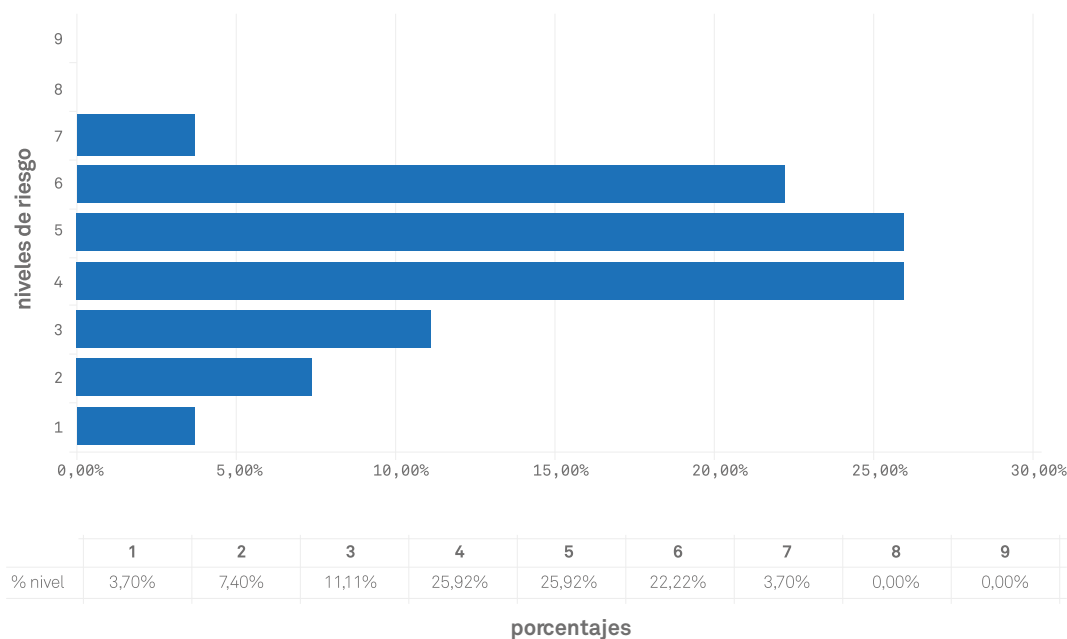


Figura 48 - Distribución de porcentajes según el nivel de riesgo (elaboración propia).

Esta distribución indica que una gran parte de los riesgos identificados tienen un nivel medio. El 51,84 %, más de la mitad, quedan situados entre el nivel 5 o moderado y el nivel 7 o importante. Un dato positivo a destacar es que ninguno de los riesgos queda situado por encima del nivel 7.

Análisis de pajarita

Se trata de un método esquemático sencillo para describir y analizar las trayectorias de un riesgo desde sus causas hasta sus consecuencias. El enfoque del análisis de pajarita se centra en los obstáculos o barreras entre las causas y el riesgo, y entre el riesgo y las consecuencias. Se utiliza para representar un riesgo, mostrando un abanico de posibles causas y consecuencias.

Para iniciar el proceso es necesaria una comprensión de la información de las causas y las consecuencias de un riesgo, así como de las barreras y controles que pueden prevenirlo, mitigarlo o incitarlo. El proceso sigue los siguientes pasos (AENOR 2011a, p. 72):

1. Identificar un riesgo determinado para el análisis y representarlo como el nudo central de una pajarita.
2. Enumerar las causas del riesgo.
3. Identificar el mecanismo por el cual se provoca el suceso crítico.
4. Dibujar líneas entre cada causa y el evento, conformando la parte izquierda de la pajarita.

5. Las barreras que deben prevenir que cada causa provoque las consecuencias indeseadas pueden verse representadas como barras en vertical sobre las líneas. En aquellas situaciones en que haya factores que puedan causar una intensificación, también se representan barreras de intensificación.
6. Identificar, en la parte derecha de la pajarita, las diferentes consecuencias potenciales y dibujar líneas que irradian desde el evento de riesgo hacia cada consecuencia potencial.
7. Las barreras de cada consecuencia se dibujan con barras sobre las líneas radiales.

El resultado es un diagrama sencillo que muestra las trayectorias del riesgo principal y las barreras que previenen o mitigan las consecuencias no deseadas, o estimulan y promueven las consecuencias deseadas (ver Figura 49).



Figura 49 - Ejemplo de un diagrama de pajarita (ISO/IEC 31010, B.21.5).

Las fortalezas del proceso incluyen (AENOR 2011a, p. 73):

- Es fácil de entender y aporta una representación gráfica clara del problema.
- Focaliza la atención en los controles que se supone que existen para prevenir y mitigar su efectividad.
- Puede utilizarse para consecuencias deseadas.
- No necesita un alto grado de experiencia para poder emplearse.

Las debilidades incluyen (AENOR 2011a, p. 73):

- No se pueden representar situaciones en que múltiples causas suceden de manera simultánea para causar las consecuencias.
- Puede simplificar demasiado las situaciones complejas.

Uno de los objetivos de usar la técnica de análisis de pajarita es identificar los controles preventivos existentes en la organización que podían ayudar a la mitigación de los riesgos. Para identificar estos controles se realizó una entrevista con la persona responsable del área de gestión documental y archivo de la Organización X el 31 de octubre del año 2017, con el objetivo de analizar cada uno de los riesgos junto a las causas de las que podían derivar y, de este análisis, poder identificar los controles preventivos existentes. No se incluyeron en el análisis los controles de intensificación de causas, tan solo los de prevención.

Se identifican, de este modo, diez controles preventivos, que se enumeran y explican en la siguiente figura (ver Figura 50). Se asigna un número identificativo a cada uno de ellos. Se representan en los gráficos de pajarita mediante barras verticales en las que se incluye dicho número.

NÚM.	CÓDIGO	CONTROLES PREVENTIVOS EXISTENTES
1	1	Controles de acceso a los depósitos físicos de custodia de documentación, normalmente mediante llave.
2	2	Controles de acceso a los edificios donde se encuentran los depósitos que custodian documentos.
3	3	Supervisión de los traslados de documentación entre edificios a través de una comisión cuyo máximo responsable es el jefe del área de archivo y gestión documental de la Organización X. Los traslados se realizan por una empresa que cumple con los requisitos de no alteración de la documentación y confidencialidad. No se tienen en consideración los traslados dentro de un mismo edificio.
4	4	Control automatizado de la temperatura y la humedad relativa en todos los depósitos de archivo (documentación semiactiva e inactiva).
5	5	Clasificación de documentos que se transfieren al archivo realizada siempre por técnicos superiores titulados en archivística y gestión de documentos, con lo que las incidencias deberían ser mínimas.
6	6	Automatización de la gestión para aquellos trámites que conllevan una “aprobación”, siendo obligatoria la gestión electrónica de los mismos. Dentro de este proceso, no es posible continuar el trámite si la clasificación del expediente no se ha realizado de manera adecuada.
7	7	Procedimiento reglado e instrucción del año 2014 enviada a todos los departamentos con la explicación sobre el proceso de eliminación.
8	8	Comisión de trabajo para el conocimiento en profundidad de las diferentes aplicaciones con las que se trabaja en la organización. El objetivo es que a partir de este conocimiento se puedan encarar nuevas etapas de gestión electrónica de un modo más controlado. Esta comisión ayuda a identificar el mal funcionamiento o posibles incidencias de las aplicaciones, contribuyendo a la prevención de que ocurran.
9	9	Acciones formativas realizadas de manera periódica y lideradas por el área de archivo y gestión documental. Además, todos los instrumentos están disponibles para el personal a través de la intranet de la organización.
10	12	Único canal de comunicación para todo lo relacionado con la gestión de documentos, siendo la persona responsable del área de archivo y gestión documental la encargada de llevar a cabo todas las comunicaciones para evitar duplicidades y malentendidos.

Figura 50 - Controles de prevención existentes en la Organización X (elaboración propia).

Durante la entrevista realizada con la responsable de gestión documental y archivo, se identifica también una acción correctiva que se lleva a cabo en la organización con relación a las situaciones de riesgo identificadas. En la Figura 51 se explica este control correctivo existente. En este caso, no puede considerarse una acción para mitigar o eliminar las causas, aunque sí puede resultar una solución a las incidencias que se detecten, dando respuestas rápidas y concretas.

NÚM.	CÓDIGO	CONTROLES CORRECTIVOS EXISTENTES
1	10	En caso de incidencia sobre la temperatura o humedad de los depósitos se avisa inmediatamente al Servicio de Mantenimiento de Edificios Municipales para que den solución.

Figura 51 - Controles correctivos existentes en la Organización X (elaboración propia).

Cabe destacar que el personal de la Organización X no era consciente de disponer de este tipo de controles (preventivos y correctivos) como tales, sino que para ellos se trataba de mecanismos e instrumentos para la gestión del día a día. Esta es una cuestión importante, que contribuye a la idea de que la implantación de sistemas de gestión documental funciona como un mecanismo de prevención de riesgos corporativo, en este caso de manera inconsciente, pero directa. Esta idea de que la gestión documental contribuye a la prevención de riesgos en las organizaciones no es nueva, pese a que aparece en los estándares internacionales en sus últimas publicaciones, como por ejemplo la actualización de la norma ISO 15489 del año 2016.

A continuación, se presenta el análisis de cada riesgo documental mediante la técnica de pajarita, incluyendo los controles preventivos y correctivos existentes.

Riesgo 1 – Pérdida de información/documentación.

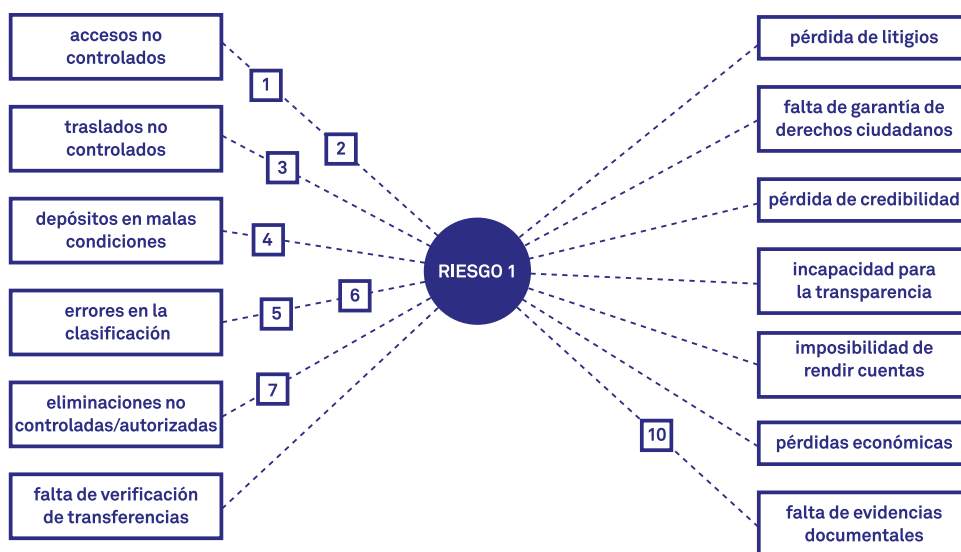


Figura 52 - Análisis de pajarita para el riesgo 1 (elaboración propia).

El riesgo 1 se ve afectado por 6 causas (a la izquierda de la pajarita) y puede tener afectación en 7 tipos de consecuencias distintos (a la derecha de la pajarita). Para evitar que el riesgo ocurra, en la organización existen 7 controles preventivos y un control correctivo.

Riesgo 2 – Falta de garantías de integridad

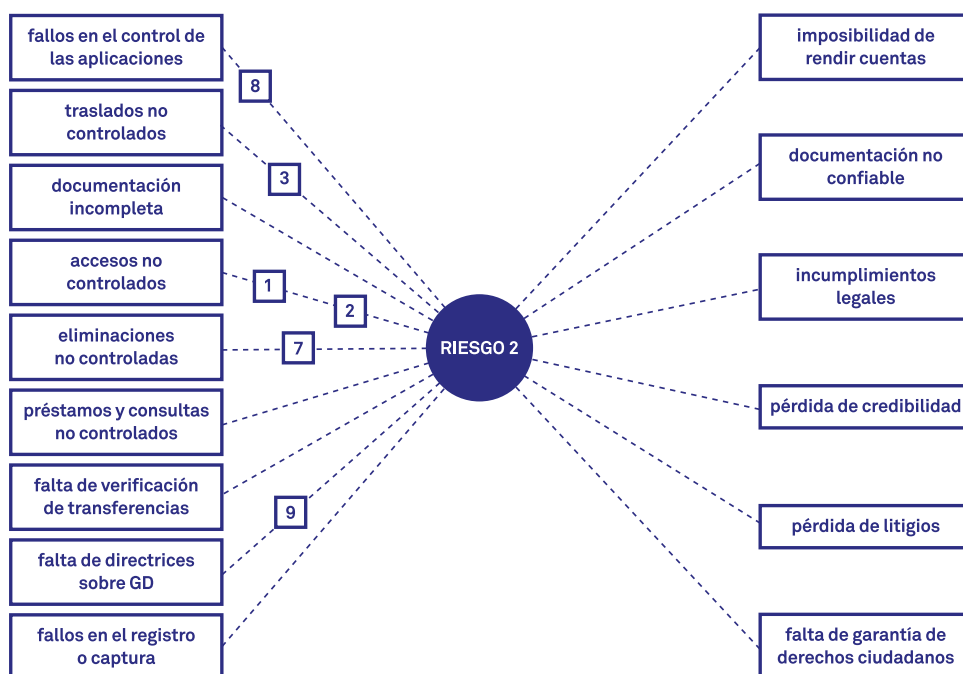


Figura 53 - Análisis de pajarita para el riesgo 2 (elaboración propia).

El riesgo 2 se ve afectado por 9 causas (a la izquierda de la pajarita) y puede tener afectación en 6 tipos de consecuencias distintas (a la derecha de la pajarita). Para evitar que el riesgo ocurra, en la organización existen 6 controles preventivos.

Riesgo 3 – Pérdida de documentos esenciales

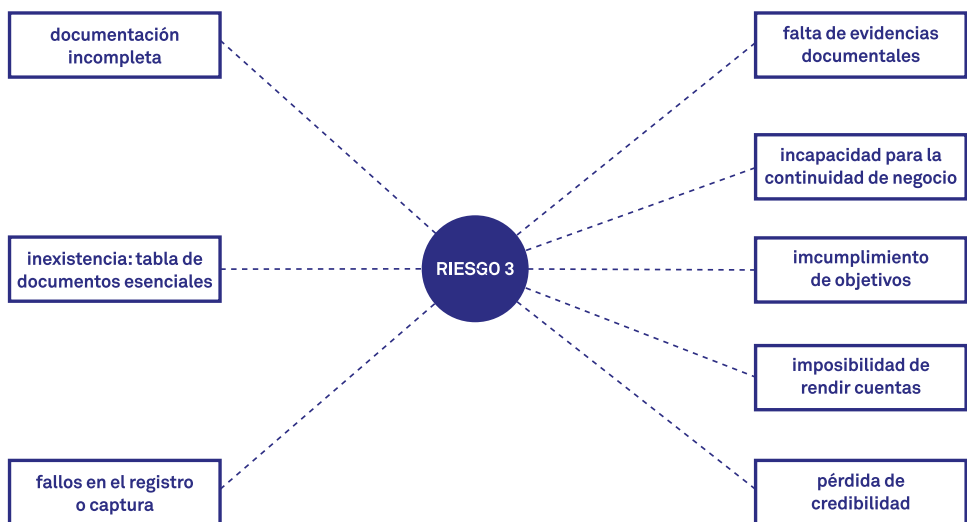


Figura 54 - Análisis de pajarita para el riesgo 3 (elaboración propia).

El riesgo 3 se ve afectado por 3 causas (a la izquierda de la pajarita) y puede tener afectación en 5 tipos de consecuencias distintos (a la derecha de la pajarita). No existen controles preventivos ni correctivos en la organización.

Riesgo 4 – No creación de evidencias documentales

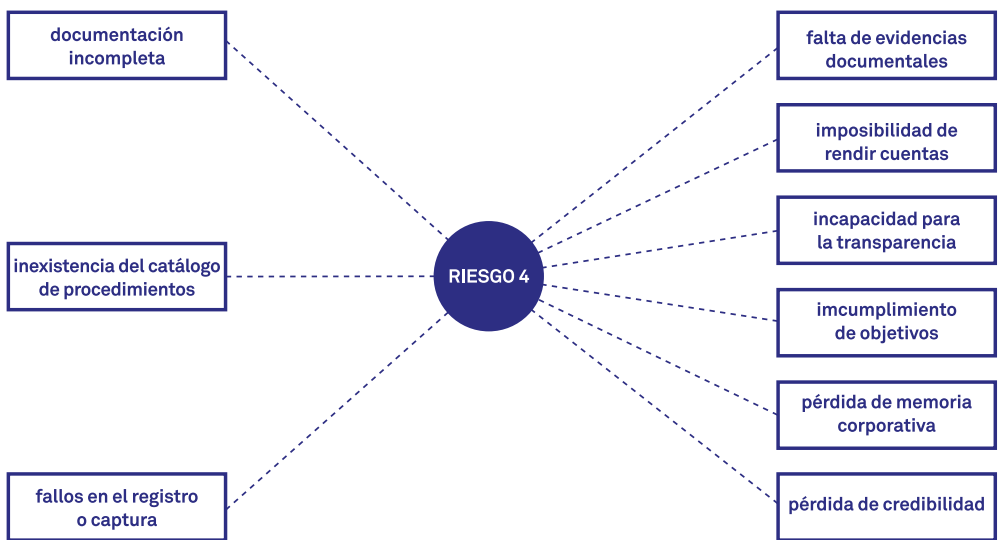


Figura 55 - Análisis de pajarita para el riesgo 4 (elaboración propia).

El riesgo 4 se ve afectado por 3 causas (a la izquierda de la pajarita) y puede tener afectación en 6 tipos de consecuencias distintos (a la derecha de la pajarita). No existen controles preventivos ni correctivos en la organización.

Riesgo 5 – No recuperación de información/documentación

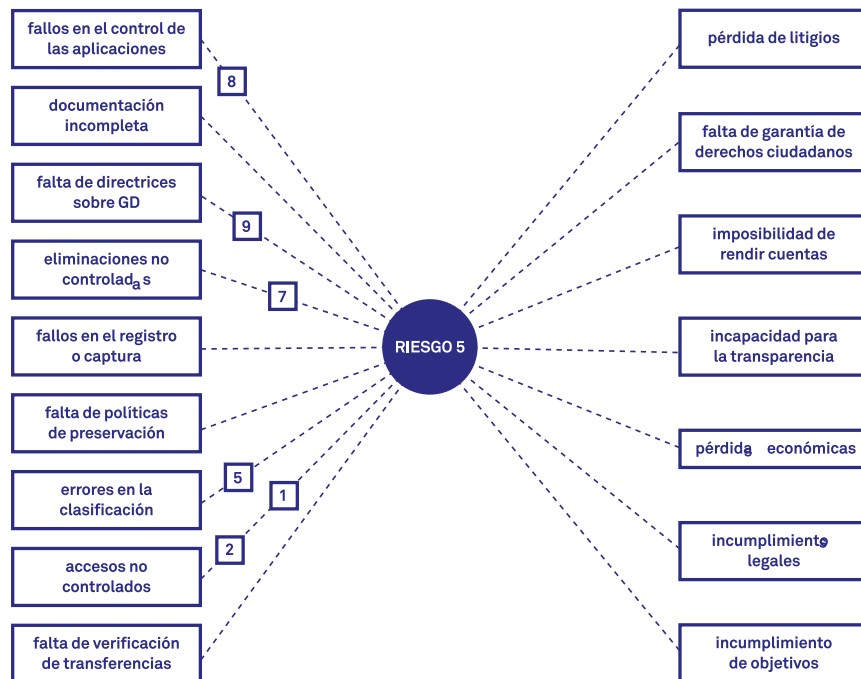


Figura 56 - Análisis de pajarita para el riesgo 5 (elaboración propia).

El riesgo 5 se ve afectado por 9 causas (a la izquierda de la pajarita) y puede tener afectación en 7 tipos de consecuencias distintas (a la derecha de la pajarita). Para evitar que el riesgo ocurra, en la organización existen 6 controles preventivos.

Riesgo 6 – Accesos indebidos a información

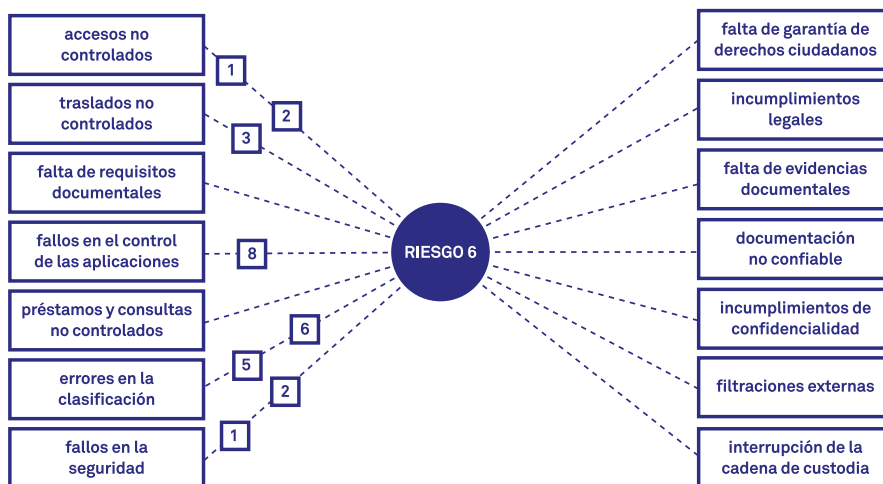


Figura 57 - Análisis de pajarita para el riesgo 6 (elaboración propia).

El riesgo 6 se ve afectado por 7 causas (a la izquierda de la pajarita) y puede tener afectación en 7 tipos de consecuencias distintas (a la derecha de la pajarita). Para evitar que el riesgo ocurra, en la organización existen 8 controles preventivos.

Riesgo 7 – Eliminación indebida de documentos

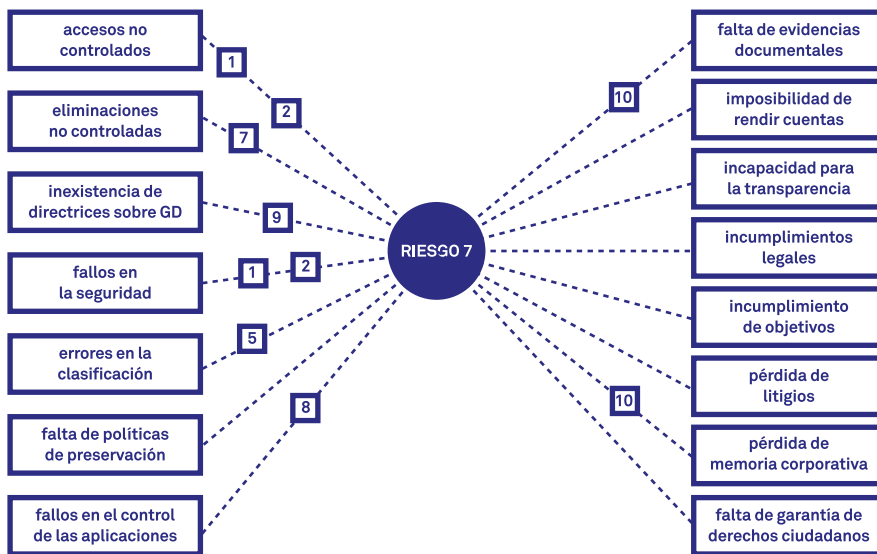


Figura 58 - Análisis de pajarita para el riesgo 7 (elaboración propia).

El riesgo 7 se ve afectado por 7 causas (a la izquierda de la pajarita) y puede tener afectación en 8 tipos de consecuencias distintos (a la derecha de la pajarita). Para evitar que el riesgo ocurra, en la organización existen 8 controles preventivos y 2 correctivos.

Riesgo 8 – Sustracción o robo de documentos

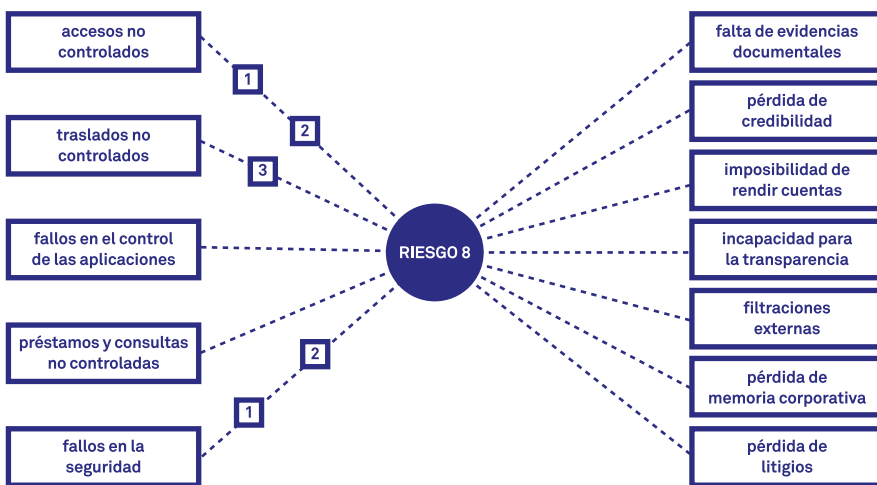


Figura 59 - Análisis de pajarita para el riesgo 8 (elaboración propia).

El riesgo 8 se ve afectado por 5 causas (a la izquierda de la pajarita) y puede tener afectación en 7 tipos de consecuencias distintos (a la derecha de la pajarita). Para evitar que el riesgo ocurra, en la organización existen 5 controles preventivos.

Riesgo 9 – Falta de garantías de accesibilidad

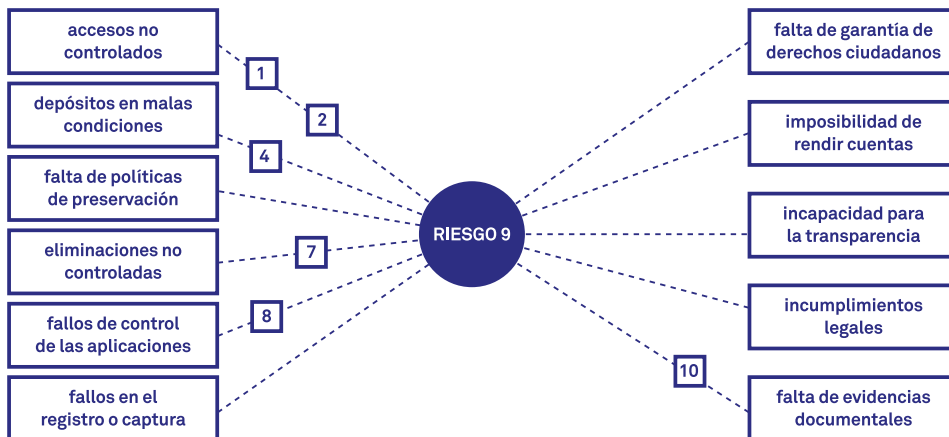


Figura 60 - Análisis de pajarita para el riesgo 9 (elaboración propia).

El riesgo 9 se ve afectado por 6 causas (a la izquierda de la pajarita) y puede tener afectación en 5 tipos de consecuencias distintos (a la derecha de la pajarita). Para evitar que el riesgo ocurra, en la organización existen 5 controles preventivos y uno correctivo.

Riesgo 10 – Falta de garantías de usabilidad

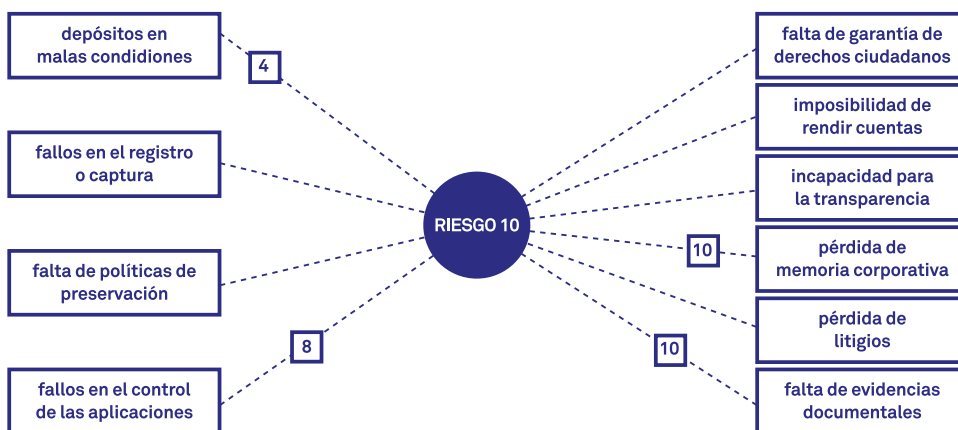


Figura 61 - Análisis de pajarita para el riesgo 10 (elaboración propia).

El riesgo 10 se ve afectado por 4 causas (a la izquierda de la pajarita) y puede tener afectación en 6 tipos de consecuencias distintos (a la derecha de la pajarita). Para evitar que el riesgo ocurra, en la organización existen 2 controles preventivos y 2 correctivos.

Riesgo 11 – No eliminación de documentos

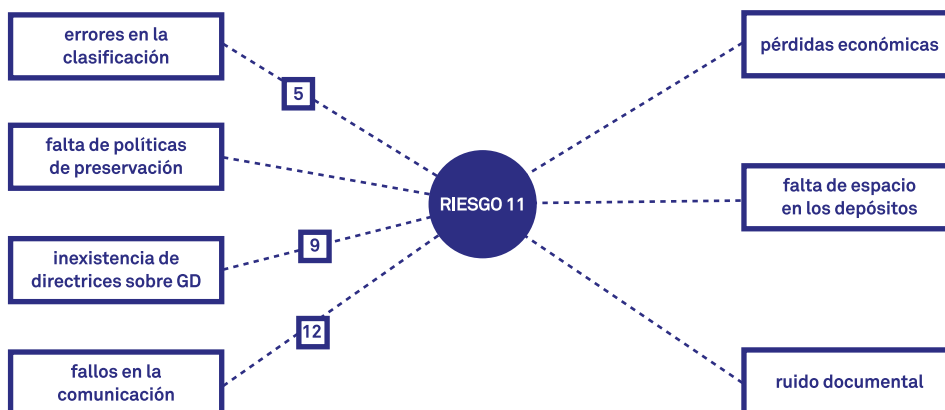


Figura 62 - Análisis de pajarita para el riesgo 11 (elaboración propia).

El riesgo 11 se ve afectado por 4 causas (a la izquierda de la pajarita) y puede tener afectación en 3 tipos de consecuencias distintos (a la derecha de la pajarita). Para evitar que el riesgo ocurra, en la organización existen 3 controles preventivos.

Riesgo 12 – Ubicación errónea o indebida de documentos

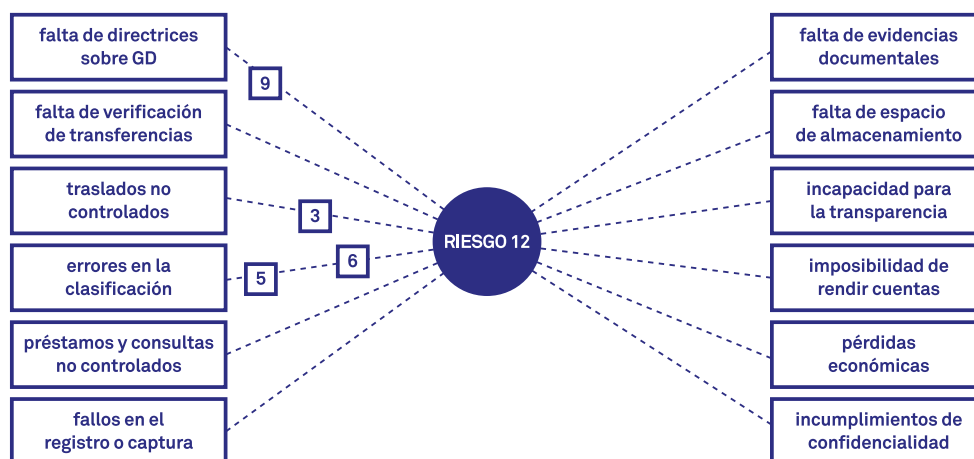


Figura 63 - Análisis de pajarita para el riesgo 12 (elaboración propia).

El riesgo 12 se ve afectado por 6 causas (a la izquierda de la pajarita) y puede tener afectación en 6 tipos de consecuencias distintos (a la derecha de la pajarita). Para evitar que el riesgo ocurra, en la organización existen 4 controles preventivos.

Riesgo 13 – Manipulación no autorizada de documentos

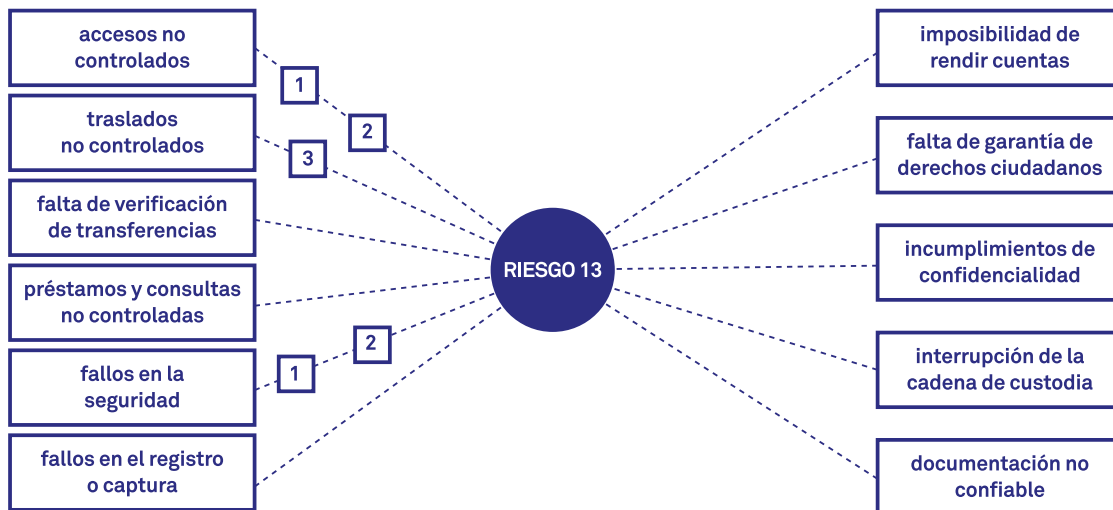


Figura 64 - Análisis de pajarita para el riesgo 13 (elaboración propia).

El riesgo 13 se ve afectado por 6 causas (a la izquierda de la pajarita) y puede tener afectación en 5 tipos de consecuencias distintos (a la derecha de la pajarita). Para evitar que el riesgo ocurra, en la organización existen 5 controles preventivos.

Riesgo 14 – Duplicidad documental

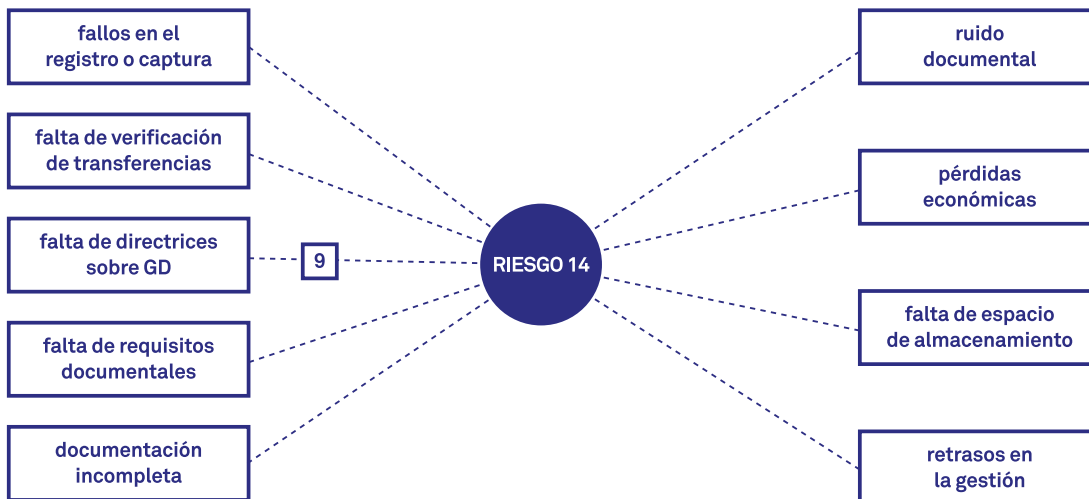


Figura 65 - Análisis de pajarita para el riesgo 14 (elaboración propia).

El riesgo 14 se ve afectado por 5 causas (a la izquierda de la pajarita) y puede tener afectación en 4 tipos de consecuencias distintos (a la derecha de la pajarita). Para evitar que el riesgo ocurra, en la organización existe un control preventivo.

Riesgo 15 – Creación innecesaria de documentos

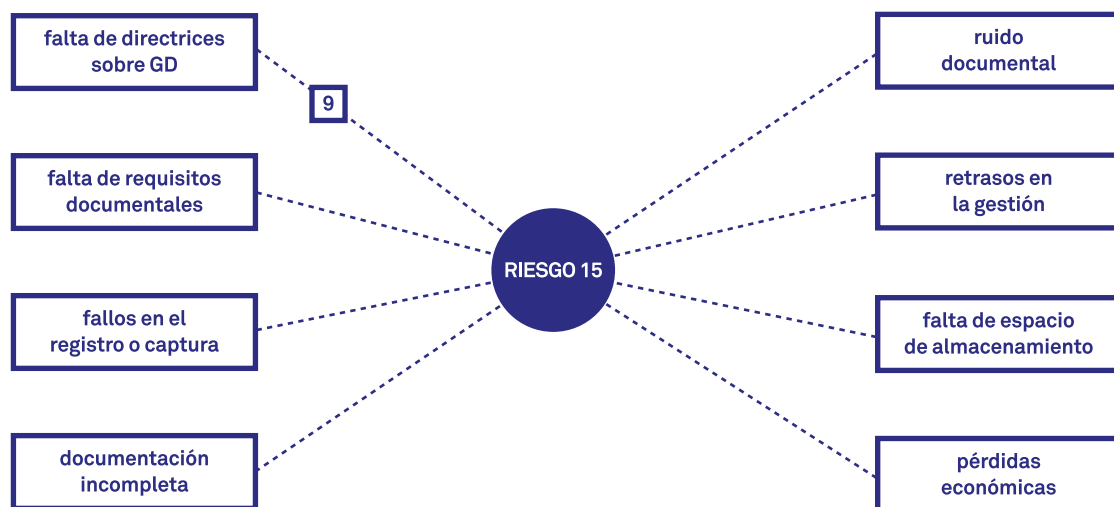


Figura 66 - Análisis de pajarita para el riesgo 15 (elaboración propia).

El riesgo 15 se ve afectado por 4 causas (a la izquierda de la pajarita) y puede tener afectación en 4 tipos de consecuencias distintos (a la derecha de la pajarita). Para evitar que el riesgo ocurra, en la organización existe un control preventivo.

Riesgo 16 – Duplicación de instrumentos de gestión documental

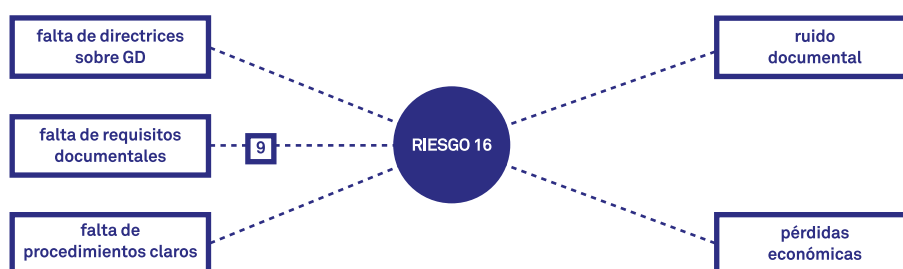


Figura 67 - Análisis de pajarita para el riesgo 16 (elaboración propia).

El riesgo 16 se ve afectado por 3 causas (a la izquierda de la pajarita) y puede tener afectación en 2 tipos de consecuencias distintos (a la derecha de la pajarita). Para evitar que el riesgo ocurra, en la organización existe un control preventivo.

Riesgo 17 – Falta de garantías de trazabilidad

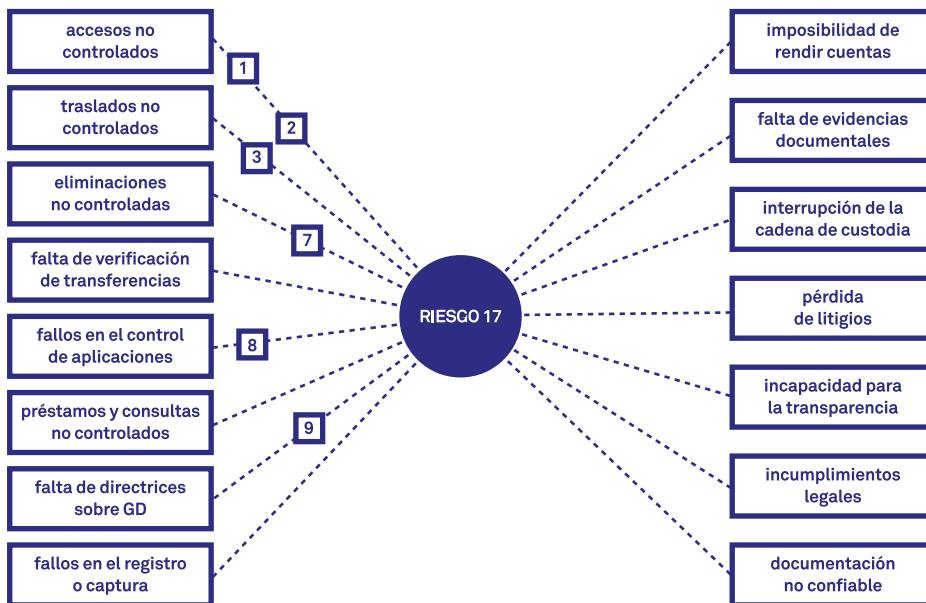


Figura 68 - Análisis de pajarita para el riesgo 17. (elaboración propia).

El riesgo 17 se ve afectado por 8 causas (a la izquierda de la pajarita) y puede tener afectación en 7 tipos de consecuencias distintos (a la derecha de la pajarita). Para evitar que el riesgo ocurra, en la organización existen 6 controles preventivos.

Riesgo 18 – Falta de garantías de autenticidad

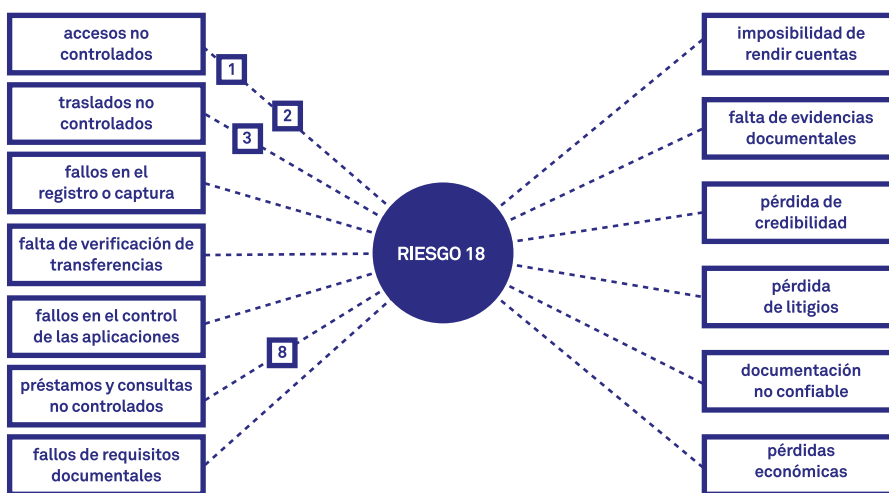


Figura 69 - Análisis de pajarita para el riesgo 18 (elaboración propia).

El riesgo 18 se ve afectado por 7 causas (a la izquierda de la pajarita) y puede tener afectación en 6 tipos de consecuencias distintos (a la derecha de la pajarita). Para evitar que el riesgo ocurra, en la organización existen 4 controles preventivos.

Riesgo 19 – Falta de garantías de fiabilidad

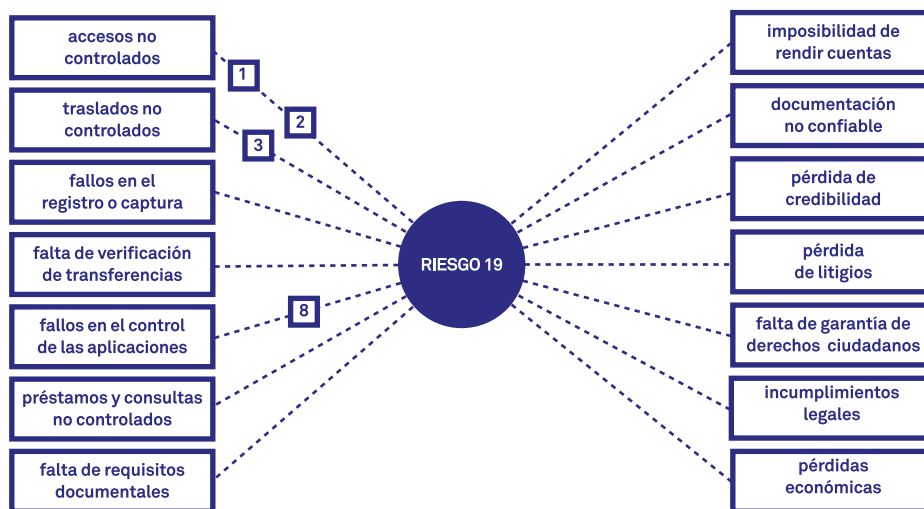


Figura 70 - Análisis de pajarita para el riesgo 19 (elaboración propia).

El riesgo 19 se ve afectado por 7 causas (a la izquierda de la pajarita) y puede tener afectación en 7 tipos de consecuencias distintos (a la derecha de la pajarita). Para evitar que el riesgo ocurra, en la organización existen 4 controles preventivos.

Riesgo 20 – Errores en la descripción documental

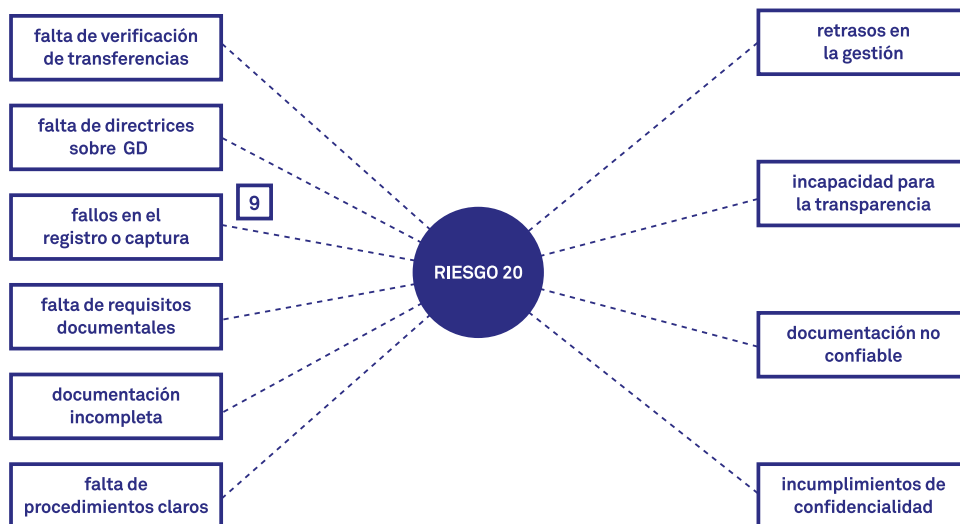


Figura 71 - Análisis de pajarita para el riesgo 20 (elaboración propia).

El riesgo 20 se ve afectado por 6 causas (a la izquierda de la pajarita) y puede tener afectación en 4 tipos de consecuencias distintos (a la derecha de la pajarita). Para evitar que el riesgo ocurra, en la organización existe un control preventivo.

Riesgo 21 – Desarrollo no controlado de aplicaciones

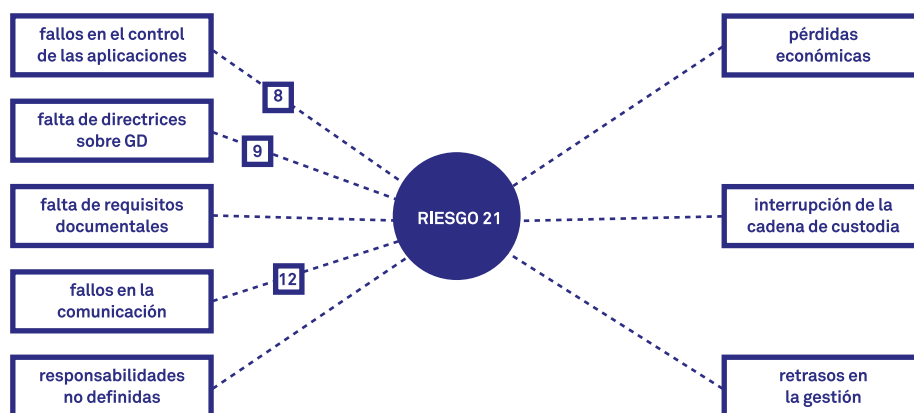


Figura 72 - Análisis de pajarita para el riesgo 21 (elaboración propia).

El riesgo 21 se ve afectado por 5 causas (a la izquierda de la pajarita) y puede tener afectación en 3 tipos de consecuencias distintos (a la derecha de la pajarita). Para evitar que el riesgo ocurra, en la organización existen 3 controles preventivos.

Riesgo 22 – Falta de interoperabilidad

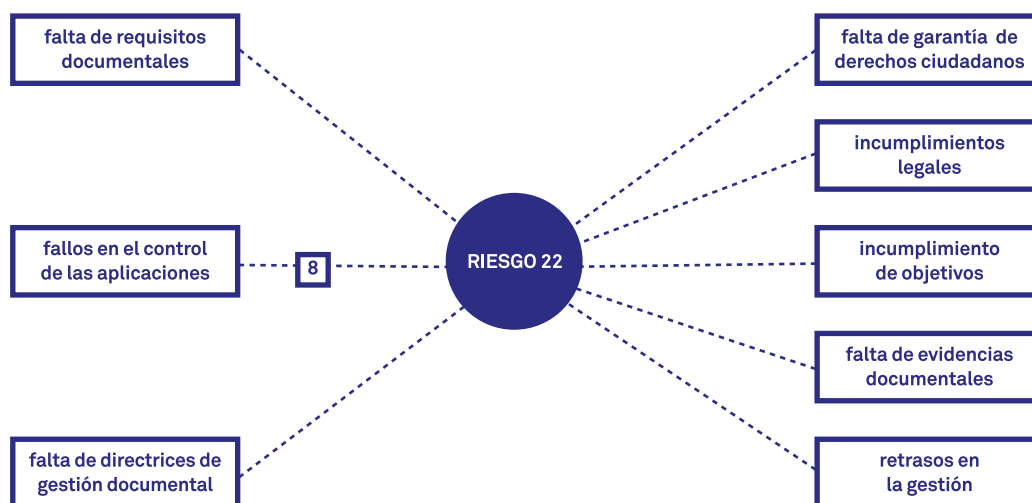


Figura 73 - Análisis de pajarita para el riesgo 22. (elaboración propia).

El riesgo 22 se ve afectado por 3 causas (a la izquierda de la pajarita) y puede tener afectación en 5 tipos de consecuencias distintos (a la derecha de la pajarita). Para evitar que el riesgo ocurra, en la organización existe un control preventivo.

Riesgo 23 – Falta de respuesta ante fallos del sistema

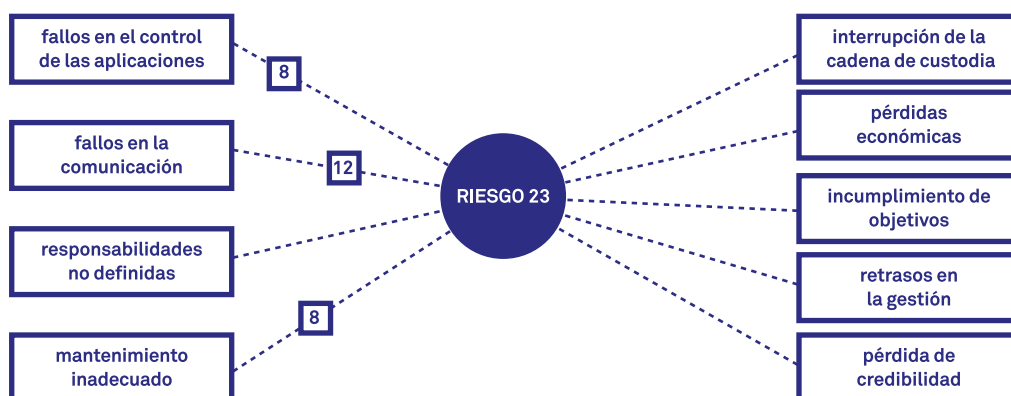


Figura 74 - Análisis de pajarita para el riesgo 23 (elaboración propia).

El riesgo 23 se ve afectado por 4 causas (a la izquierda de la pajarita) y puede tener afectación en 5 tipos de consecuencias distintos (a la derecha de la pajarita). Para evitar que el riesgo ocurra, en la organización existen 3 controles preventivos.

Riesgo 24 – Infraestructura insuficiente

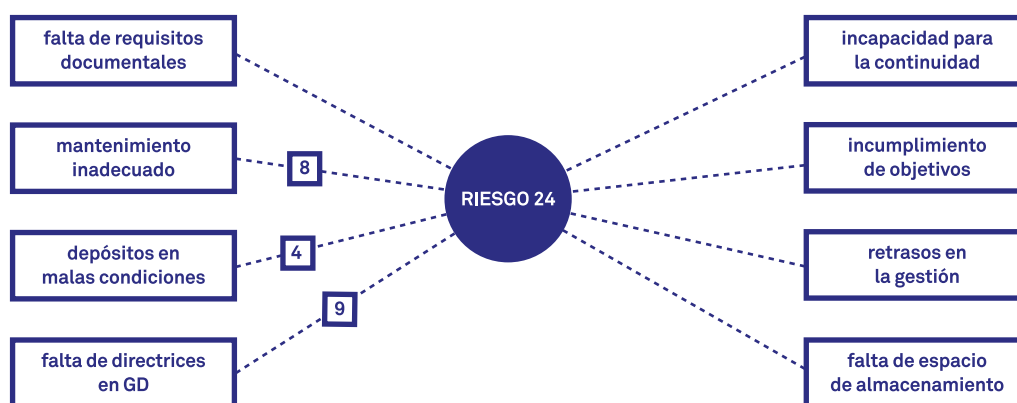


Figura 75 - Análisis de pajarita para el riesgo 24 (elaboración propia).

El riesgo 24 se ve afectado por 4 causas (a la izquierda de la pajarita) y puede tener afectación en 4 tipos de consecuencias distintos (a la derecha de la pajarita). Para evitar que el riesgo ocurra, en la organización existen 3 controles preventivos.

Riesgo 25 – Interrupción de la actividad

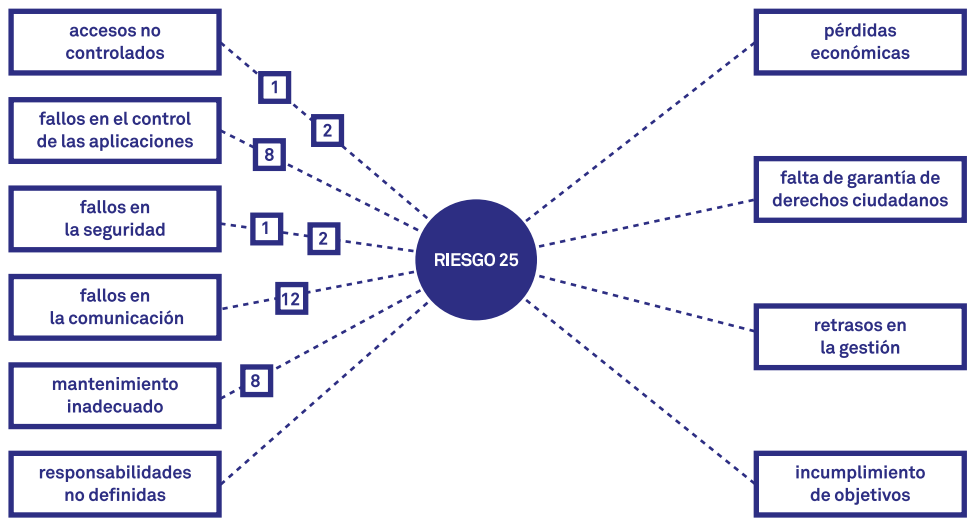


Figura 76 - Análisis de pajarita para el riesgo 25 (elaboración propia).

El riesgo 25 se ve afectado por 6 causas (a la izquierda de la pajarita) y puede tener afectación en 4 tipos de consecuencias distintos (a la derecha de la pajarita). Para evitar que el riesgo ocurra, en la organización existen 7 controles preventivos.

Riesgo 26 - Accesos indebidos a las aplicaciones

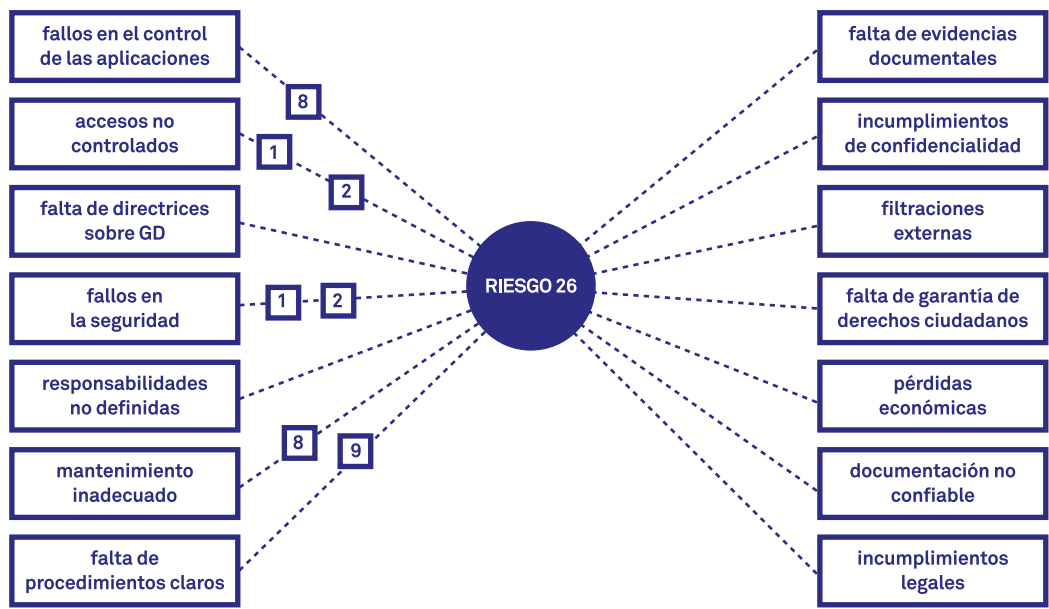


Figura 77 - Análisis de pajarita para el riesgo 26 (elaboración propia).

El riesgo 26 se ve afectado por 7 causas (a la izquierda de la pajarita) y puede tener afectación en 7 tipos de consecuencias distintos (a la derecha de la pajarita). Para evitar que el riesgo ocurra, en la organización existen 7 controles preventivos.

Riesgo 27 – Incapacidad para acceder a las aplicaciones

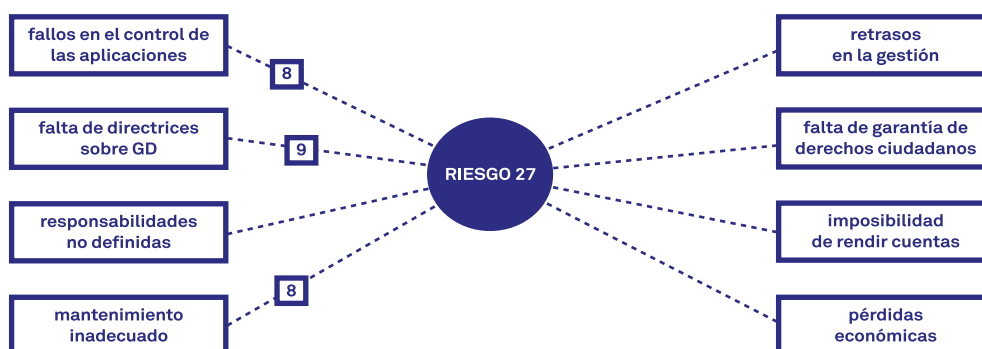


Figura 78 - Análisis de pajarita para el riesgo 27 (elaboración propia).

El riesgo 27 se ve afectado por 4 causas (a la izquierda de la pajarita) y puede tener afectación en 4 tipos de consecuencias distintos (a la derecha de la pajarita). Para evitar que el riesgo ocurra, en la organización existen 3 controles preventivos.

El análisis de los riesgos mediante la técnica de la pajarita permite recopilar las causas principales que en la Organización X pueden acabar desencadenando un riesgo documental. Es fundamental analizar este listado con el objetivo de identificar qué causas aparecen con mayor frecuencia para, de este modo, centrar los esfuerzos de prevención.

Listado general de consecuencias identificadas

NÚM.	CAUSAS
1CA	Accesos no controlados: falta de control y supervisión sobre el acceso a la información, sea en papel o electrónica.
2CA	Traslados no controlados: falta de control y supervisión del traslado interno de documentos en la organización, sea dentro de un mismo edificio o entre edificios distintos de la misma corporación.
3CA	Depósitos en malas condiciones: espacios en los que se conserva documentación que no disponen de las condiciones adecuadas de temperatura, humedad y mobiliario.
4CA	Errores en la clasificación: asignación de un código erróneo de clasificación a los documentos o falta de clasificación.
5CA	Falta de políticas de preservación: inexistencia de directrices y objetivos definidos sobre preservación de documentos a medio y largo plazo.
6CA	Eliminaciones no controladas/autorizadas: destrucción documental que no sigue el procedimiento ni los plazos definidos.
7CA	Fallos en el control de las aplicaciones: falta de seguimiento y verificación de las herramientas tecnológicas que ayudan a la gestión de documentos.

NÚM.	CAUSAS
8CA	Documentación incompleta: documentos y/o expedientes que no disponen de toda la información necesaria para la tramitación. Puede ser un documento sin la información o los datos completos, o un expediente sin todos los documentos necesarios para su tramitación.
9CA	Préstamos y consultas no controlados: procedimientos de acceso, consulta y préstamo de expedientes que no son supervisados y de los que no puede garantizarse su correcta realización.
10CA	Falta de verificación de transferencias: transferencias de documentos en las que se verifican la clasificación y la descripción, pero no se verifica si esto coincide con los documentos que se transfieren de las unidades productoras al archivo.
11CA	Falta de directrices sobre gestión documental: desarrollo incompleto de los instrumentos necesarios para una correcta gestión documental en la organización.
12CA	Fallos en el registro o captura: errores a la hora de realizar los procesos de registro y/o captura de documentos que se reciben o se envían por la organización.
13CA	Fallos en la seguridad: errores y falta de control en la seguridad, tanto física como electrónica, de los documentos y la información.
14CA	Falta de requisitos documentales: falta de definición de los requisitos necesarios para la gestión de los documentos a lo largo del ciclo de vida documental.
15CA	Fallos en la comunicación: errores en los canales de comunicación en cuanto a aspectos relacionados con la gestión de documentos.
16CA	Responsabilidades no definidas: falta de designación de responsables y de delimitación de responsabilidades sobre gestión documental en los distintos niveles de la organización.
17CA	Falta de procedimientos claros: definición incompleta o inexistente de procedimientos de gestión documental.
18CA	Mantenimiento inadecuado de las aplicaciones: fallos en el control y supervisión de las aplicaciones que gestionan documentos y que conllevan una mala gestión de las mismas.
19CA	Inexistencia de Tabla de documentos esenciales
20CA	Inexistencia del Catálogo de procedimientos

Figura 79 - Listado general de causas identificadas (elaboración propia).

No todas las causas aparecen con la misma frecuencia al realizar el análisis, sino que algunas tienen una mayor recurrencia que otras, tal y como se aprecia en la siguiente figura (ver Figura 80).

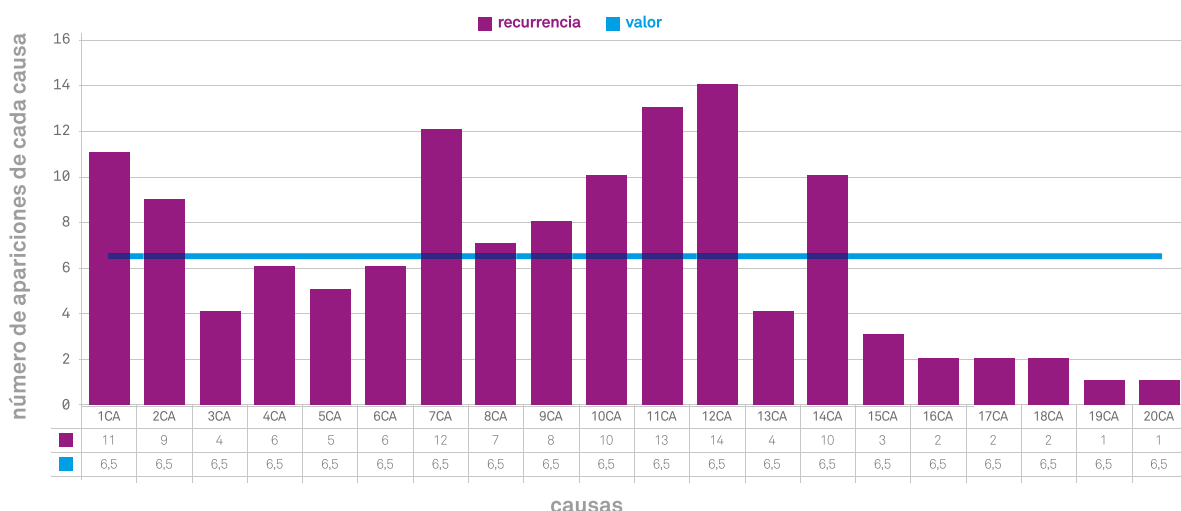


Figura 80 - Recurrencia de las causas identificadas, con valor medio (elaboración propia).

Se detectan algunas causas con un índice de aparición muy superior a otras, como es el caso de la 7CA, 11CA y 12CA con una recurrencia superior a 12. En cambio, las causas 19CA y 20CA aparecen tan solo en una ocasión. Resulta fundamental conocer la recurrencia en la aparición de las causas al analizar los riesgos de manera global, puesto que, de este modo, se dispone de información cuantitativa sobre cada causa, independientemente del riesgo que se pueda ver afectado.

La aparición recurrente de una causa en el análisis global resulta muy útil en la medida en que se puede priorizar la actuación sobre aquellas causas que se repitan de manera constante. De este modo, al minimizar, o incluso eliminar la causa, la afectación de esa acción concreta sobre el análisis global puede ser mayor, puesto que tiene repercusión sobre un número mayor de riesgos que si se actúa sobre una causa con menor recurrencia.

Para establecer la prioridad de actuación de manera objetiva se puede partir del valor medio de recurrencia, que para este caso concreto es de 6,5.

Por tanto, en el análisis no solo se deben tener en cuenta probabilidades y consecuencias, sino que resulta de suma importancia conocer y analizar las causas, para poder priorizar las acciones de tratamiento en la siguiente fase.

Lo mismo ocurre con las consecuencias que aparecen al analizar los riesgos mediante la técnica de la pajarita. Se presenta a continuación un listado de las mismas, con las explicaciones de cada una.

Listado general de consecuencias identificadas

NÚM.	CONSECUENCIAS
1CO	Pérdida de litigios: derivada de una falta de documentos probatorios.
2CO	Pérdida de credibilidad: percepción negativa de los usuarios externos e internos (ciudadanos y trabajadores) de la organización.
3CO	Falta de garantía de derechos ciudadanos: incumplimiento con las obligaciones de la organización de garantizar derechos a sus usuarios externos (ciudadanos).
4CO	Imposibilidad de rendir cuentas: incumplimiento de los procesos de rendición de cuentas, por no disponer o no ser capaz de localizar la información y documentación en el momento en que se necesita.
5CO	Incapacidad para la transparencia: imposibilidad de cumplir con las obligaciones de transparencia por no disponer o no ser capaz de localizar la información y documentos necesarios.
6CO	Pérdidas económicas: inversión de recursos humanos y económicos en la localización de información y documentación, que con un control adecuado de los documentos no sería necesaria.
7CO	Incumplimientos legales: incapacidad de cumplir con la legislación vigente por una mala gestión de la información y los documentos.
8CO	Incumplimiento de objetivos: incapacidad de cumplir con los objetivos fijados por una mala gestión de la información y los documentos.
9CO	Falta de evidencias documentales: no disponer de documentos probatorios cuando son necesarios.
10CO	Incumplimientos de confidencialidad: falta de garantías de confidencialidad de datos personales.
11CO	Filtraciones externas: fuga de información y documentación confidencial.
12CO	Interrupción de la cadena de custodia: incapacidad para garantizar la cadena de custodia de la información y la documentación.
13CO	Falta de espacio de almacenamiento: problemas en la conservación de documentos, ya sea en papel o en electrónico, por falta de capacidad en los depósitos o repositorios.
14CO	Ruido documental: búsquedas de información que dan resultados poco exactos.
15CO	Retrasos en la gestión: incapacidad de continuar con la tramitación en los plazos establecidos.
16CO	Pérdida de memoria corporativa: incapacidad de recuperar o conservar documentos sobre la historia y evolución de la organización a lo largo del tiempo.
17CO	Documentación no confiable: evidencias documentales de las que no se puede garantizar su fiabilidad, autenticidad o integridad.
18CO	Incapacidad para la continuidad de negocio: falta de capacidad de la organización para continuar con su actividad normal.

Figura 81 - Listado general de consecuencias identificadas (elaboración propia).

Analizando el número de apariciones de cada consecuencia se puede realizar un análisis más exhaustivo de las situaciones a las que puede enfrentarse la organización en caso de que algún riesgo suceda. En la Figura 82 se aprecia la recurrencia de las consecuencias identificadas, de manera global.

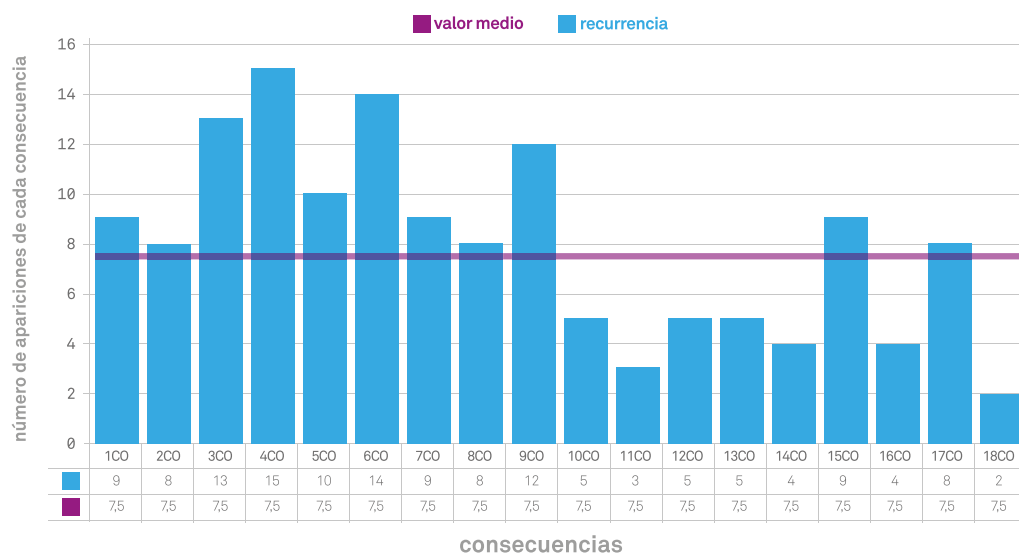


Figura 82 - Recurrencia de las consecuencias identificadas, con valor medio (elaboración propia).

Al analizar de manera global las posibles consecuencias relacionadas con cada riesgo, se aprecia que algunas aparecen con mayor frecuencia que otras. Es el caso de las consecuencias 3CO, 4CO, 6CO y 9CO, con valores superiores a 12. En cambio, la 11CO y la 18CO tienen valores de 3 y 2 respectivamente, siendo el contraste importante. Este análisis global tiene el objetivo de visualizar qué efectos negativos pueden ocurrir con mayor probabilidad, partiendo de la idea de que, a mayor recurrencia, mayor es la posibilidad de que llegue a ocurrir, ya sea debido a un riesgo u otro.

Del mismo modo que en el análisis global de causas, en este caso puede utilizarse el valor medio, de 7,5, como el valor mínimo frente al que priorizar las acciones correctivas relacionadas con los riesgos.

Conclusiones

Una de las conclusiones principales es la demostración de la práctica inexistencia de controles correctivos para evitar las consecuencias de un riesgo, habiendo identificado tan solo uno con relación a la conservación física de documentos. En los análisis de pajarita se puede observar claramente que existe una serie de controles preventivos que actúan de barrera entre las causas y el riesgo. Sin embargo, se observa que no pasa lo mismo entre el riesgo y las consecuencias derivadas. Esta situación se considera negativa en tanto en cuanto no se dispone de ninguna previsión para el momento en que el riesgo ocurra.

También se observa que los responsables de la gestión de documentos en la organización no son conscientes de disponer de medidas preventivas para evitar o minimizar las causas de que los riesgos ocurran. En cambio, sí disponen de algunas “barreras”, enumeradas anteriormente en este apartado, para evitar o frenar las causas que pueden ocasionar situaciones de riesgo. Con una mayor concienciación en este aspecto, seguramente se pueden conseguir unos mejores resultados de prevención, incluso sin una gran inversión de tiempo y personal.

Del análisis global de causas, se deduce que hay algunas más presentes en el día a día de la organización que otras. La más importante, duplicando el valor medio de recurrencia, se relaciona directamente con una de las responsabilidades del área de gestión documental y archivo, ya que se trata de la indefinición de los requisitos que se deben cumplir con relación a los documentos y a su gestión. Como solución, se puede partir de los requisitos establecidos en estándares internacionales para, de este modo, ahorrar tiempo y recursos. La definición de requisitos documentales mejoraría enormemente la gestión de documentos en la organización a medio y largo plazo.

Del análisis global de consecuencias que pueden suceder, la más recurrente es la imposibilidad de rendir cuentas por la organización. Este resultado es muy importante en una actualidad que se rige por una mayor transparencia y acceso a la información y por una mayor fiscalización de las decisiones y actuaciones de las administraciones públicas. Se hace evidente que la Organización X es muy vulnerable a las incidencias en procesos de rendición de cuentas.

Se considera fundamental poder aprovechar los resultados del análisis de causas y consecuencias en la decisión sobre las acciones de tratamiento de los riesgos, en la medida en que la actuación sobre las causas y la voluntad de prevención de las consecuencias, pueden contribuir a una orientación e incidencia más ajustadas de las acciones de tratamiento.

5.3.3 Evaluación de riesgos

La finalidad de la evaluación es ayudar a la toma de decisiones, determinando los riesgos a tratar y la prioridad para implementar el tratamiento, siempre partiendo de los resultados del análisis del riesgo. Evitar todos los riesgos es tanto imposible como improductivo (Lemieux 2004a, p. 20) y es por ello que la evaluación resulta una pieza clave

en la prevención. Para llevar a cabo el proceso de evaluación se emplea la técnica de los índices de riesgo, que se complementa con los resultados obtenidos en la fase de análisis. Se explica a continuación.

Índices de riesgo

Un índice de riesgo es una medición del riesgo semicuantitativa que consiste en una estimación que se obtiene al utilizar un tanteo usando escalas ordinales (AENOR 2011a, p. 90). Esta técnica se puede utilizar para la clasificación de diferentes riesgos asociados con una actividad, como es el caso de este estudio. Permite la integración de un rango de factores que afectan al nivel de riesgo en una única puntuación numérica para dicho nivel.

Las entradas se derivan del análisis de la organización o de un conocimiento amplio del contexto. Para el caso de la Organización X, se parte del conocimiento adquirido tanto del contexto interno como del externo y se emplean los resultados y la información obtenidos en las primeras fases del proceso de gestión del riesgo.

La evaluación comienza por comprender y describir el sistema, tal y como se hizo en la fase de análisis del contexto. Con este conocimiento, se debe desarrollar la calificación o puntuación para cada componente de modo que se puedan combinar para proporcionar un índice compuesto. Las calificaciones o puntuaciones se pueden dar para componentes del riesgo (por ejemplo: probabilidad, exposición, consecuencia) o para factores que aumentan o disminuyen el riesgo. Para este estudio de caso se seleccionan los siguientes componentes:

- A. Número de causas, obtenido a partir del análisis de pajarita.
- B. Número de consecuencias, obtenido a partir del análisis de pajarita.
- C. Número de procesos relacionados, obtenido a partir de las fichas de riesgos (ver el apartado *Documentación del proceso*).
- D. Número de riesgos relacionados, obtenido a partir de las fichas de riesgos.

Los valores individuales de cada parámetro se combinan para obtener una puntuación final de cada riesgo, con la finalidad de servir de base para la toma de decisiones.

Las fortalezas de esta técnica incluyen (AENOR 2011a, p. 91):

- Los índices pueden proporcionar una buena herramienta para clasificar riesgos diferentes.
- Permiten incorporar múltiples factores que afectan al nivel de riesgo en una única clasificación numérica para el nivel de riesgo.

Las debilidades incluyen (AENOR 2011a, p. 91):

- Si el proceso y su resultado no son validados correctamente, los resultados pueden carecer de significado. El hecho de que el resultado sea un valor numérico para el riesgo puede ser mal interpretado, por ejemplo, en posteriores análisis de coste y beneficio.

- En muchas situaciones en que se utilizan índices no existe un modelo fundamental para definir si las escalas individuales de factores de riesgo son lineales, logarítmicas o de alguna otra forma, y ningún modelo define cómo deberían combinarse los factores. En estas situaciones, la clasificación es poco fiable.

Para realizar los cálculos necesarios para la evaluación de riesgos, en primer lugar, se realiza una recopilación de los datos para los parámetros seleccionados. En este paso, con relación al número de causas se considera importante poder incluir la influencia de las acciones preventivas existentes, ya que estas permiten disminuir o prevenir la causa. Para poder calcular esta influencia, se emplea la siguiente fórmula, donde VCA corresponde al Valor final de la Causa:

$$VCA = \left(1 - \left(\frac{np}{3}\right)^2\right) + 0,02$$

El valor final de cada causa (VCA) se calcula a partir del valor 1, que es el valor que se asigna por defecto a cada causa. A este valor se le debe restar la influencia o afectación de las acciones preventivas existentes (np). Previamente, por tanto, es necesario calcular el valor de esta afectación.

Para ello, se parte de la hipótesis de que, para la Organización X, disponer de tres acciones preventivas asociadas a una misma causa puede llegar prácticamente a eliminar la causa. La reducción del valor de la causa se vería afectada de manera exponencial. Es decir, a más acciones de prevención existentes, mayor disminución del valor de la causa.

Por último, en la fórmula se incluye un valor de corrección (+0,02) ya que, si bien es cierto que las acciones preventivas pueden disminuir las causas de manera significativa, siempre existirá el factor humano, que puede llevar al error pese a una prevención controlada.

De este modo, se puede calcular el valor de las causas frente al número total de causas (ver Figura 83).

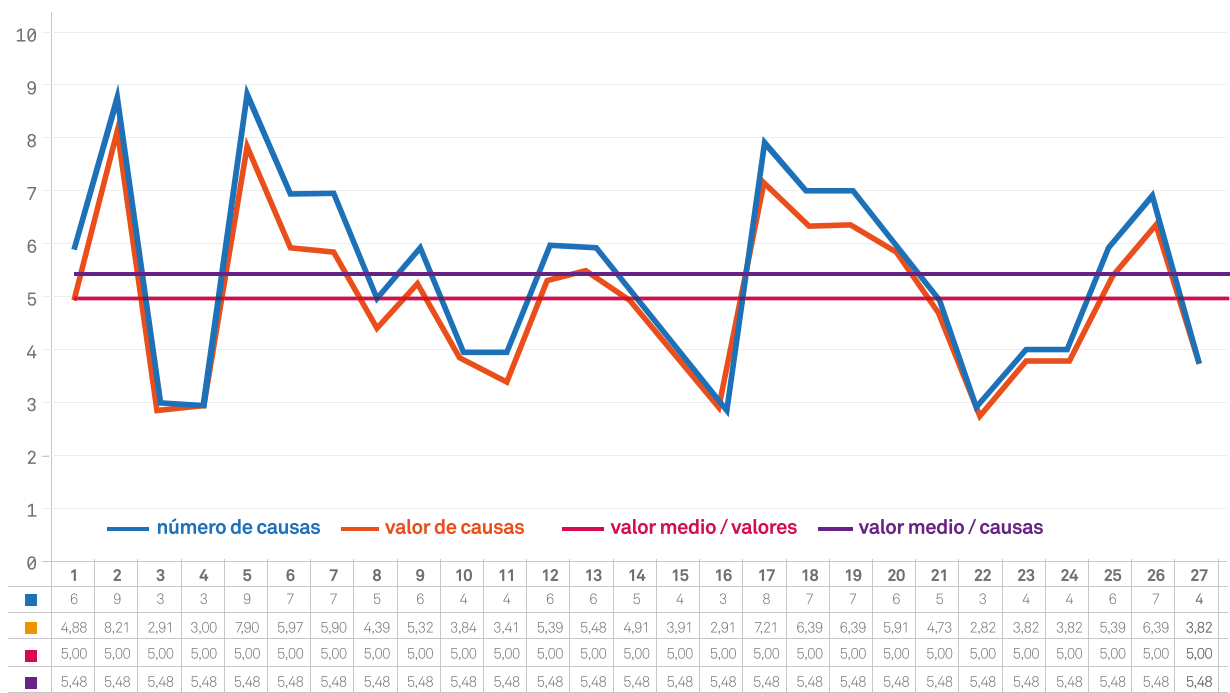


Figura 83 - Comparación entre el número y el valor de las causas (elaboración propia).

En la Figura 83 se refleja en color azul el número total de causas que afectan a cada riesgo y en color naranja el valor de dichas causas, a partir del cálculo explicado anteriormente. Puede apreciarse una ligera desviación entre ambos valores, siendo la mayoría de veces superior el número de causas que su valor. Esto es así, debido a la disminución del valor a través de las medidas preventivas existentes. Además, es importante la observación de los valores medios de ambos parámetros, donde se aprecia claramente una diferencia de casi medio punto entre el número y el valor.

Se considera más realista el cálculo en función del valor ya que tiene en cuenta más parámetros y, por tanto, el resultado es más ajustado al contexto de la Organización X. Se puede apreciar que no en todos los casos influye del mismo modo, ya que depende completamente de la existencia y del número de medidas preventivas. Son un ejemplo los riesgos 4, 16 y 22, que tienen 3 causas asociadas cada uno. Pese a ello, en el caso del riesgo 4, el número y el valor de causa es el mismo, manteniéndose en 3. En el riesgo 16, disminuye a 2,91 debido a la existencia de 1 acción preventiva. En el riesgo 22, disminuye a 2,82, puesto que, en este, caso son 2 las acciones preventivas que frenan las causas. Por tanto, a mayor prevención, menor es el valor de las causas para la evaluación.

Con relación al número de consecuencias se considera igualmente importante poder incluir la influencia de las acciones correctivas existentes en el valor, ya que estas permiten modificar la consecuencia. Para poder calcular esta influencia, se emplea la misma fórmula que para las causas, pero en este caso teniendo en cuenta el número de acciones correctivas existentes, donde *VCO* corresponde al Valor final de la consecuencia:

$$VCO = \left(1 - \left(\frac{nc}{3}\right)^2\right) + 0,02$$

El valor final de cada consecuencia (*VCO*) se calcula a partir del valor 1, que es el valor que se asigna por defecto a cada consecuencia. A este valor se le debe restar la influencia o afectación de las acciones correctivas existentes (*nc*). Previamente, por tanto, es necesario calcular el valor de esta afectación.

Para ello, se parte de la hipótesis de que, para la Organización X, disponer de tres acciones correctivas asociadas a una misma consecuencia puede llegar prácticamente a eliminar la afectación de dicha consecuencia. La reducción del valor de la consecuencia se vería afectada de manera exponencial. Es decir, a más acciones de corrección existentes, mayor disminución del valor de la consecuencia.

Por último, en la fórmula se incluye también un valor de corrección (+0,02) ya que, si bien es cierto que las acciones correctivas pueden disminuir las consecuencias de manera significativa, siempre existirá el factor humano, que puede llevar al error pese a una acción de corrección controlada.

De este modo, se puede calcular el valor de las consecuencias frente al número total de consecuencias (ver Figura 84).

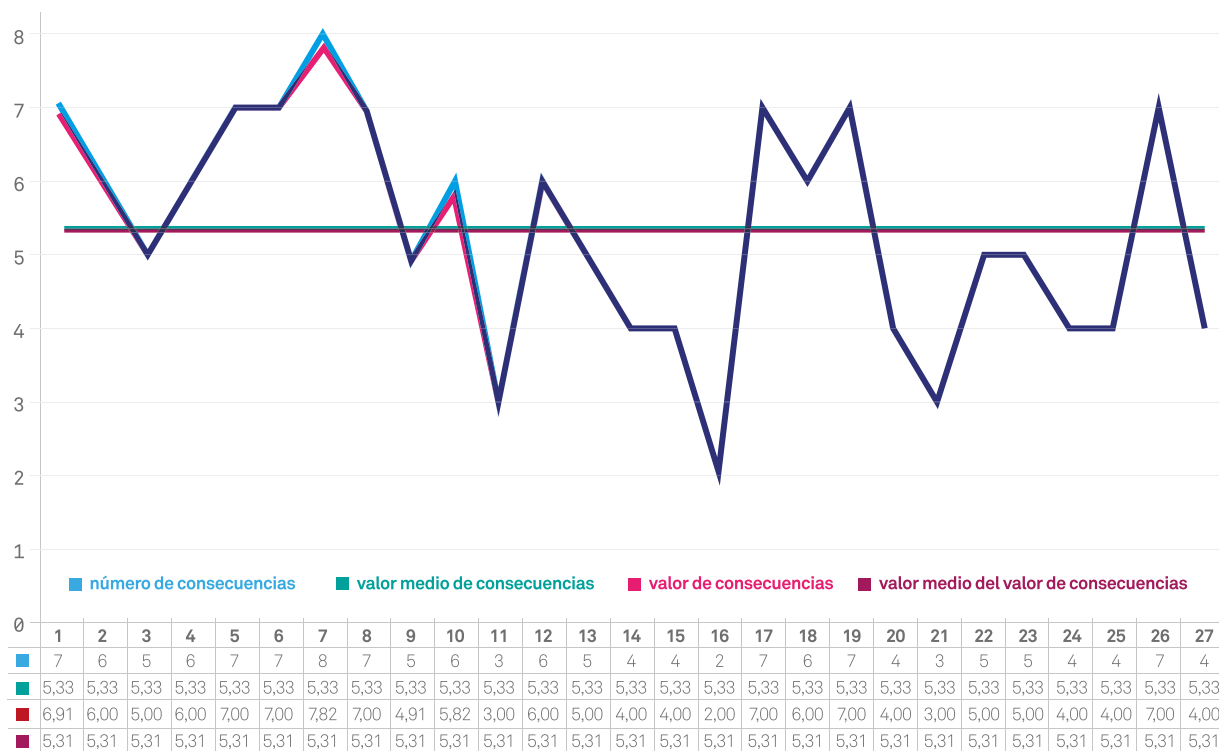


Figura 84 - Comparación entre el número y el valor de las consecuencias (elaboración propia).

A diferencia de lo sucedido con el valor de las causas, en el caso de las consecuencias los resultados obtenidos son casi coincidentes entre el número y el valor de consecuencias. Esto es así debido a la existencia mínima de controles correctivos, que tan solo actúan en algunos casos para evitar las consecuencias. Estos casos son los riesgos 1, 7, 9 y 10. Se aprecia una mayor desviación (de 0,18 puntos) en los riesgos 7 y 10 debido a que existen dos controles correctivos en ambos.

Lo más destacado del cálculo del valor de las consecuencias es la obtención de resultados coincidentes en el 85,19 % de los riesgos. De este modo, se evidencia la falta de controles correctivos en la Organización X, que pueden ayudar a reducir la afectación de las consecuencias.

Una vez calculado el valor de las causas y las consecuencias, se procede a la evaluación de los riesgos a partir de los parámetros antes mencionados y siguiendo la técnica de los índices de riesgo. Para ello, se sustituyen los parámetros del número de causas y del número de consecuencias por el valor de las causas y el valor de las consecuencias, quedando de la siguiente forma:

- A. Valor de causas, obtenido a partir del número de causas y el número de acciones preventivas existentes, a partir del análisis de pajarita.

- B. Valor de consecuencias, obtenido del número de consecuencias y el número de acciones correctivas existentes, a partir del análisis de pajarita.
- C. Número de procesos relacionados, obtenido a partir de las fichas de riesgos.
- D. Número de riesgos relacionados, obtenido a partir de las fichas de riesgos.

La evaluación se calcula a través de la siguiente fórmula, donde VR equivale al Valor del riesgo (ver Figura 85).

$$VR = \frac{(A + B + C + D)}{4}$$

La evaluación de riesgos debe resultar útil para la priorización de acciones de prevención y tratamiento. En la Figura 85 se aprecia que casi la mitad de los riesgos se encuentran por encima del valor medio, concretamente el 48,14 %.

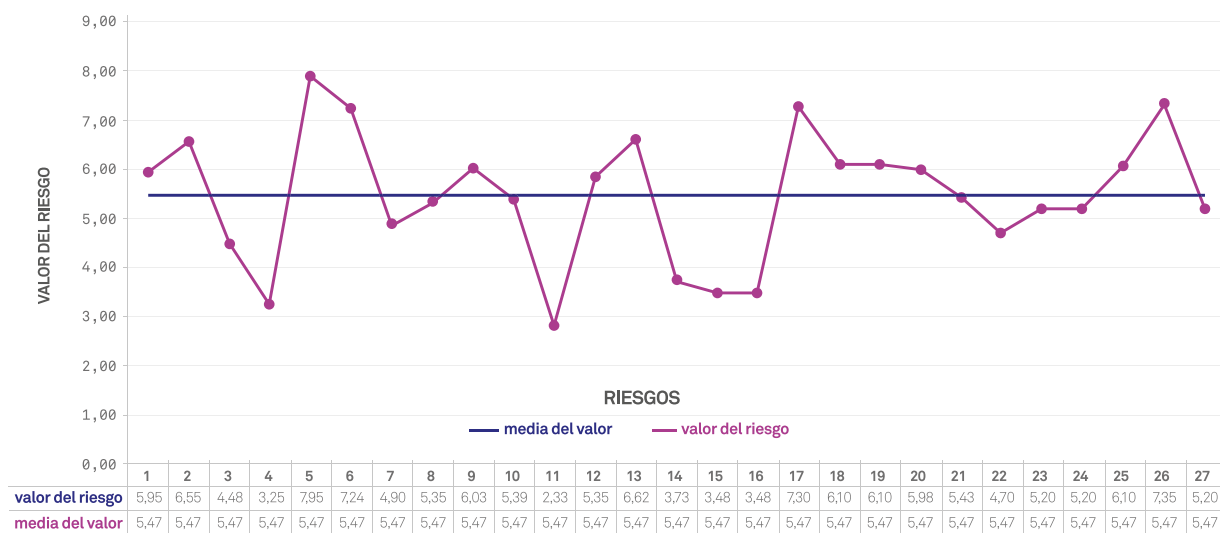


Figura 85 - Comparación entre el número y el valor de las consecuencias (elaboración propia).

Si se sitúa el nivel de tolerancia al riesgo en el valor medio, los resultados obtenidos indican que existe una necesidad importante de llevar a cabo acciones de tratamiento de riesgos en la Organización X. Estas acciones deben priorizar aquellos riesgos que se sitúan por encima del valor medio, de 5,47 puntos, en la Figura 85. Son los siguientes: 1, 2, 5, 6, 9, 12, 13, 17, 18, 19, 20, 25 y 26.

- . 1 – Pérdida de información/documentación
- . 2 – Falta de garantías de integridad
- . 5 – No recuperación de información/documentación
- . 6 – Accesos indebidos a información
- . 9 – Falta de garantías de accesibilidad
- . 12 – Ubicación errónea o indebida de documentos
- . 13 – Manipulación no autorizada de documentos
- . 17 – Falta de garantías de trazabilidad
- . 18 – Falta de garantías de autenticidad
- . 19 – Falta de garantías de fiabilidad
- . 20 – Errores en la descripción documental
- . 25 – Interrupción de la actividad
- . 26 – Accesos indebidos a las aplicaciones

Dentro de este listado de riesgos prioritarios, se tiene también en cuenta que los riesgos 5, 6, 17 y 26 son los únicos que se sitúan por encima del valor de 7 y, por tanto, debe darse mayor prioridad a su tratamiento y prevención.

Sin embargo, cabe recordar que no por el hecho de decidir priorizar unos riesgos sobre otros, se debe olvidar el tratamiento sobre aquellos con menor valor de evaluación. Lo que sí es importante para la Organización X es poder definir un plan de actuación a medida de sus necesidades, y, por este motivo, los resultados de la evaluación resultan tan importantes.

Para la priorización, la Organización X tiene establecidos unos criterios en función del valor del riesgo (ver Figura 86). Estos valores se basan en el análisis de riesgos definido por la organización, que se basa en tres grados de probabilidad y tres grados de consecuencia, que dan como resultado cinco niveles de riesgo. El tipo de riesgo (nivel), para la Organización X tiene una correspondencia con una escala de prioridad y con un plazo para implementar actuaciones o acciones de tratamiento y prevención.

PRIORIDAD	TIPO DE RIESGO (NIVEL)	ACTUACIÓN
1	Riesgo intolerable	Inmediata
2	Riesgo importante	A corto plazo (< 3 meses)
3	Riesgo moderado	A medio plazo (< 6 meses)
4	Riesgo tolerable	A largo plazo (< 1 año)
5	Riesgo trivial	Solo control u otro plazo definido

Figura 86 - Valor y prioridad del riesgo definidos por la Organización X.

Por su parte, en el estudio de caso se desarrolla una tabla muy similar pero basada en cinco grados de probabilidad y cinco grados de consecuencia o severidad, lo que da como resultado una mayor diversificación en la prioridad (ver Figura 87).

VALOR DEL RIESGO	PRIORIDAD DE ACTUACIÓN	CÓDIGO DE PRIORIDAD
0 a 0,99	nula	A
1 a 1,99	extremadamente baja	B
2 a 2,99	muy baja	C
3 a 3,99	baja	D
4 a 4,99	media	E
5 a 5,99	alta	F
6 a 6,99	muy alta	G
7 a 7,99	extremadamente alta	H
8 a 8,99	urgente	I

Figura 87 - Correspondencia entre los valores de riesgo y la prioridad de tratamiento (elaboración propia).

A partir de la Figura 87, se considera necesario realizar una correlación ente los valores fijados por la Organización X y los fijados para el estudio de caso. La correlación se establece de la siguiente manera (ver Figura 88):

PRIORIDAD DEL ESTUDIO DE CASO	PRIORIDAD ORGANIZACIÓN X	TIPO DE RIESGO ORGANIZACIÓN X	ACTUACIÓN ORGANIZACIÓN X
A	5	Trivial	Control u otro plazo definido
B	5	Trivial	Control u otro plazo definido
C	4	Tolerable	A largo plazo (< 1 año)
D	4	Tolerable	A largo plazo (< 1 año)
E	3	Moderado	A medio plazo (< 6 meses)
F	3	Moderado	A medio plazo (< 6 meses)
G	2	Importante	A corto plazo (< 3 meses)
H	2	Importante	A corto plazo (< 3 meses)
I	1	Intolerable	Inmediata

Figura 88 - Correspondencia entre la prioridad definida en el estudio de caso y la definida por la Organización X (elaboración propia).

Es interesante incluir esta información en estudio de caso, ya que contempla una periodización para la definición de las acciones de tratamiento o prevención para la organización, asociada al nivel de riesgo (“tipo de riesgo” según la Organización X). Esta información debe ser tenida en cuenta a la hora de establecer el calendario de actuaciones, tras la evaluación de riesgos, en la fase de tratamiento.

En la siguiente tabla se asigna a cada valor de riesgo, la prioridad de tratamiento asociada para el estudio de caso (ver Figura 89).

N.	RIESGO IDENTIFICADO	VALOR	PRIORIDAD	ACTUACIÓN
1	Pérdida de información/documentación	5,95	F / 3	< 6 meses
2	Falta de garantías de integridad	6,55	G / 2	< 3 meses
3	Pérdida de documentos esenciales	4,48	E / 3	< 6 meses
4	No creación de evidencias documentales	3,25	D / 4	< 1 año
5	No recuperación de información/documentación	7,95	H / 2	< 3 meses
6	Accesos indebidos a información	7,24	H / 2	< 3 meses
7	Eliminación indebida de documentos	4,90	E / 3	< 6 meses
8	Sustracción o robo de documentos	5,35	F / 3	< 6 meses
9	Falta de garantías de accesibilidad	6,03	G / 2	< 3 meses
10	Falta de garantías de usabilidad	5,39	F / 3	< 6 meses
11	No eliminación de documentos	2,83	C / 4	< 1 año
12	Ubicación errónea o indebida de documentos	5,85	F / 3	< 6 meses
13	Manipulación no autorizada de documentos	6,62	G / 2	< 3 meses
14	Duplicidad documental	3,73	D / 4	< 1 año
15	Creación innecesaria de documentos	3,48	D / 4	< 1 año
16	Duplicación de instrumentos de gestión documental	3,48	D / 4	< 1 año
17	Falta de garantías de trazabilidad	7,30	H / 2	< 3 meses
18	Falta de garantías de autenticidad	6,10	G / 2	< 3 meses
19	Falta de garantías de fiabilidad	6,10	G / 2	< 3 meses
20	Errores en la descripción documental	5,98	F / 3	< 6 meses
21	Desarrollo no controlado de aplicaciones	5,43	F / 3	< 6 meses
22	Falta de interoperabilidad	4,70	E / 3	< 6 meses
23	Falta de respuesta ante fallos del sistema	5,20	F / 3	< 6 meses
24	Infraestructura insuficiente	5,20	F / 3	< 6 meses
25	Interrupción de la actividad	6,10	G / 2	< 3 meses
26	Accesos indebidos a las aplicaciones	7,35	H / 2	< 3 meses
27	Incapacidad para acceder a las aplicaciones	5,20	F / 3	< 6 meses

Figura 89 - Evaluación de riesgos documentales de la Organización X (elaboración propia).

Para facilitar la gestión de riesgos en la Organización X se decide seguir los grados de prioridad y los plazos de actuación definidos en la misma (ver Figura 88 para las correlaciones) pese a que en la tabla se puede observar la inclusión de ambos grados de prioridad. Se decide incluirlos para facilitar la comprensión de la evaluación realizada en el estudio de caso y, a la vez, encajar los resultados obtenidos en la metodología existente en la organización.

A partir de los resultados obtenidos, se decide analizar la distribución de porcentajes según el valor del riesgo obtenido en la evaluación, tal como se había realizado previamente en el análisis con los niveles de riesgo (ver Figura 47 para los niveles de riesgo y Figura 85 para los valores de riesgo).

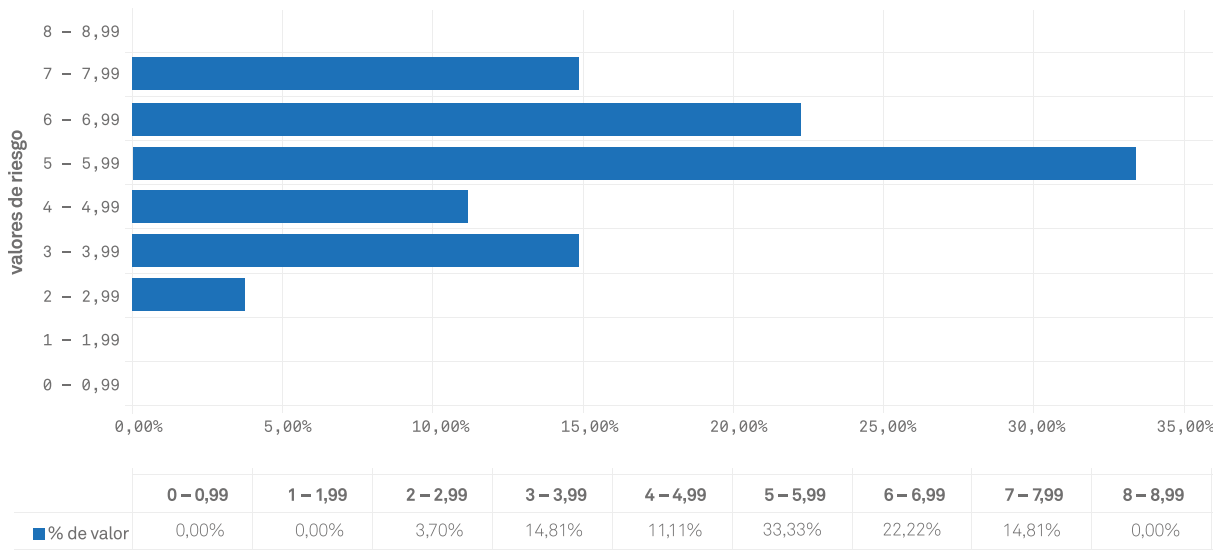


Figura 90 - Distribución de porcentajes según el valor del riesgo (elaboración propia).

Se observa (ver Figura 90) que gran parte de los riesgos, un 70,36 %, se sitúa entre valores de 5 y 7,99, mientras que los valores de 0 a 2,99 tan solo se corresponden con un 3,70 % de los riesgos identificados. Esto indica que la gran mayoría de los riesgos necesitan una prioridad media-alta de tratamiento.

Se comparan estos porcentajes con los obtenidos del análisis (ver Figura 91), con la finalidad, en primer lugar, de contrastar los resultados y, en segundo lugar, para obtener una visión global sobre el grado de prioridad que debe aplicarse a las acciones de tratamiento.

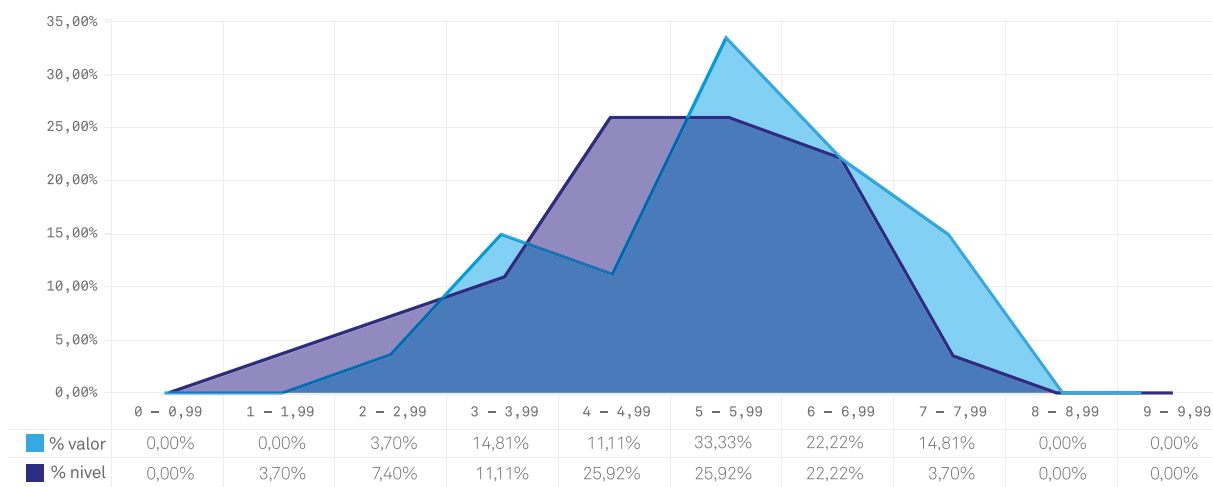


Figura 91 - Comparación de porcentajes entre niveles y valores del riesgo (elaboración propia).

Se aprecia claramente cómo, de forma mayoritaria, los resultados son coincidentes. En la Figura 91 se puede ver como los riesgos con menores y mayores niveles y valores son inferiores a los que tienen un valor o nivel medio. Estos resultados pueden dificultar las decisiones a la hora de priorizar el tratamiento, puesto que la mayoría de los riesgos se concentran en valores intermedios. Deben, por tanto, tenerse en cuenta otros criterios además de los valores y niveles, para justificar las acciones sobre unos riesgos antes que sobre otros. Para ello, se dispone de información sobre las causas y consecuencias asociadas, así como también medidas de prevención existentes, número de procesos relacionados y número de riesgos relacionados entre sí. Estos datos ayudarán, sin duda, en el proceso de toma de decisiones y en la justificación sobre la prioridad de tratamiento de la Organización X.

Junto con el análisis de estos datos, la definición del nivel de tolerancia para la priorización en el tratamiento de los riesgos es un factor importante. Se decide que el nivel de tolerancia se haga coincidir con la media del valor de los riesgos. Por tanto, todos los riesgos que se sitúen por encima de la media en la evaluación deben tener prioridad de actuación en el tratamiento.

Con la finalidad de ajustar el plan de actuación y tratamiento, se decide realizar también una comparación entre los resultados obtenidos de los procesos de análisis (nivel de riesgo) y de evaluación (valor de riesgo) (ver Figura 92).

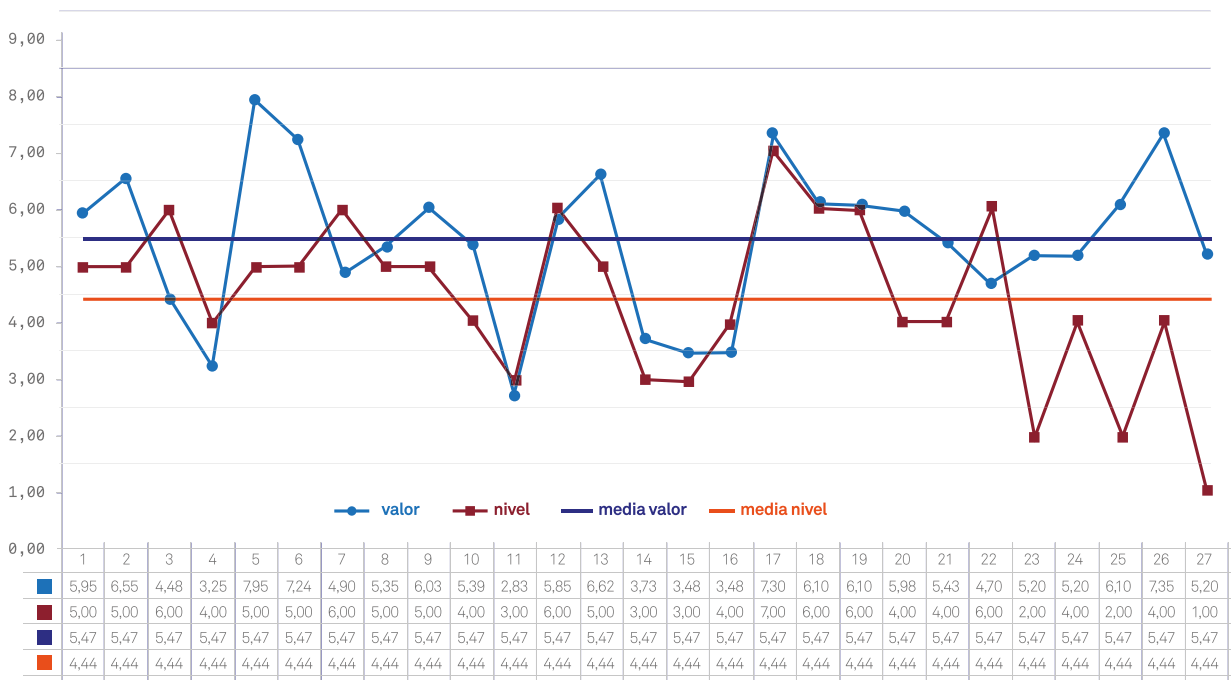


Figura 92 - Comparación entre valores y niveles del riesgo (elaboración propia).

En la Figura 92 se aprecia una comparativa entre los niveles obtenidos a partir del análisis de los riesgos (color granate), así como los valores obtenidos a partir de la evaluación (color azul). Si bien es cierto que existe cierta divergencia en algunos de los riesgos, se puede apreciar una gran coincidencia en aquellos que se sitúan por encima del valor medio o nivel de tolerancia definido.

La finalidad de realizar esta comparativa es poder ajustar la priorización en el tratamiento de los riesgos. Al realizar la misma operación a partir de los resultados obtenidos en el análisis (nivel de riesgo), se parte de una media (nivel de tolerancia) ligeramente inferior, de 4,44 puntos, a la de la evaluación, de 5,47 puntos. Los riesgos que se sitúan por encima de esta son: 1, 2, 3, 5, 6, 7, 8, 9, 12, 13, 17, 18, 19 y 22. De estos catorce, diez coinciden con los identificados a partir de la evaluación y enumerados anteriormente. Por tanto, un 71,42 % son coincidentes. Los cuatro que no se sitúan por encima de la media en la evaluación son: 3, 7, 8 y 22:

- 3 – Pérdida de documentos esenciales
- 7 – Eliminación indebida de documentos
- 8 – Sustracción o robo de documentos
- 22 – Falta de interoperabilidad

Puede estudiarse su inclusión en el plan de actuación, como prioritarios junto con los diez restantes.

En este gráfico comparativo se aprecia una diferencia destacable en los riesgos 23, 25, 26 y 27. El nivel y el valor no son coincidentes, sino más bien divergentes. Estos riesgos están directamente relacionados con aspectos informáticos. A la hora de realizar el análisis, la probabilidad de que ocurran es relativamente baja. En cambio, en la realización de la evaluación, al incluir factores que no se han tenido en cuenta en el análisis, como son por ejemplo el número de procesos afectados o el número de consecuencias, los resultados obtenidos varían notablemente. Esto es así porque, pese a que las probabilidades de que alguno de estos riesgos suceda son bajas, las consecuencias y la afectación en distintos procesos de gestión documental son superiores a otros riesgos.

Resultados

La técnica de los índices de riesgo resulta funcional y aporta resultados útiles para poder decidir sobre la priorización en el tratamiento de riesgos. Resulta muy interesante poder comparar los resultados de esta técnica con los de la técnica empleada en el análisis de riesgos. Complementando los datos obtenidos con ambos métodos se puede obtener información más precisa para la toma de decisiones, que revierte en una mejor prevención en la organización.

A partir de los datos obtenidos del resultado de la evaluación, la prioridad en el tratamiento de los riesgos debe seguir el siguiente orden:

Grupo 1: riesgos 5 y 17. Son los riesgos situados por encima del nivel de tolerancia en los resultados de la evaluación y que tienen el valor más alto de la evaluación realizada. Por este motivo se considera prioritario su tratamiento. Coinciden con un plazo de actuación inferior a 3 meses, según los plazos fijados por la Organización X en su procedimiento de gestión del riesgo. Debido a que su valor es muy elevado con relación a otros riesgos, se considera ajustar a inmediata la prioridad de actuación para ambos.

Grupo 2: riesgos 2, 6, 9, 13, 18, 19, 25 y 26. Son los riesgos que, independientemente de si están situados por enci-

ma o por debajo del nivel de tolerancia, tienen asignada una prioridad de 2. Esta prioridad implica que el plazo de actuación sobre estos riesgos debe ser inferior a 3 meses.

Grupo 3: riesgos 1, 3, 7, 8, 10, 12, 20, 21, 22, 23, 24 y 27. Son los riesgos que, independientemente de si están situados por encima o por debajo del nivel de tolerancia, tienen asignada una prioridad de 3. Según el criterio seguido, deben tratarse en un plazo inferior a 6 meses.

Grupo 4: riesgos 4, 11, 14, 15 y 16. Son los riesgos por debajo del nivel de tolerancia en la evaluación y que tienen una prioridad asignada, según los resultados de la evaluación, de 4. Implica que las actuaciones sobre estos riesgos deben implementarse en un plazo inferior a 1 año.

5.4 Fase 3. Propuesta para el tratamiento del riesgo

A partir de la información recopilada en los procesos de análisis y evaluación, deben decidirse y llevarse a cabo las acciones de tratamiento y prevención de los riesgos identificados. Además, el plan de tratamiento debe identificar de manera clara el orden de prioridad de las diferentes acciones que se quieren implementar en la Organización X para facilitar la disposición de los recursos y obtener unos mejores resultados.

Esta fase del estudio de caso no se ha llevado a la práctica, sino que es una propuesta entregada a la organización con el objetivo de que se decida a nivel interno cómo implementar las diferentes acciones de tratamiento que se proponen y sus responsables.

Metodología

El tratamiento del riesgo implica la selección y la implementación de una o varias opciones para modificar los riesgos. Estas opciones no se excluyen necesariamente unas a otras, ni son apropiadas en todas las circunstancias. Pueden incluir lo siguiente (AENOR 2010, p. 25):

1. Evitar el riesgo, decidiendo no iniciar o continuar con la actividad que causa el riesgo.
2. Aceptar o aumentar el riesgo a fin de perseguir una oportunidad.
3. Eliminar la fuente (causa) del riesgo.
4. Modificar la probabilidad.
5. Modificar las consecuencias.
6. Compartir el riesgo con otras partes (incluyendo los contratos y la financiación del riesgo).

7. Retener el riesgo basándose en una decisión informada.

De estas opciones de tratamiento, para el estudio de caso de la Organización X se pueden poner en práctica la 1, 3, 4, 5 y 6. Se descartan las opciones 2 y 7, puesto que no se consideran apropiadas para los objetivos perseguidos.

Dentro de estas opciones hay que encajar los tipos de acciones preventivas ya existentes y definidas en el procedimiento de gestión del riesgo de la Organización X, que están codificadas y se presentan a continuación (ver Figura 93). Cabe recordar que este procedimiento se realiza en el marco de la norma ISO 18001, que especifica los requisitos para un sistema de gestión de la Seguridad y Salud en el Trabajo, por lo que algunas de las acciones preventivas no resultan funcionales para el tratamiento de riesgos documentales. En la siguiente figura se presentan dichas tipologías:

CÓDIGO	TIPO DE ACCIÓN PREVENTIVA PROPUESTA
a	Supervisión preventiva del mando: revisión y control general por parte de la persona responsable de la unidad de trabajo, que ha recibido formación específica en prevención de riesgos.
b	Información preventiva del mando: recepción de la información sobre el análisis y evaluación de riesgos por parte del responsable de la unidad de trabajo, que será el encargado de transmitir a los trabajadores dicha información, así como las medidas preventivas a tener en cuenta.
c	Planificación de la prevención por la unidad de trabajo: el responsable de la unidad de trabajo es el encargado de planificar e incorporar los elementos de prevención en el día a día de la unidad.
d	Equipos de protección individual: revisión del material que forma parte de los equipos de protección de los trabajadores.
f	Compra de nuevo equipo de trabajo: adquisición de nuevos instrumentos para la prevención de riesgos en la organización.
g	Elementos de seguridad: revisión periódica de los elementos de control, prevención y seguridad, como guantes, equipos de protección o instalaciones eléctricas.
h	Mantenimiento de locales: conservación y vigilancia de los espacios en los que se realizan trabajos por parte de los trabajadores de la organización.
i	Formación general y específica: formar a los trabajadores, según su nivel de responsabilidad dentro de la organización, en materia de prevención a nivel general y a nivel específico, dependiendo de su unidad de trabajo.
j	Vigilancia de la salud: consiste en la recogida sistemática y continua de datos acerca de un problema específico de salud, su análisis, interpretación y utilización en la planificación, implementación y evaluación de programas de salud (Instituto Nacional de Seguridad e Higiene en el trabajo 1998, p. 1).
k	Estudios de Prevención de Riesgos especializados: realización de análisis sobre cómo prevenir y mitigar ciertos riesgos de materias concretas o específicas.

Figura 93 - Tipos de acciones preventivas definidas por la Organización X (elaboración propia).

A estas tipologías de acciones preventivas ya definidas por la organización se añade otra opción que se cree necesaria para el estudio de caso:

- 1 – Desarrollo de instrumentos preventivos: creación de herramientas (procedimientos, instrucciones, instrumentos, entre otros) que ayuden a mejorar la prevención en la organización.

Proceso

Dentro de la previsión de actuaciones de tratamiento se decide, además de actuar sobre los riesgos, hacerlo también sobre las causas. En el análisis de riesgos efectuado mediante la técnica de pajaritas, se observó que algunas de las causas aparecían en numerosos riesgos. En línea con varias de las opciones de tratamiento que propone la norma ISO 31000, como, por ejemplo, evitar el riesgo decidiendo no continuar con la actividad que causa el riesgo, o eliminar la fuente del riesgo, se decide definir actuaciones específicas para tratar las causas. Para ello, se define un criterio de mínimos, sobre el que poder basar la decisión de actuar o no sobre estas. En la Figura 80 se apreciaba claramente una serie de causas que superaban la media de recurrencia. Estas son: 1CA, 2CA, 7CA, 8CA, 9CA, 10CA, 11CA, 12CA, 14CA:

- 1 CA – Accesos no controlados
- 2 CA – Traslados no controlados
- 7 CA – Fallos en el control de las aplicaciones
- 8 CA – Documentación incompleta
- 9 CA – Préstamos y consultas no controlados
- 10 CA – Falta de verificación de transferencias
- 11CA – Falta de directrices sobre gestión documental
- 12 CA – Fallos en el registro o captura
- 14 CA – Falta de requisitos documentales

De estas 9 causas, 5 tienen una recurrencia de 10 o superior, lo cual proporciona un criterio de priorización para su tratamiento. Concretamente, estas 5 causas son: 1CA, 7CA, 11CA, 12CA y 14CA. Sobre ellas se deben realizar actuaciones en un plazo menor a las realizadas sobre el resto de causas que superan el valor medio de recurrencia. Se propone un plazo de 3 meses, en línea con los plazos de actuación establecidos por la organización para el tratamiento de riesgos. El resto de causas con valores superiores a la media, se deben tratar en un plazo de 6 meses.

El objetivo de actuar sobre las causas es disminuir o eliminar el origen del riesgo, lo que lleva a que este se produzca. En el caso de las causas mencionadas, su aparición recurrente a lo largo del análisis de riesgos, da una idea de la importancia que su tratamiento puede tener en la disminución del nivel y el valor de los riesgos.

Para el tratamiento de causas, se decide emplear los tipos de acciones preventivas ya mencionados, con la finalidad de no dispersar recursos y aprovechar la metodología desarrollada. En la siguiente figura se presentan las acciones preventivas a desarrollar para cada una de las causas seleccionadas, independientemente de la prioridad con la que se llevarán a cabo (ver Figura 94).

CAUSA	ACCIONES PREVENTIVAS A IMPLEMENTAR
1 CA	<p>l1 – desarrollo de un cuadro de roles y permisos para la organización.</p> <p>b1 – acción informativa sobre los cambios en la gestión de accesos a los documentos.</p> <p>i1 – acción formativa con relación a los cambios sobre la gestión de accesos para todo el personal afectado, en todos los niveles de la organización.</p> <p>a1 – control y revisión de los cambios por el responsable o responsables de las distintas unidades de trabajo.</p>
2 CA	<p>l2 – definición de una instrucción de trabajo sobre traslados.</p> <p>i2 – acción formativa con relación a los cambios sobre la gestión de los traslados en la organización, para todo el personal afectado.</p>
7 CA	<p>c1 – planificación de las acciones preventivas y revisión de las existentes, con relación al control de las aplicaciones informáticas.</p> <p>a2 – control y revisión continuos de la persona responsable del área de sistemas de información, para asegurar que las acciones preventivas se llevan a cabo según el calendario marcado, así como para realizar las adaptaciones necesarias en función de las necesidades de la organización.</p>
8 CA	<p>l3 – desarrollo de documentos normalizados o plantillas que prevengan la omisión de información o el desarrollo de índices de los expedientes para evitar la omisión de documentos.</p> <p>i3 – acción formativa y de concienciación sobre la necesidad de trabajar a partir de las plantillas existentes y sobre la importancia de generar y mantener todos los documentos necesarios de los distintos tipos de expedientes.</p>
9 CA	<p>l4 – revisión y actualización de los procedimientos o instrucciones existentes sobre préstamos y consultas.</p> <p>b2 – comunicación de los cambios a las personas con responsabilidad de las distintas áreas que realizan préstamos y consultas de documentación.</p> <p>i4 – acciones formativas para el personal que realiza préstamos y consultas con relación a la actualización del procedimiento, así como también para los archiveros implicados en estos procesos de trabajo.</p> <p>a3 – control y revisión, por parte de los responsables del área de gestión documental y archivo, de que la metodología establecida se está aplicando de manera adecuada.</p>
10 CA	<p>c2 – organización de la verificación de las transferencias que se realizan en la Organización X, con los recursos disponibles. Si a la hora de realizar la planificación se hiciese patente la necesidad de aumentar los recursos, debería hacerse llegar esta información a la dirección del organismo, informando de los riesgos y consecuencias asociados.</p> <p>a4 – la persona responsable del área de archivo y gestión documental debe revisar y supervisar que se verifican todas las transferencias realizadas en la organización.</p>

CAUSA	ACCIONES PREVENTIVAS A IMPLEMENTAR
11CA	<p>i5 – desarrollo de las herramientas necesarias para una adecuada praxis en la gestión documental. Asimismo, se deben revisar y actualizar los instrumentos existentes para aumentar las medidas preventivas a partir de los riesgos identificados y sus causas.</p> <p>b3 – estos instrumentos deberán comunicarse a los responsables de las distintas áreas de la organización, para ponerlos en su conocimiento y para que estos puedan transmitir la información a los trabajadores.</p> <p>i5 – acciones informativas y formativas necesarias para asegurar que los trabajadores conocen los instrumentos y la metodología a seguir en materia de gestión documental. También cabrá plantearse acciones de seguimiento y acompañamiento de la implantación de nuevas praxis para todo el personal.</p> <p>a5 – control y revisión de que los instrumentos se conocen y se utilizan de manera adecuada en cada área.</p>
12 CA	<p>a6 – seguimiento del proceso de captura y registro por los responsables del área que realiza estas tareas durante un periodo prefijado, para detectar incidencias y solucionar los posibles errores.</p>
14CA	<p>i6 – definición de los requisitos para la creación y gestión de documentos a partir del análisis de las necesidades de la organización y los requisitos de negocio y legales, si es necesario. Esta medida preventiva se relaciona directamente con las actuaciones propuestas para prevenir la causa 11CA, con las que debería trabajarse de manera conjunta.</p> <p>b4 – acción informativa para los responsables de área sobre los requisitos definidos y cómo afectan a la gestión de documentos.</p> <p>i6 – acciones formativas y de acompañamiento para los trabajadores, con la finalidad de que conozcan los requisitos que deben cumplir a la hora de crear y gestionar la documentación en la organización.</p> <p>a7 – supervisión de los responsables de área para controlar que se cumplen los requisitos establecidos y detectar posibles incidencias o desviaciones.</p>

Figura 94 - Acciones preventivas sobre las causas de riesgo con mayor recurrencia (elaboración propia).

Con relación a la prioridad de las acciones de tratamiento sobre las causas, se desarrolla un cronograma (ver Figura 95) en el que se incluye la calendarización de los tratamientos. Se decide disponer de un plazo lo suficientemente amplio como para poder llevar a cabo las distintas actuaciones preventivas en todos los niveles de la organización, así como poder compaginarlas con las acciones de tratamiento de los riesgos.

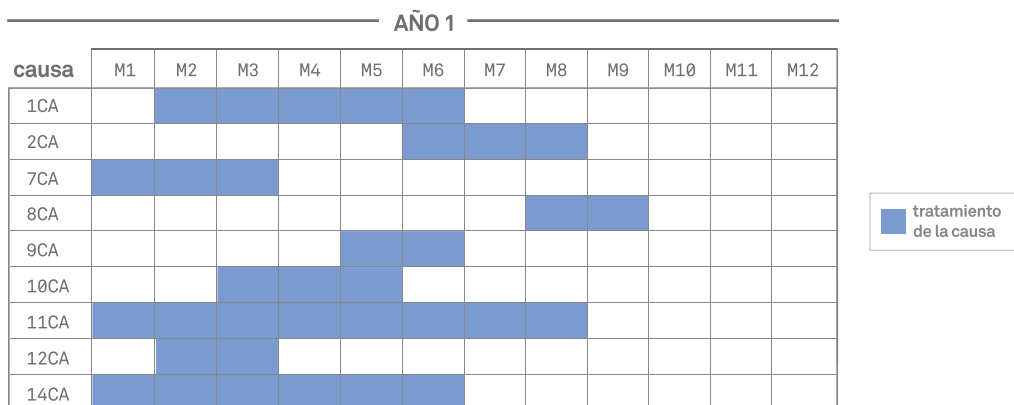


Figura 95 - Cronograma de tratamiento de las causas de riesgo (elaboración propia).

Para la Organización X es igualmente prioritario tratar tanto los riesgos, como aquellas causas con una recurrencia mayor, puesto que este segundo caso se ve como una oportunidad de aumentar el porcentaje de prevención global a partir de actuaciones concretas. Esta estrategia se alinea perfectamente con los estándares de gestión del riesgo. Ya en la norma ISO 31000, en el apartado 5.5.1 se menciona la actuación sobre las fuentes de riesgo o sobre las actividades que causan los riesgos, como parte del tratamiento. Es esta línea la que la Organización X ha decidido seguir, juntamente con el resto de acciones de tratamiento que se describen a continuación.

Siguiendo con el objetivo de prevenir o mitigar los riesgos y en línea con los resultados del proceso de evaluación, se propone a la Organización X una serie de actuaciones preventivas sobre los riesgos identificados. El tipo de acciones a implementar siguen las establecidas en el procedimiento de gestión del riesgo desarrollado por la propia organización, explicadas anteriormente (ver Figura 96).

RIESGO	ACCIONES PREVENTIVAS A IMPLEMENTAR
1	<p>i7 – acciones formativas y de concienciación sobre gestión documental para todos los trabajadores de la organización, en todos los niveles. Especialmente, cuestiones relacionadas con la ordenación, clasificación, descripción y archivo de los documentos.</p> <p>a8 – el responsable de cada una de las áreas, junto con el responsable de gestión documental y archivo, deberá llevar a cabo la supervisión de las diferentes acciones relacionadas con las causas que llevan al riesgo.</p>
2	<p>b5 – acción informativa del responsable de gestión documental, coordinada con el responsable de cada área, sobre la importancia de la integridad de la información y los documentos que se gestionan en la organización.</p> <p>i8 – acciones formativas y de concienciación sobre gestión documental para todos los trabajadores de la organización, en todos los niveles, haciendo hincapié en la importancia de la integridad de la información y la documentación.</p> <p>a9 – el responsable de cada una de las áreas, junto con el responsable de gestión documental y archivo, deberá llevar a cabo la supervisión de las diferentes acciones relacionadas con las causas que llevan al riesgo.</p>
3	i7 – desarrollar la tabla de documentos esenciales.
4	i8 – desarrollar el catálogo de procedimientos.
5	<p>a10 – el responsable de cada una de las áreas, junto con el responsable de gestión documental y archivo, deberá llevar a cabo la supervisión de las diferentes acciones relacionadas con las causas que llevan al riesgo.</p> <p>i9 – acciones formativas y de concienciación sobre gestión documental para todos los trabajadores de la organización, en todos los niveles. Estas acciones deben centrarse en la importancia de seguir las instrucciones sobre gestión documental para garantizar que la información y los documentos se gestionan de manera adecuada y pueden recuperarse cuando sea necesario.</p>

RIESGO	ACCIONES PREVENTIVAS A IMPLEMENTAR
6	<p>a11 – el responsable de cada una de las áreas, junto con el responsable de gestión documental y archivo, deberá llevar a cabo la supervisión de las diferentes acciones relacionadas con las causas que llevan al riesgo.</p>
7	<p>i10 – acciones formativas y de concienciación sobre gestión documental para todos los trabajadores de la organización, en todos los niveles, haciendo hincapié en la importancia de seguir el procedimiento establecido para la eliminación de documentos.</p> <p>h1 – tareas de mantenimiento para asegurar que los accesos a los depósitos de archivo disponen de las medidas de seguridad adecuadas y en funcionamiento.</p> <p>a12 – el responsable de cada una de las áreas, junto con el responsable de gestión documental y archivo, deberá llevar a cabo la supervisión de los procesos de eliminación de documentos.</p>
8	<p>h2 – tareas de mantenimiento para asegurar que los accesos a los depósitos de archivo disponen de las medidas de seguridad adecuadas y en funcionamiento.</p>
9	<p>c3 – planificación, desde el área de gestión documental y archivo en coordinación con el resto de dependencias de la organización, con relación a la prevención sobre los procesos de gestión documental que permiten el acceso a los documentos, en especial aquellos relacionados con la preservación y la seguridad.</p> <p>h3 – tareas de mantenimiento para asegurar que los depósitos de archivo disponen de las medidas de conservación preventiva necesarias.</p>
10	<p>h4– tareas de mantenimiento para asegurar que los depósitos de archivo disponen de las medidas de conservación preventiva necesarias.</p> <p>c4 – planificación, desde el área de gestión documental y archivo en coordinación con el resto de dependencias de la organización, con relación a la prevención sobre los procesos de gestión documental que permiten el uso de los documentos a medio y largo plazo, en especial aquellos relacionados con la preservación digital y la conservación física de los mismos.</p>
11	<p>b6 – acción informativa del responsable de gestión documental, coordinada con el responsable de cada área, sobre la importancia de seguir el procedimiento establecido para la eliminación de documentos.</p>
12	<p>b7 – acción informativa del responsable de gestión documental, coordinada con el responsable de cada área, sobre la importancia de seguir las directrices establecidas en la ordenación y archivo de los documentos.</p> <p>a13 – el responsable de cada una de las áreas, junto con el responsable de gestión documental y archivo, deberá llevar a cabo la supervisión de las diferentes acciones relacionadas con las causas que llevan al riesgo.</p>
13	<p>i11 – acciones de concienciación sobre gestión documental para todos los trabajadores de la organización, en todos los niveles.</p>
14	<p>b8 – acción informativa del responsable de gestión documental, coordinada con el responsable de cada área, sobre la importancia de no generar copias de documentos no necesarias para el funcionamiento de la organización.</p>
15	<p>b9 – acción informativa del responsable de gestión documental, coordinada con el responsable de cada área, sobre la importancia de no generar documentos o copias de documentos no necesarias para el funcionamiento de la organización.</p>
16	<p>c5 – planificación desde el área de gestión documental para supervisar los instrumentos de gestión documental existentes, evaluarlos, eliminar posibles duplicidades y actualizarlos.</p> <p>a14 – el responsable de gestión documental y archivo deberá llevar a cabo la supervisión del cumplimiento con la planificación, así como de los resultados obtenidos.</p>

RIESGO	ACCIONES PREVENTIVAS A IMPLEMENTAR
17	<p>b10 – acción informativa del responsable de gestión documental, coordinada con el responsable de cada área, sobre la importancia de la trazabilidad de la información y los documentos que se gestionan en la organización.</p> <p>i12 – acciones de concienciación sobre gestión documental para todos los trabajadores de la organización, en todos los niveles.</p> <p>a15 – el responsable de cada una de las áreas, junto con el responsable de gestión documental y archivo, deberá llevar a cabo la supervisión de las diferentes acciones relacionadas con las causas que llevan al riesgo.</p>
18	<p>b11– acción informativa del responsable de gestión documental, coordinada con el responsable de cada área, sobre la importancia de la autenticidad de la información y los documentos que se gestionan en la organización.</p> <p>i13 – acciones de concienciación sobre gestión documental para todos los trabajadores de la organización, en todos los niveles.</p> <p>a16 – el responsable de cada una de las áreas, junto con el responsable de gestión documental y archivo, deberá llevar a cabo la supervisión de las diferentes acciones relacionadas con las causas que llevan al riesgo.</p>
19	<p>b12 – acción informativa del responsable de gestión documental, coordinada con el responsable de cada área, sobre la importancia de la fiabilidad de la información y los documentos que se gestionan en la organización.</p> <p>i14 – acciones de concienciación sobre gestión documental para todos los trabajadores de la organización, en todos los niveles.</p> <p>a17 – el responsable de cada una de las áreas, junto con el responsable de gestión documental y archivo, deberá llevar a cabo la supervisión de las diferentes acciones relacionadas con las causas que llevan al riesgo.</p>
20	<p>b13 – acción informativa del responsable de gestión documental, coordinada con el responsable de cada área, sobre la importancia de seguir las directrices sobre descripción documental.</p> <p>i15 – acciones formativas sobre la descripción de documentos para todos los trabajadores de la organización que realicen este proceso, especialmente los archiveros.</p>
21	<p>i9 – realización de un inventario de aplicaciones informáticas existentes por parte del área de sistemas de información.</p> <p>c6 – planificación desde el área de sistemas de información sobre las necesidades de aplicaciones informáticas en la organización.</p>
22	<p>a18 – auditoría de las características de las aplicaciones informáticas existentes sobre la interoperabilidad,.</p> <p>c7 – planificación de los cambios y actualizaciones de las aplicaciones informáticas para cumplir con los requisitos de interoperabilidad.</p>
23	<p>b14 – acción informativa del responsable de gestión documental, coordinada con el responsable del área de sistemas de información, sobre la importancia de una rápida respuesta ante fallos del sistema cuando sea necesario. En esta acción se aprovechará para resolver dudas sobre el procedimiento a seguir.</p> <p>i16 – acción formativa específica para explicar el procedimiento a seguir en caso de un fallo del sistema. Esta acción debe dirigirse a aquellas personas que estén involucradas de alguna manera en dicho procedimiento.</p> <p>a19 – el responsable de cada una de las áreas, junto con el responsable de gestión documental y archivo, deberá llevar a cabo la supervisión de las diferentes acciones relacionadas con las causas que llevan al riesgo.</p>

RIESGO	ACCIONES PREVENTIVAS A IMPLEMENTAR
<p>24</p>	<p>i10 – desarrollo de un informe sobre las necesidades de infraestructura (física y tecnológica) de la organización.</p> <p>c8 – planificación de los cambios que deberán realizarse a partir del informe (físicos y tecnológicos).</p> <p>h5 – tareas de mantenimiento para asegurar que se dispone de depósitos de archivo adecuados a las necesidades de la organización.</p>
<p>25</p>	<p>b15 – acción informativa del responsable de gestión documental, coordinada con el responsable del área de sistemas de información, sobre la importancia de una rápida respuesta ante la interrupción de la actividad en la organización.</p> <p>i17 – acción formativa específica para explicar el procedimiento a seguir en caso de una interrupción. Esta acción debe dirigirse a aquellas personas que estén involucradas de alguna manera en dicho procedimiento.</p>
<p>26</p>	<p>i18 – acciones formativas y de concienciación sobre gestión documental para todos los trabajadores de la organización, en todos los niveles, haciendo hincapié en la importancia de seguir las directrices establecidas sobre el acceso a las aplicaciones informáticas.</p> <p>a20 – el responsable de cada una de las áreas, junto con el responsable de gestión documental y archivo, deberá llevar a cabo la supervisión de las diferentes acciones relacionadas con las causas que llevan al riesgo.</p>
<p>27</p>	<p>b16 – acción informativa del responsable de gestión documental, coordinada con el responsable del área de sistemas de información, sobre el procedimiento a seguir por los trabajadores en caso de no poder acceder a las aplicaciones.</p> <p>c9 – planificación de la respuesta sobre las incidencias relacionados con los accesos a las aplicaciones.</p>

Figura 96 - Acciones preventivas sobre los riesgos (elaboración propia).

Para la implantación de estas actuaciones, se elabora un cronograma (ver Figura 97) con la previsión de cuando se deben implementar las acciones de prevención de cada uno de los riesgos.

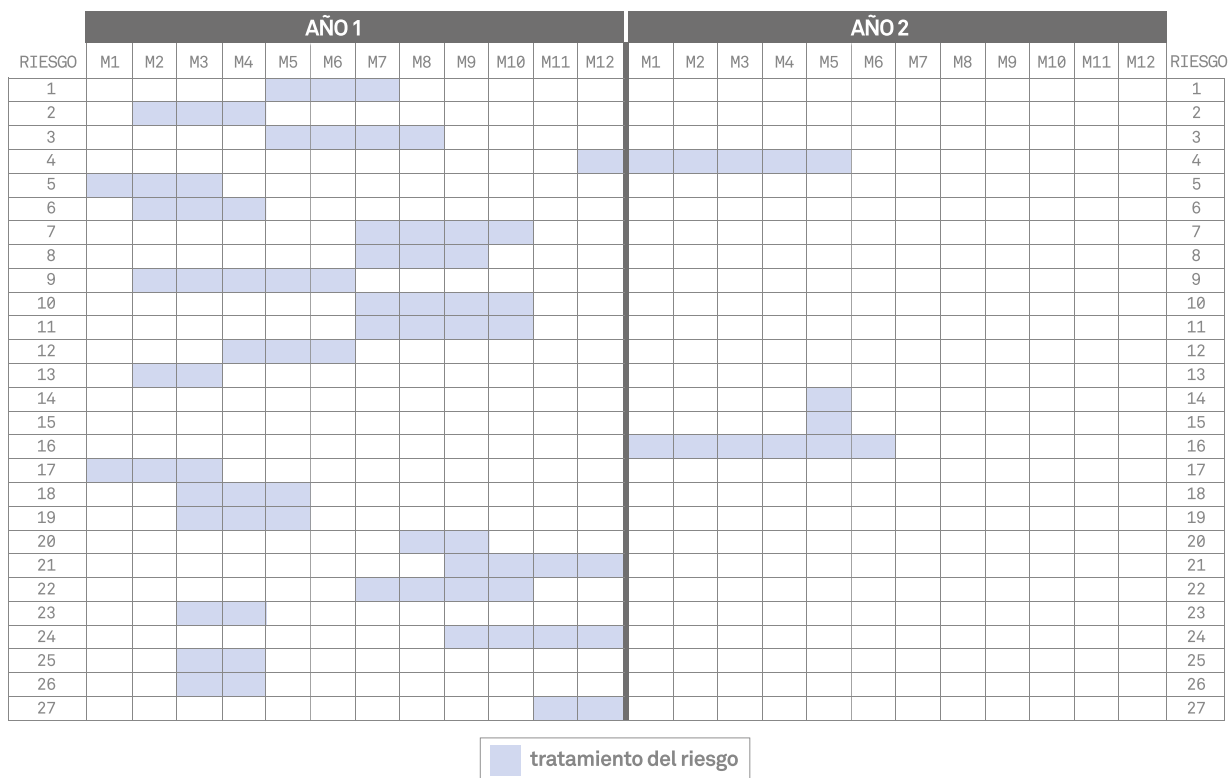


Figura 97 - Cronograma para el tratamiento de riesgos (elaboración propia).

En este cronograma se aprecia que no todas las actuaciones se planifican al mismo tiempo, sino que, en función de los grupos y niveles de prioridad, el tratamiento se define con una mayor o menor urgencia. Se decide trabajar sobre un periodo de tiempo amplio para facilitar el seguimiento por parte de los trabajadores de la Organización X. Cabe recordar que la falta de recursos mencionada por los interlocutores de la organización es un aspecto destacado del análisis del contexto, por lo que es fundamental tenerlo en cuenta a la hora de planificar el tratamiento y revisión de los riesgos. Por este motivo se opta por unos plazos amplios y una implantación de acciones escalonada en el tiempo.

El plazo final marcado es de 18 meses, a contar desde la primera acción de tratamiento o prevención. El cronograma está pensado para que el volumen de trabajo nunca suponga un inconveniente que impida realizarlo. Se basa en el valor del riesgo y su prioridad asociada, a partir de la evaluación.

Este cronograma debe leerse en complementariedad con el calendario de acciones de prevención de las causas (ver Figura 95). Actuando tanto sobre los riesgos como sobre las causas, los resultados deben poder apreciarse en un margen de tiempo inferior y deben conseguirse unos mejores resultados de prevención, contribuyendo a una mejora en la consecución de los objetivos de la organización.

Conclusiones

Pese a que esta fase no se ha llevado a cabo todavía en la Organización X, sí se considera una planificación ajustada tanto a las necesidades de la misma como a sus recursos actuales. Es un objetivo principal poder distribuir las distintas actuaciones de tratamiento en el tiempo, de manera que puedan asumirse realmente con los recursos disponibles.

Siguiendo la metodología de la Organización X, se definen acciones de tratamiento directas y muy concretas, en la mayoría de casos. Estas se deben llevar a cabo en un periodo temporal amplio, si bien la mayoría de los tratamientos se enmarcan en los primeros 10 meses. De este modo, junto con el tratamiento de las causas que también se enmarca dentro del mismo plazo de tiempo, se consigue una doble prevención.

En 10 meses se habrán aplicado medidas de tratamiento a todas las causas seleccionadas en función de los criterios explicados anteriormente. Cabe recordar que estas son las causas con una mayor recurrencia y que afectan a un mayor número de riesgos, con lo que, implementando las medidas preventivas definidas se actúa en la prevención de los riesgos. Esta estrategia permite, por tanto, actuar sobre los riesgos doblemente, desde su origen hasta el riesgo propiamente. Se considera una decisión acertada y se espera poder obtener buenos resultados.

Por otro lado, se considera positivo haber partido de los tipos de actuaciones preventivas ya definidas en la organización para obtener una mayor implicación y comprensión de los trabajadores en el proceso de prevención. Disponer de una metodología ya definida facilita la planificación del tratamiento de riesgos y facilitará enormemente su comprensión por parte de los trabajadores implicados de la Organización X. Además, esto permite el conocimiento de la metodología existente de gestión de riesgos por áreas y personal no implicados directamente en la prevención de riesgos laborales, lo que favorecerá las sinergias y mejoras globales de la metodología existente.

5.5 Fase 4. Propuesta de seguimiento y revisión

Este apartado engloba las acciones de seguimiento y revisión de los riesgos. Estas deben abarcar todos los aspectos del proceso de gestión del riesgo, con la finalidad de (AENOR 2010, p. 26):

- Asegurar que los controles son eficaces y eficientes tanto en su diseño como en su utilización.
- Obtener la información adicional para mejorar la apreciación del riesgo.
- Analizar y sacar conclusiones de los sucesos, cambios, tendencias, éxitos y fallos.
- Detectar los cambios en el contexto interno y externo, incluidos los cambios en los criterios de riesgo y en el propio riesgo, que puedan requerir la revisión de los tratamientos de riesgo y de las prioridades.
- Identificar los riesgos emergentes.

Esta fase tampoco se ha llevado a cabo en la organización, sino que se trata de una propuesta entregada sobre la base de la anterior propuesta de tratamientos.

Siguiendo el procedimiento de la Organización X, una vez establecidas las acciones preventivas, con la finalidad de eliminar o reducir los riesgos detectados, es necesario establecer un control periódico para comprobar la correcta implantación de las acciones preventivas y ver si su elección es adecuada o si, en caso contrario, deben cambiarse por otras más eficaces. Por este motivo, y en línea con lo establecido también en los estándares internacionales, se proponen medidas de revisión, tanto de las acciones preventivas como de los riesgos, dejando pasar un plazo prudencial desde la previsión de la implantación de los tratamientos.

Se trabaja con dos cronogramas. El primero se elabora a partir del calendario de tratamiento para las causas (ver Figura 95) y el segundo, a partir del calendario de tratamiento de riesgos (ver Figura 97). En ambos casos, se establece un periodo prudencial para dejar actuar las acciones de tratamiento antes de la revisión.

Para el seguimiento de los tratamientos de las causas, se incluye tan solo una revisión. Es necesario comprobar que las actuaciones llevadas a cabo están realmente afectando a las causas. Para ello, se proponen revisiones para cada uno de los tratamientos, en función del calendario establecido en la fase anterior.

En cambio, para el seguimiento de los tratamientos de riesgos se incluyen dos tipos de revisiones:

- Revisión del tratamiento: previsión de cuándo se deben evaluar las acciones de tratamiento de cada uno de los riesgos.
- Apreciación del riesgo: realización del proceso de identificación, análisis y evaluación para una nueva toma de decisiones sobre el tratamiento.

Se incluye la apreciación del riesgo en este calendario con el objetivo de que la organización vuelva a iniciar el proceso pasados unos meses del tratamiento. De este modo, no solo se incluye la revisión del tratamiento en esta fase, sino que queda también planificado el inicio del proceso nuevamente. Cabe recordar que la gestión del riesgo debe entenderse de manera cíclica. Debido a que se producen sucesos externos e internos, el contexto y los conocimientos cambian, se realiza el seguimiento y la revisión de riesgos, surgen nuevos riesgos, algunos cambian y otros desaparecen (AENOR 2010, p. 14).

Para el tratamiento de causas, se establece la revisión en los últimos meses del periodo anual definido, tal y como se puede ver en la Figura 98. Se parte del calendario de priorización establecido en función del valor de cada causa. El objetivo es concentrar la revisión en un mismo periodo para, de este modo, obtener una visión global de los objetivos conseguidos. Para ello, se determinan dos meses para las revisiones, considerándolo un plazo suficiente a la vista de los recursos disponibles en la Organización X.

Es una posibilidad que, una vez revisados los tratamientos de algunas de las causas, estas lleguen a desaparecer. Por este motivo, debe llevarse a cabo esta revisión con la visión global del proceso de gestión del riesgo y, sobre todo, incluyendo estas acciones de supervisión dentro de la revisión de los tratamientos de los riesgos.

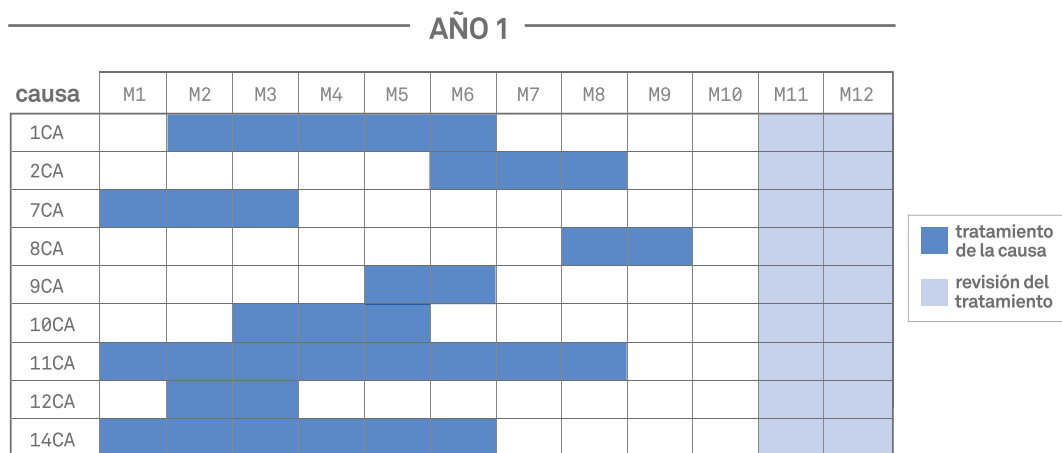


Figura 98 - Cronograma para el tratamiento y revisión de las causas de riesgo (elaboración propia).

Para la revisión del tratamiento de riesgos se planifica el calendario en función de los grupos de prioridad resultantes de la evaluación. Además, se contempla un periodo de 2 meses al final del segundo año para llevar a cabo una nueva apreciación del riesgo (ver Figura 99). Este proceso debe incluir la identificación de nuevos riesgos, así como un nuevo análisis y evaluación tanto de los nuevos riesgos como de los ya identificados en la primera apreciación. Es fundamental para el éxito de la gestión de riesgos en la organización no olvidar que se trata de un proceso continuo, que no finaliza con la implantación de las acciones de tratamiento.

Esta decisión no es fácil, puesto que tal y como se puede apreciar en el cronograma de tratamiento de riesgos, algunas de las revisiones quedan muy alejadas de los tratamientos y otras muy cercanas en el tiempo. El objetivo es encontrar el punto exacto en el que poder realizar las revisiones por grupos para poder obtener resultados fiables sobre la efectividad de los tratamientos.

Cabe mencionar que la planificación propuesta no se ha llevado a cabo todavía en la organización y es posible que se produzcan cambios a medida que se avance en los tratamientos. Planificar es siempre arriesgado, pero se considera que, con ambos cronogramas, el calendario se ajusta a las necesidades y recursos de la Organización X a partir del análisis del contexto realizado.

5.6 Documentación del proceso

Según la norma ISO 31000 las actividades de gestión del riesgo deben ser trazables. Para ello es fundamental documentar el proceso, no de manera finalista, sino desde el inicio e incluyendo las revisiones y actualizaciones de la información que se obtienen a lo largo de las distintas fases.

Para la Organización X se ha desarrollado una ficha para documentar cada riesgo. Esta ficha se diseña a partir del modelo planteado en el informe técnico ISO/TR 18128. En el Anexo A (informativo) de esta norma se propone un ejemplo de entrada en un registro de riesgos, con el objetivo de tener documentadas todas las informaciones relativas a un riesgo, desde la descripción, la probabilidad y consecuencias, hasta el coste para la organización en caso de producirse. Se trata de un ejemplo muy preciso y con un amplio abanico de informaciones a considerar.

A partir de este ejemplo, se adaptan los campos de información a la Organización X y se simplifica la ficha. Esta decisión se toma de acuerdo con los recursos existentes que pueden dedicarse al control de estas informaciones. Por ello, se desarrolla una ficha con un gran volumen de información, pero sin incluir todos los puntos del informe técnico mencionado. El objetivo final es que resulte un instrumento práctico y funcional para la organización.

La ficha diseñada incluye las siguientes áreas de información:

- Identificación del riesgo
- Análisis del riesgo
- Evaluación del riesgo
- Tratamiento del riesgo

Se corresponden con las distintas fases del proceso de gestión del riesgo. Dentro de cada una de las áreas se incluyen diferentes informaciones de interés para el control y seguimiento de cada uno de los riesgos.

Ficha del riesgo	
Campos de la ficha	Explicación del contenido
Identificación del riesgo	
ID del riesgo	Número identificativo
Nombre del riesgo	Identificación breve
Descripción	Explicación del riesgo
Proceso de gestión documental relacionado ⁸⁵	Enumeración de los procesos de gestión documental afectados por el riesgo
Análisis del riesgo	
Probabilidad	Según escala de probabilidad
Impacto/Consecuencias	Según escala de impacto
Nivel del riesgo	Según la matriz de probabilidad e impacto
Riesgos relacionados	Enumeración de otros riesgos identificados que se relacionen
Evaluación del riesgo	
Valor del riesgo	Según la evaluación del riesgo
Prioridad de tratamiento	Según el valor de riesgo determinado
Tratamiento del riesgo	
Tipo de actuaciones	Según la tipología definida por la organización X en su procedimiento de gestión del riesgo
Fecha límite del tratamiento	Plazo para llevar a cabo el tratamiento
Revisión del tratamiento	Plazo para llevar a cabo la revisión del tratamiento

Figura 100 - Ficha de riesgo (elaboración propia).

Esta ficha debe cumplimentarse con la información de cada uno de los riesgos para los distintos campos de información.

⁸⁵ – Los procesos de gestión documental identificados en las fichas se basan en los procesos para la creación, captura y gestión de los documentos enumerados y descritos en la norma internacional ISO 15489: 2016.

Fichas informadas de la Organización X

Se cumplimenta una ficha por cada riesgo. Las fichas definidas se presentan a continuación.

Ficha del riesgo	
Identificación del riesgo	
ID del riesgo	1
Nombre del riesgo	Pérdida de información/documentación
Descripción	Extravío o desaparición de información o documentación generada o recibida por la organización en el ejercicio de sus funciones.
Proceso de gestión documental relacionado	<ul style="list-style-type: none"> • Creación y Captura • Clasificación • Acceso • Almacenamiento • Uso y reutilización • Migración y conversión • Disposición
Análisis del riesgo	
Probabilidad	2
Impacto/Consecuencias	4
Nivel del riesgo	V – Moderado
Riesgos relacionados	3 – Pérdida de documentos esenciales 5 – No recuperación de información/documentación 7 – Eliminación indebida de documentos 8 – Sustracción o robo de documentos 26 – Accesos indebidos a las aplicaciones
Evaluación del riesgo	
Valor del riesgo	5,72
Prioridad de tratamiento	3
Tratamiento del riesgo	
Tipo de actuaciones	i – Formación general y específica a – Supervisión preventiva del mando
Fecha límite del tratamiento	< 6 meses
Revisión del tratamiento	< 11 meses

Figura 101 - Ficha de riesgo 1 (elaboración propia).

Ficha del riesgo	
Identificación del riesgo	
ID del riesgo	2
Nombre del riesgo	Falta de garantías de integridad
Descripción	Documentos y/o expedientes de los que no puede certificarse o asegurarse su completitud o inalterabilidad a lo largo del tiempo en que deben ser conservados.
Proceso de gestión documental relacionado	<ul style="list-style-type: none"> • Creación y Captura • Clasificación • Acceso • Almacenamiento • Uso y reutilización • Migración y conversión • Disposición
Análisis del riesgo	
Probabilidad	2
Impacto/Consecuencias	4
Nivel del riesgo	V – Moderado
Riesgos relacionados	6 – Accesos indebidos a información 12 – Ubicación errónea o indebida de documentos 13 – Manipulación no autorizada de documentos 17 – Falta de garantías de trazabilidad 26 – Accesos indebidos a las aplicaciones
Evaluación del riesgo	
Valor del riesgo	6,55
Prioridad de tratamiento	2
Tratamiento del riesgo	
Tipo de actuaciones	b – Información preventiva del mando i – Formación general y específica a – Supervisión preventiva del mando
Fecha límite del tratamiento	< 3 meses
Revisión del tratamiento	< 11 meses

Figura 102 - Ficha de riesgo 2 (elaboración propia).

Ficha del riesgo	
Identificación del riesgo	
ID del riesgo	3
Nombre del riesgo	Pérdida de documentos esenciales
Descripción	Falta de generación o pérdida de evidencias documentales consideradas fundamentales para la gestión de las funciones de la organización.
Proceso de gestión documental relacionado	<ul style="list-style-type: none"> • Creación y Captura • Clasificación
Análisis del riesgo	
Probabilidad	2
Impacto/Consecuencias	5
Nivel del riesgo	VI – Considerable
Riesgos relacionados	1 – Pérdida de información/documentación 4 – No creación de evidencias documentales 5 – No recuperación de información/documentación 6 – Accesos indebidos a información 7 – Eliminación indebida de documentos 8 – Sustracción o robo de documentos 12 – Ubicación errónea o indebida de documentos 26 – Accesos indebidos a las aplicaciones
Evaluación del riesgo	
Valor del riesgo	4,48
Prioridad de tratamiento	3
Tratamiento del riesgo	
Tipo de actuaciones	I – Desarrollo de instrumentos para la prevención
Fecha límite del tratamiento	< 6 meses
Revisión del tratamiento	< 15 meses

Figura 103 - Ficha de riesgo 3 (elaboración propia).

Ficha del riesgo	
Identificación del riesgo	
ID del riesgo	4
Nombre del riesgo	No creación de evidencias documentales
Descripción	Falta de generación de documentos, considerados necesarios para la gestión de las funciones y actividades de la organización.
Proceso de gestión documental relacionado	<ul style="list-style-type: none"> • Creación y Captura • Clasificación
Análisis del riesgo	
Probabilidad	3
Impacto/Consecuencias	2
Nivel del riesgo	IV – Leve
Riesgos relacionados	3 – Pérdida de documentos esenciales 27 – Incapacidad para acceder a las aplicaciones
Evaluación del riesgo	
Valor del riesgo	3,25
Prioridad de tratamiento	4
Tratamiento del riesgo	
Tipo de actuaciones	l– Desarrollo de instrumentos para la prevención
Fecha límite del tratamiento	< 1 año
Revisión del tratamiento	< 21 meses

Figura 104 - Ficha de riesgo 4 (elaboración propia).

Ficha del riesgo	
Identificación del riesgo	
ID del riesgo	5
Nombre del riesgo	No recuperación de información/documentación
Descripción	Incapacidad para localizar o acceder a información o documentación generada o recibida por la organización en el ejercicio de sus funciones.
Proceso de gestión documental relacionado	<ul style="list-style-type: none"> • Creación y Captura • Clasificación • Acceso • Almacenamiento • Uso y reutilización • Migración y conversión • Disposición
Análisis del riesgo	
Probabilidad	3
Impacto/Consecuencias	3
Nivel del riesgo	V – Moderado
Riesgos relacionados	1 - Pérdida de información/documentación 3 - Pérdida de documentos esenciales 6 - Accesos indebidos a información 7 - Eliminación indebida de documentos 8 - Sustracción o robo de documentos 12 - Ubicación errónea o indebida de documentos 20 - Errores en la descripción documental 24 - Infraestructura insuficiente 25 - Interrupción de la actividad 27 - Incapacidad para acceder a las aplicaciones
Evaluación del riesgo	
Valor del riesgo	7,95
Prioridad de tratamiento	2
Tratamiento del riesgo	
Tipo de actuaciones	a – Supervisión preventiva del mando i – Formación general y específica
Fecha límite del tratamiento	< 3 meses
Revisión del tratamiento	< 7 meses

Figura 105 - Ficha de riesgo 5 (elaboración propia).

Ficha del riesgo	
Identificación del riesgo	
ID del riesgo	6
Nombre del riesgo	Accesos indebidos a información
Descripción	Entrada a o lectura de información sin disponer de permiso o autorización para ello.
Proceso de gestión documental relacionado	<ul style="list-style-type: none"> • Clasificación • Acceso • Almacenamiento de documentos • Uso y reutilización • Disposición
Análisis del riesgo	
Probabilidad	3
Impacto/Consecuencias	3
Nivel del riesgo	V – Moderado
Riesgos relacionados	1 - Pérdida de información/documentación 2 - Falta de garantías de integridad 3 - Pérdida de documentos esenciales 5 - No recuperación de información/documentación 7 - Eliminación indebida de documentos 8 - Sustracción o robo de documentos 12 - Ubicación errónea o indebida de documentos 13 - Manipulación no autorizada de documentos 17 - Falta de garantías de trazabilidad 19 - Falta de garantías de fiabilidad 26 - Accesos indebidos a las aplicaciones
Evaluación del riesgo	
Valor del riesgo	7,24
Prioridad de tratamiento	2
Tratamiento del riesgo	
Tipo de actuaciones	a – Supervisión preventiva del mando
Fecha límite del tratamiento	< 3 meses
Revisión del tratamiento	< 11 meses

Figura 106 - Ficha de riesgo 6 (elaboración propia).

Ficha del riesgo	
Identificación del riesgo	
ID del riesgo	7
Nombre del riesgo	Eliminación indebida de documentos
Descripción	Dstrucción de información o documentación sin disponer del permiso o autorización para ello, o por error.
Proceso de gestión documental relacionado	<ul style="list-style-type: none"> • Acceso • Almacenamiento • Disposición
Análisis del riesgo	
Probabilidad	2
Impacto/Consecuencias	5
Nivel del riesgo	VI – Considerable
Riesgos relacionados	1 - Pérdida de información/documentación 3 - Pérdida de documentos esenciales 20 - Errores en la descripción documental
Evaluación del riesgo	
Valor del riesgo	4,95
Prioridad de tratamiento	3
Tratamiento del riesgo	
Tipo de actuaciones	i – Formación general y específica h – Mantenimiento de locales a – Supervisión preventiva del mando
Fecha límite del tratamiento	< 6 meses
Revisión del tratamiento	< 15 meses

Figura 107 - Ficha de riesgo 7 (elaboración propia).

Ficha del riesgo	
Identificación del riesgo	
ID del riesgo	8
Nombre del riesgo	Sustracción o robo de documentos
Descripción	Hurto de documentación o información.
Proceso de gestión documental relacionado	<ul style="list-style-type: none"> • Clasificación • Acceso • Almacenamiento • Uso y reutilización • Disposición
Análisis del riesgo	
Probabilidad	1
Impacto/Consecuencias	5
Nivel del riesgo	V – Moderado
Riesgos relacionados	1 - Pérdida de información/documentación 3 - Pérdida de documentos esenciales 6 - Accesos indebidos a información 12 - Ubicación errónea o indebida de documentos 26 - Accesos indebidos a las aplicaciones
Evaluación del riesgo	
Valor del riesgo	5,35
Prioridad de tratamiento	3
Tratamiento del riesgo	
Tipo de actuaciones	h – Mantenimiento de locales
Fecha límite del tratamiento	< 6 meses
Revisión del tratamiento	< 15 meses

Figura 108 - Ficha de riesgo 8 (elaboración propia).

Ficha del riesgo	
Identificación del riesgo	
ID del riesgo	9
Nombre del riesgo	Falta de garantías de accesibilidad
Descripción	Documentación de la que no puede certificarse o asegurarse su localización, recuperación y acceso a lo largo del tiempo en que debe ser conservada.
Proceso de gestión documental relacionado	<ul style="list-style-type: none"> • Creación y Captura • Clasificación • Acceso • Almacenamiento • Uso y reutilización • Migración y conversión • Disposición
Análisis del riesgo	
Probabilidad	2
Impacto/Consecuencias	4
Nivel del riesgo	V – Moderado
Riesgos relacionados	3 - Pérdida de documentos esenciales 5 - No recuperación de información/documentación 7 - Eliminación indebida de documentos 8 - Sustracción o robo de documentos 10 - Falta de garantías de usabilidad 12 - Ubicación errónea o indebida de documentos 17 - Falta de garantías de trazabilidad
Evaluación del riesgo	
Valor del riesgo	6,05
Prioridad de tratamiento	2
Tratamiento del riesgo	
Tipo de actuaciones	c – Planificación de la prevención por la unidad de trabajo h – Mantenimiento de locales
Fecha límite del tratamiento	< 3 meses
Revisión del tratamiento	< 11 meses

Figura 109 - Ficha de riesgo 9 (elaboración propia).

Ficha del riesgo	
Identificación del riesgo	
ID del riesgo	10
Nombre del riesgo	Falta de garantías de usabilidad
Descripción	Incapacidad para asegurar la localización, recuperación, presentación, interpretación y uso de un documento a lo largo del tiempo en que debe ser conservado.
Proceso de gestión documental relacionado	<ul style="list-style-type: none"> • Creación y Captura • Clasificación • Acceso • Almacenamiento • Uso y reutilización • Migración y conversión • Disposición
Análisis del riesgo	
Probabilidad	1
Impacto/Consecuencias	4
Nivel del riesgo	IV – Leve
Riesgos relacionados	1 – Pérdida de información/documentación 6 – No recuperación de información/documentación 9 – Falta de garantías de accesibilidad 18 – Falta de garantías de trazabilidad 25 – Falta de interoperabilidad
Evaluación del riesgo	
Valor del riesgo	5,43
Prioridad de tratamiento	3
Tratamiento del riesgo	
Tipo de actuaciones	h – Mantenimiento de locales c – Planificación de la prevención por la unidad de trabajo
Fecha límite del tratamiento	< 6 meses
Revisión del tratamiento	< 21 meses

Figura 110 - Ficha de riesgo 10 (elaboración propia).

Ficha del riesgo	
Identificación del riesgo	
ID del riesgo	11
Nombre del riesgo	No eliminación de documentos
Descripción	Conservación innecesaria de documentación, pese a estar establecida su eliminación en el calendario de conservación y en las directrices de disposición.
Proceso de gestión documental relacionado	<ul style="list-style-type: none"> • Clasificación • Almacenamiento • Disposición
Análisis del riesgo	
Probabilidad	2
Impacto/Consecuencias	2
Nivel del riesgo	III – Muy leve
Riesgos relacionados	12 - Ubicación errónea o indebida de documentos 14 - Duplicidad documental
Evaluación del riesgo	
Valor del riesgo	2,83
Prioridad de tratamiento	4
Tratamiento del riesgo	
Tipo de actuaciones	b – Información preventiva del mando
Fecha límite del tratamiento	< 1 año
Revisión del tratamiento	< 21 meses

Figura 111 - Ficha de riesgo 11 (elaboración propia).

Ficha del riesgo	
Identificación del riesgo	
ID del riesgo	12
Nombre del riesgo	Ubicación errónea o indebida de documentos
Descripción	Falta de control y seguimiento en el almacenamiento de la documentación (ya sea en papel o electrónica) en los depósitos físicos o en los repositorios electrónicos.
Proceso de gestión documental relacionado	<ul style="list-style-type: none"> • Creación y Captura • Clasificación • Acceso • Almacenamiento • Migración y conversión • Disposición
Análisis del riesgo	
Probabilidad	3
Impacto/Consecuencias	4
Nivel del riesgo	VI – Considerable
Riesgos relacionados	1 - Pérdida de información/documentación 3 - Pérdida de documentos esenciales 5 - No recuperación de información/documentación 6 - Accesos indebidos a información 8 - Sustracción o robo de documentos 13 - Manipulación no autorizada de documentos
Evaluación del riesgo	
Valor del riesgo	5,85
Prioridad de tratamiento	3
Tratamiento del riesgo	
Tipo de actuaciones	b – Información preventiva del mando a – Supervisión preventiva del mando
Fecha límite del tratamiento	< 6 meses
Revisión del tratamiento	< 11 meses

Figura 112 - Ficha de riesgo 12 (elaboración propia).

Ficha del riesgo	
Identificación del riesgo	
ID del riesgo	13
Nombre del riesgo	Manipulación no autorizada de documentos o expedientes
Descripción	Realización de cambios en el contenido o formato de los documentos sin consentimiento, aprobación o permiso previos.
Proceso de gestión documental relacionado	<ul style="list-style-type: none"> • Creación y Captura • Clasificación • Acceso • Almacenamiento • Uso y reutilización • Migración y conversión • Disposición
Análisis del riesgo	
Probabilidad	3
Impacto/Consecuencias	4
Nivel del riesgo	VI – Considerable
Riesgos relacionados	1 - Pérdida de información/documentación 2 - Falta de garantías de integridad 3 - Pérdida de documentos esenciales 6 - Accesos indebidos a información 12 - Ubicación errónea o indebida de documentos 17 - Falta de garantías de trazabilidad 18 - Falta de garantías de autenticidad 19 - Falta de garantías de fiabilidad 26 - Accesos indebidos a las aplicaciones
Evaluación del riesgo	
Valor del riesgo	6,62
Prioridad de tratamiento	2
Tratamiento del riesgo	
Tipo de actuaciones	i – Formación general y específica
Fecha límite del tratamiento	< 3 meses
Revisión del tratamiento	< 11 meses

Figura 113 - Ficha de riesgo 13 (elaboración propia).

Ficha del riesgo	
Identificación del riesgo	
ID del riesgo	14
Nombre del riesgo	Duplicidad documental
Descripción	Creación de varias copias idénticas de un mismo documento.
Proceso de gestión documental relacionado	<ul style="list-style-type: none"> • Creación y Captura • Clasificación • Uso y reutilización • Migración y conversión • Disposición
Análisis del riesgo	
Probabilidad	3
Impacto/Consecuencias	1
Nivel del riesgo	III – Muy leve
Riesgos relacionados	15 - Creación innecesaria de documentos
Evaluación del riesgo	
Valor del riesgo	3,73
Prioridad de tratamiento	4
Tratamiento del riesgo	
Tipo de actuaciones	b – Información preventiva del mando
Fecha límite del tratamiento	< 1 año
Revisión del tratamiento	< 21 meses

Figura 114 - Ficha de riesgo 14 (elaboración propia).

Ficha del riesgo	
Identificación del riesgo	
ID del riesgo	15
Nombre del riesgo	Creación innecesaria de documentos
Descripción	Generación de documentos, sean copias u originales, no requeridos para la gestión de la organización.
Proceso de gestión documental relacionado	<ul style="list-style-type: none"> • Creación y Captura • Clasificación • Almacenamiento • Migración y conversión • Disposición
Análisis del riesgo	
Probabilidad	3
Impacto/Consecuencias	1
Nivel del riesgo	III – Muy leve
Riesgos relacionados	14 – Duplicidad documental
Evaluación del riesgo	
Valor del riesgo	3,48
Prioridad de tratamiento	4
Tratamiento del riesgo	
Tipo de actuaciones	b – Información preventiva del mando
Fecha límite del tratamiento	< 1 año
Revisión del tratamiento	< 21 meses

Figura 115 - Ficha de riesgo 15 (elaboración propia).

Ficha del riesgo	
Identificación del riesgo	
ID del riesgo	16
Nombre del riesgo	Duplicación de instrumentos de gestión documental
Descripción	Desarrollo de varios protocolos o directrices, internos, para un mismo proceso de gestión documental.
Proceso de gestión documental relacionado	<ul style="list-style-type: none"> • Creación y Captura • Clasificación • Acceso • Almacenamiento • Migración y conversión • Disposición
Análisis del riesgo	
Probabilidad	1
Impacto/Consecuencias	4
Nivel del riesgo	IV – Leve
Riesgos relacionados	7 - Eliminación indebida de documentos 11 - No eliminación de documentos 14 - Duplicidad documental
Evaluación del riesgo	
Valor del riesgo	3,48
Prioridad de tratamiento	4
Tratamiento del riesgo	
Tipo de actuaciones	c – Planificación de la prevención por la unidad de trabajo a – Supervisión preventiva del mando
Fecha límite del tratamiento	< 1 año
Revisión del tratamiento	< 21 meses

Figura 116 - Ficha de riesgo 16 (elaboración propia).

Ficha del riesgo	
Identificación del riesgo	
ID del riesgo	17
Nombre del riesgo	Falta de garantías de trazabilidad
Descripción	Incapacidad para asegurar la creación, incorporación y conservación de información (que se incluye en metadatos) sobre la gestión y uso de un documento a lo largo del tiempo en que debe este ser conservado.
Proceso de gestión documental relacionado	<ul style="list-style-type: none"> • Creación y Captura • Clasificación • Acceso • Almacenamiento • Uso y reutilización • Migración y conversión • Disposición
Análisis del riesgo	
Probabilidad	3
Impacto/Consecuencias	5
Nivel del riesgo	VII – Importante
Riesgos relacionados	2 - Falta de garantías de integridad 5 - No recuperación de información/documentación 7 - Eliminación indebida de documentos 9 - Falta de garantías de accesibilidad 13 - Manipulación no autorizada de documentos 18 - Falta de garantías de autenticidad 19 - Falta de garantías de fiabilidad 20 - Errores en la descripción documental
Evaluación del riesgo	
Valor del riesgo	7,30
Prioridad de tratamiento	2
Tratamiento del riesgo	
Tipo de actuaciones	b – Información preventiva del mando i – Formación general y específica a – Supervisión preventiva del mando
Fecha límite del tratamiento	< 3 meses
Revisión del tratamiento	< 7 meses

Figura 117 - Ficha de riesgo 17 (elaboración propia).

Ficha del riesgo	
Identificación del riesgo	
ID del riesgo	18
Nombre del riesgo	Falta de garantías de autenticidad
Descripción	Incapacidad para asegurar la legitimidad y veracidad de un documento a lo largo del tiempo en que debe ser conservado.
Proceso de gestión documental relacionado	<ul style="list-style-type: none"> • Creación y Captura • Clasificación • Acceso • Almacenamiento • Uso y reutilización • Migración y conversión • Disposición
Análisis del riesgo	
Probabilidad	2
Impacto/Consecuencias	5
Nivel del riesgo	VI – Considerable
Riesgos relacionados	2 - Falta de garantías de integridad 6 - Accesos indebidos a información 13 - Manipulación no autorizada de documentos 17 - Falta de garantías de trazabilidad 19 - Falta de garantías de fiabilidad
Evaluación del riesgo	
Valor del riesgo	6,10
Prioridad de tratamiento	2
Tratamiento del riesgo	
Tipo de actuaciones	b – Información preventiva del mando i – Formación general y específica a – Supervisión preventiva del mando
Fecha límite del tratamiento	< 3 meses
Revisión del tratamiento	< 11 meses

Figura 118 - Ficha de riesgo 18 (elaboración propia).

Ficha del riesgo	
Identificación del riesgo	
ID del riesgo	19
Nombre del riesgo	Falta de garantías de fiabilidad
Descripción	Incapacidad para asegurar la confiabilidad de un documento a lo largo del tiempo en que debe ser conservado.
Proceso de gestión documental relacionado	<ul style="list-style-type: none"> • Creación y Captura • Clasificación • Acceso • Almacenamiento • Uso y reutilización • Migración y conversión • Disposición
Análisis del riesgo	
Probabilidad	2
Impacto/Consecuencias	5
Nivel del riesgo	VI – Considerable
Riesgos relacionados	2 -Falta de garantías de integridad 13 - Manipulación no autorizada de documentos 17 - Falta de garantías de trazabilidad 18 - Falta de garantías de autenticidad
Evaluación del riesgo	
Valor del riesgo	6,10
Prioridad de tratamiento	2
Tratamiento del riesgo	
Tipo de actuaciones	b – Información preventiva del mando i – Formación general y específica a – Supervisión preventiva del mando
Fecha límite del tratamiento	< 3 meses
Revisión del tratamiento	< 11 meses

Figura 119 - Ficha de riesgo 19 (elaboración propia).

Ficha del riesgo	
Identificación del riesgo	
ID del riesgo	20
Nombre del riesgo	Errores en la descripción documental
Descripción	Fallos e incidencias a la hora de incluir información sobre el contexto, contenido y estructura de los documentos.
Proceso de gestión documental relacionado	<ul style="list-style-type: none"> • Creación y Captura • Clasificación • Acceso • Almacenamiento
Análisis del riesgo	
Probabilidad	2
Impacto/Consecuencias	3
Nivel del riesgo	IV – Leve
Riesgos relacionados	1 - Pérdida de información/documentación 3 - Pérdida de documentos esenciales 5 - No recuperación de información/documentación 6 - Accesos indebidos a información 7 - Eliminación indebida de documentos 10 - Falta de garantías de usabilidad 11 - No eliminación de documentos 12 - Ubicación errónea o indebida de documentos 17 - Falta de garantías de trazabilidad 19 - Falta de garantías de fiabilidad
Evaluación del riesgo	
Valor del riesgo	5,98
Prioridad de tratamiento	3
Tratamiento del riesgo	
Tipo de actuaciones	b – Información preventiva del mando i – Formación general y específica
Fecha límite del tratamiento	< 6 meses
Revisión del tratamiento	< 15 meses

Figura 120 - Ficha de riesgo 20 (elaboración propia).

Ficha del riesgo	
Identificación del riesgo	
ID del riesgo	21
Nombre del riesgo	Desarrollo no controlado de aplicaciones
Descripción	Creación de distintos aplicativos informáticos para realizar las mismas funciones o muy similares, en relación a la gestión de documentos.
Proceso de gestión documental relacionado	<ul style="list-style-type: none"> • Creación y Captura • Clasificación • Acceso • Uso y reutilización • Migración y conversión • Disposición
Análisis del riesgo	
Probabilidad	1
Impacto/Consecuencias	4
Nivel del riesgo	IV – Leve
Riesgos relacionados	5 - No recuperación de información/documentación 10 - Falta de garantías de usabilidad 12 - Ubicación errónea o indebida de documentos 17 - Falta de garantías de trazabilidad 22 - Falta de interoperabilidad 24 - Infraestructura insuficiente 26 - Accesos indebidos a las aplicaciones 27 - Incapacidad para acceder a las aplicaciones
Evaluación del riesgo	
Valor del riesgo	5,43
Prioridad de tratamiento	3
Tratamiento del riesgo	
Tipo de actuaciones	l – Desarrollo de instrumentos para la prevención c – Planificación de la prevención por la unidad de trabajo
Fecha límite del tratamiento	< 6 meses
Revisión del tratamiento	< 21 meses

Figura 121 - Ficha de riesgo 21 (elaboración propia).

Ficha del riesgo	
Identificación del riesgo	
ID del riesgo	22
Nombre del riesgo	Falta de interoperabilidad
Descripción	Incapacidad para compartir datos y posibilitar el intercambio de información entre departamentos o entre organizaciones.
Proceso de gestión documental relacionado	<ul style="list-style-type: none"> • Creación y Captura • Clasificación • Acceso • Almacenamiento • Uso y reutilización • Migración y conversión • Disposición
Análisis del riesgo	
Probabilidad	3
Impacto/Consecuencias	4
Nivel del riesgo	VI – Considerable
Riesgos relacionados	5 - No recuperación de información/documentación 9 - Falta de garantías de accesibilidad 14 - Duplicidad documental 24 - Infraestructura insuficiente
Evaluación del riesgo	
Valor del riesgo	4,70
Prioridad de tratamiento	3
Tratamiento del riesgo	
Tipo de actuaciones	a – Supervisión preventiva del mando c – Planificación de la prevención por la unidad de trabajo
Fecha límite del tratamiento	< 6 meses
Revisión del tratamiento	< 15 meses

Figura 122 - Ficha de riesgo 22 (elaboración propia).

Ficha del riesgo	
Identificación del riesgo	
ID del riesgo	23
Nombre del riesgo	Falta de respuesta ante fallos del sistema
Descripción	Incapacidad de la organización de actuar frente a incidencias en las aplicaciones informáticas de gestión documental.
Proceso de gestión documental relacionado	<ul style="list-style-type: none"> • Creación y Captura • Clasificación • Acceso • Almacenamiento • Uso y reutilización • Migración y conversión • Disposición
Análisis del riesgo	
Probabilidad	1
Impacto/Consecuencias	2
Nivel del riesgo	II – Extremadamente leve
Riesgos relacionados	1 - Pérdida de información 5 - No recuperación de información/documentación 17 - Falta de garantías de trazabilidad 24 - Infraestructura insuficiente 27 - Incapacidad para acceder a las aplicaciones
Evaluación del riesgo	
Valor del riesgo	5,20
Prioridad de tratamiento	3
Tratamiento del riesgo	
Tipo de actuaciones	b – Información preventiva del mando i – Formación general y específica a – Supervisión preventiva del mando
Fecha límite del tratamiento	< 6 meses
Revisión del tratamiento	< 21 meses

Figura 123 - Ficha de riesgo 23 (elaboración propia).

Ficha del riesgo	
Identificación del riesgo	
ID del riesgo	24
Nombre del riesgo	Infraestructura insuficiente
Descripción	No disponer de los elementos necesarios para el correcto desempeño de los procesos de gestión documental en la organización.
Proceso de gestión documental relacionado	<ul style="list-style-type: none"> • Creación y Captura • Clasificación • Acceso • Almacenamiento • Uso y reutilización • Migración y conversión • Disposición
Análisis del riesgo	
Probabilidad	1
Impacto/Consecuencias	4
Nivel del riesgo	IV – Leve
Riesgos relacionados	5 - No recuperación de información/documentación 10 - Falta de garantías de usabilidad 22 - Falta de interoperabilidad 23 - Falta de respuesta ante fallos del sistema 25 - Interrupción de la actividad 27 - Incapacidad para acceder a las aplicaciones
Evaluación del riesgo	
Valor del riesgo	5,20
Prioridad de tratamiento	3
Tratamiento del riesgo	
Tipo de actuaciones	l – Desarrollo de instrumentos para la prevención c – Planificación de la prevención por la unidad de trabajo h – Mantenimiento de locales
Fecha límite del tratamiento	< 6 meses
Revisión del tratamiento	< 21 meses

Figura 124 - Ficha de riesgo 24 (elaboración propia).

Ficha del riesgo	
Identificación del riesgo	
ID del riesgo	25
Nombre del riesgo	Interrupción de la actividad
Descripción	Suspensión temporal del funcionamiento de las aplicaciones de gestión documental de la organización.
Proceso de gestión documental relacionado	<ul style="list-style-type: none"> • Creación y Captura • Clasificación • Acceso • Almacenamiento • Uso y reutilización • Migración y conversión • Disposición
Análisis del riesgo	
Probabilidad	1
Impacto/Consecuencias	2
Nivel del riesgo	II – Extremadamente leve
Riesgos relacionados	1 - Pérdida de información/documentación 4 - No creación de evidencias documentales 5 - No recuperación de información/documentación 9 - Falta de garantías de accesibilidad 17 - Falta de garantías de trazabilidad 23 - Falta de respuesta ante fallos del sistema 24 - Infraestructura insuficiente 27 - Incapacidad para acceder a las aplicaciones
Evaluación del riesgo	
Valor del riesgo	6,10
Prioridad de tratamiento	2
Tratamiento del riesgo	
Tipo de actuaciones	b – Información preventiva del mando i – Formación general y específica
Fecha límite del tratamiento	< 3 meses
Revisión del tratamiento	< 15 meses

Figura 125 - Ficha de riesgo 25 (elaboración propia).

Ficha del riesgo	
Identificación del riesgo	
ID del riesgo	26
Nombre del riesgo	Accesos indebidos a las aplicaciones
Descripción	Entrada a las aplicaciones de gestión documental sin disponer de permiso o autorización para ello.
Proceso de gestión documental relacionado	<ul style="list-style-type: none"> • Creación y Captura • Clasificación • Acceso • Almacenamiento • Uso y reutilización • Migración y conversión • Disposición
Análisis del riesgo	
Probabilidad	3
Impacto/Consecuencias	2
Nivel del riesgo	IV – Leve
Riesgos relacionados	1 - Pérdida de información/documentación 2 - Falta de garantías de integridad 3 - Pérdida de documentos esenciales 6 - Accesos indebidos a información 7 - Eliminación indebida de documentos 8 - Sustracción o robo de documentos 13 - Manipulación no autorizada de documentos 17 - Falta de garantías de trazabilidad 19 - Falta de garantías de fiabilidad
Evaluación del riesgo	
Valor del riesgo	7,35
Prioridad de tratamiento	2
Tratamiento del riesgo	
Tipo de actuaciones	i – Formación general y específica a – Supervisión preventiva del mando
Fecha límite del tratamiento	< 3 meses
Revisión del tratamiento	< 15 meses

Figura 126 - Ficha de riesgo 26 (elaboración propia).

Ficha del riesgo	
Identificación del riesgo	
ID del riesgo	27
Nombre del riesgo	Incapacidad para acceder a las aplicaciones
Descripción	Imposibilidad de entrada a las aplicaciones informáticas que permiten la gestión de documentos.
Proceso de gestión documental relacionado	<ul style="list-style-type: none"> • Creación y Captura • Clasificación • Acceso • Almacenamiento • Uso y reutilización • Migración y conversión • Disposición
Análisis del riesgo	
Probabilidad	1
Impacto/Consecuencias	1
Nivel del riesgo	I – Irrelevante
Riesgos relacionados	4 - No creación de evidencias documentales 5 - No recuperación de información/documentación 8 - Sustracción o robo de documentos 10 - Falta de garantías de usabilidad 24 - Infraestructura insuficiente 25 - Interrupción de la actividad
Evaluación del riesgo	
Valor del riesgo	5,20
Prioridad de tratamiento	3
Tratamiento del riesgo	
Tipo de actuaciones	b – Información preventiva del mando c – Planificación de la prevención por la unidad de trabajo
Fecha límite del tratamiento	< 6 meses
Revisión del tratamiento	< 21 meses

Figura 127 - Ficha de riesgo 27 (elaboración propia).

La documentación en fichas de la información obtenida en las distintas fases del proceso de gestión del riesgo permite a los responsables de la gestión de riesgos documentales tener, en un espacio reducido, una gran cantidad de información. El objetivo es servir de apoyo a la organización para conseguir una mejor gestión de sus riesgos.

Se considera muy positiva y funcional la estructura siguiendo las distintas fases del proceso de gestión del riesgo, por resultar de utilidad desde el principio de dicho proceso. Pese a que la información se incluye a medida que se avanza por las etapas, desde un buen inicio se dispone de un documento recopilatorio en el que consultar de un vistazo aquella información que se considera de vital importancia para la gestión del riesgo.

Del mismo modo, las fichas deben servir a la organización en los procesos de revisión y seguimiento, como un instrumento más de la gestión del riesgo. La Organización X no disponía de este tipo de herramienta, con lo que se incorpora como una novedad con los pros y contras que esto supone. Cabrá esperar a la evolución del proceso de revisión para poder analizar los resultados de esta incorporación.

5.6.1 Visualización de los datos

La realización de las fichas documentales de cada riesgo permite poner en relación unos riesgos con otros a partir del apartado de “riesgos relacionados”. Para poder visualizar estas relaciones se realiza un mapa de nodos. Se utiliza la herramienta “onodo”⁸⁶, disponible a través de internet. Esta herramienta es una aplicación web que permite, entre otras cosas, realizar tablas de relaciones entre nodos, establecer tipologías de nodos y establecer tipologías de relaciones, que es lo que se hizo para este estudio de caso.

En el mapa (ver Figura 128), los riesgos se identifican con el número asignado en el proceso de identificación. El tamaño de los nodos (riesgos) aumenta o disminuye en función del número de relaciones que estos tengan entre sí. Por tanto, a mayor tamaño del nodo (riesgo) mayor número de relaciones de este con otros riesgos identificados en la Organización X. Esta figura permite tener una visión global de las relaciones entre los riesgos identificados.

⁸⁶ – La herramienta es accesible a través del siguiente enlace: <https://onodo.org/> (consultado el 29/04/2018).

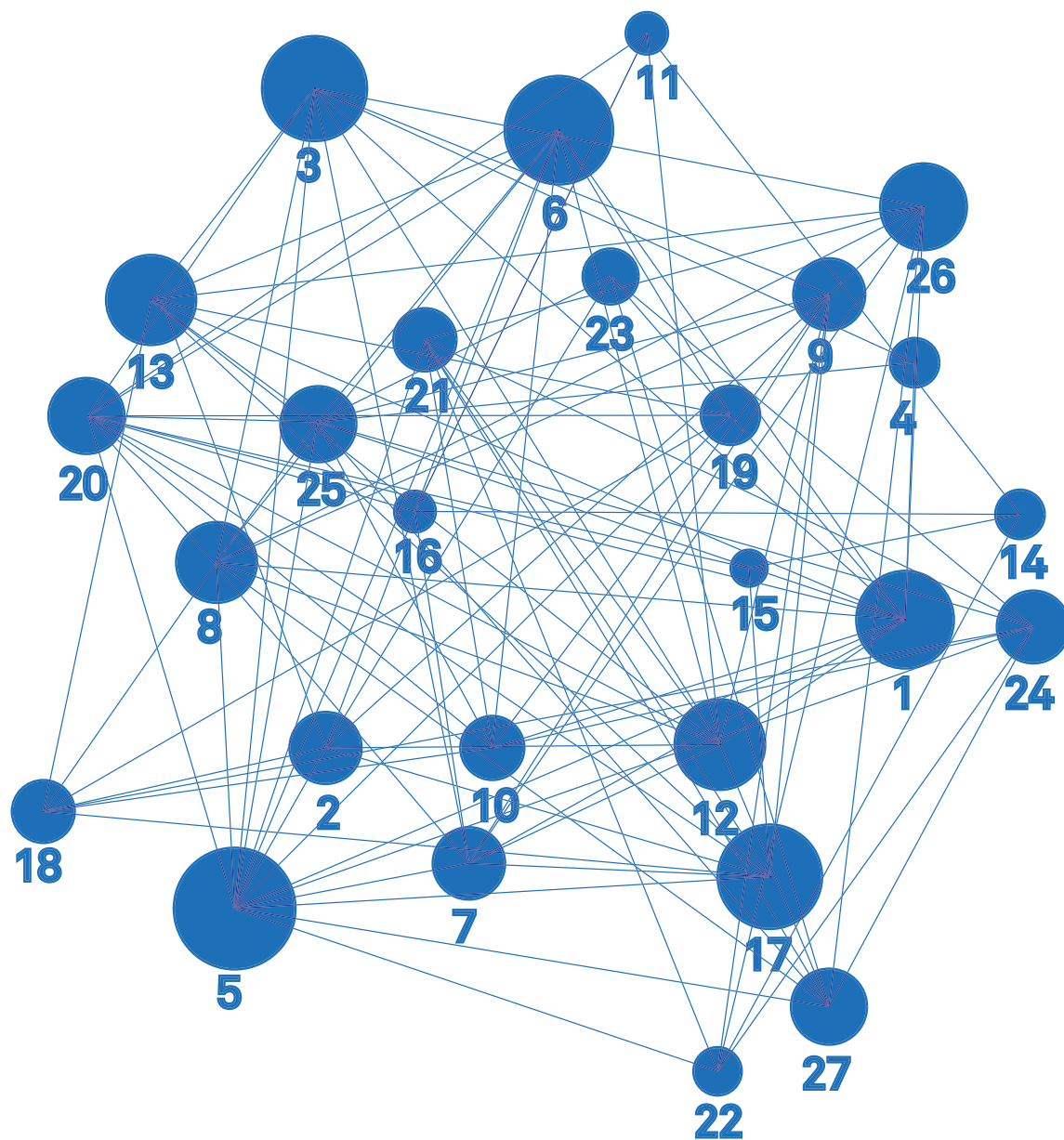
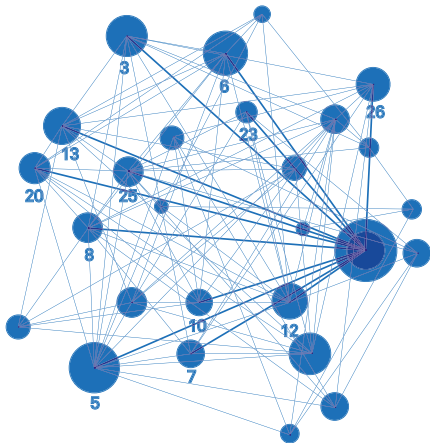


Figura 128 – Mapa de relaciones entre los riesgos documentales identificados en la organización X (elaboración propia).

Lo interesante de este tipo de mapa es poder visualizar las relaciones entre los nodos (riesgos). Es por ello que a continuación se presentan, en distintas figuras, todos los riesgos identificados y sus relaciones con otros riesgos.

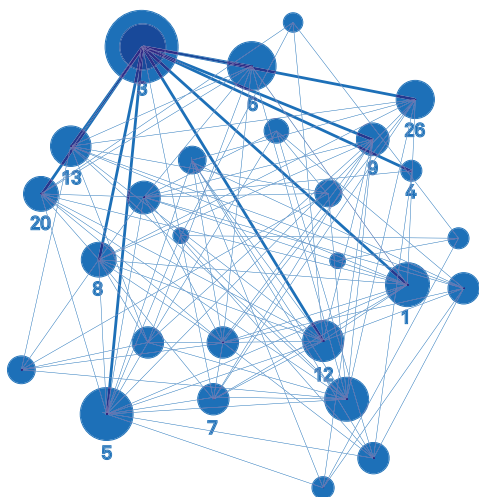
Riesgo 1



Riesgo 2



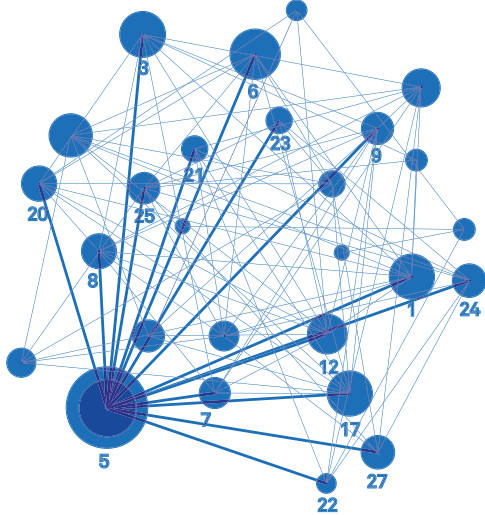
Riesgo 3



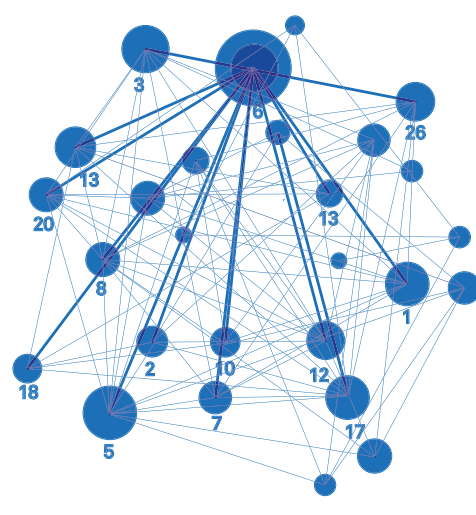
Riesgo 4



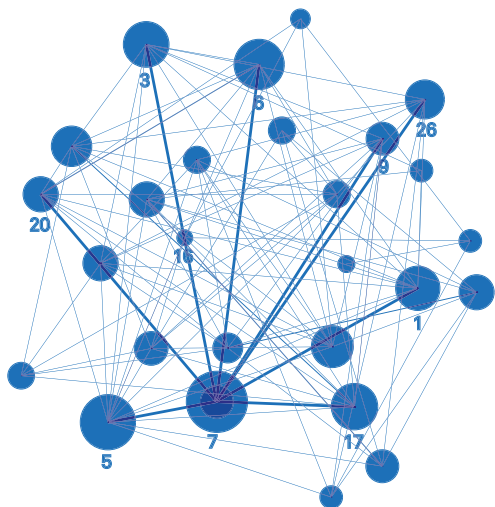
Riesgo 5



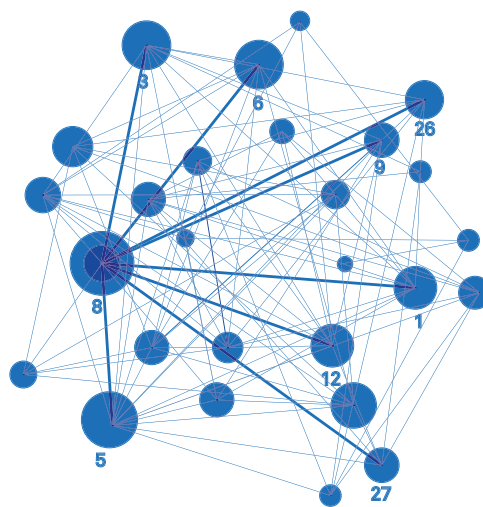
Riesgo 6



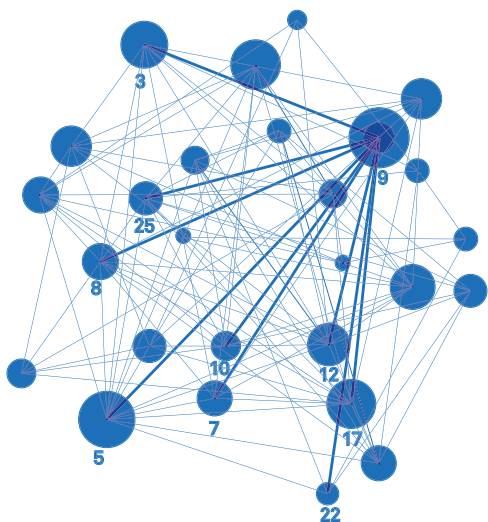
Riesgo 7



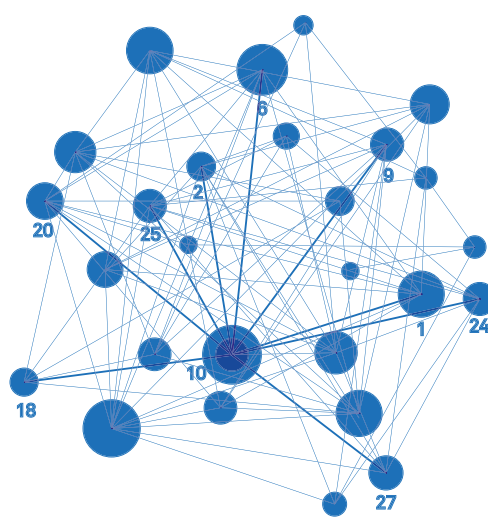
Riesgo 8



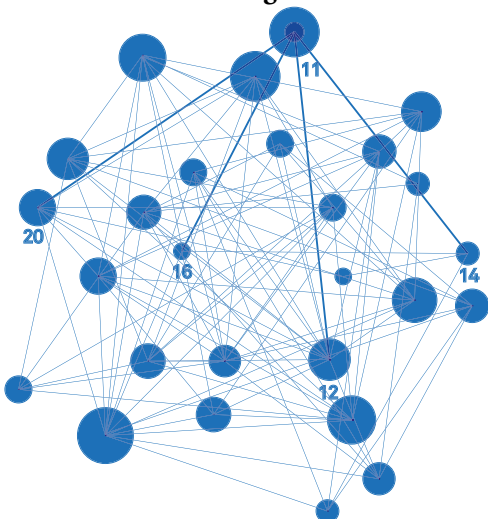
Riesgo 9



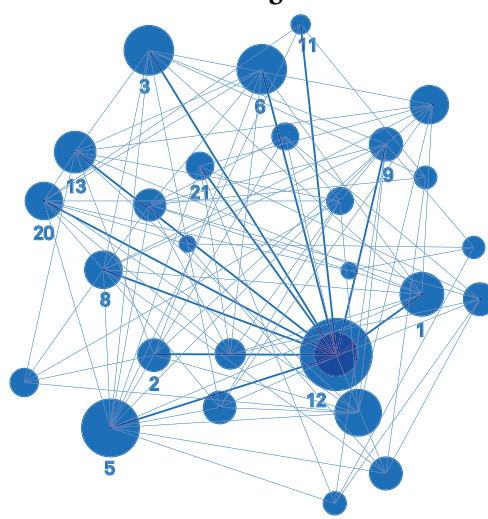
Riesgo 10



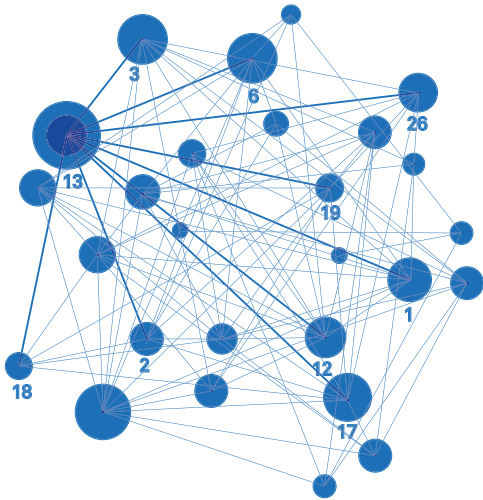
Riesgo 11



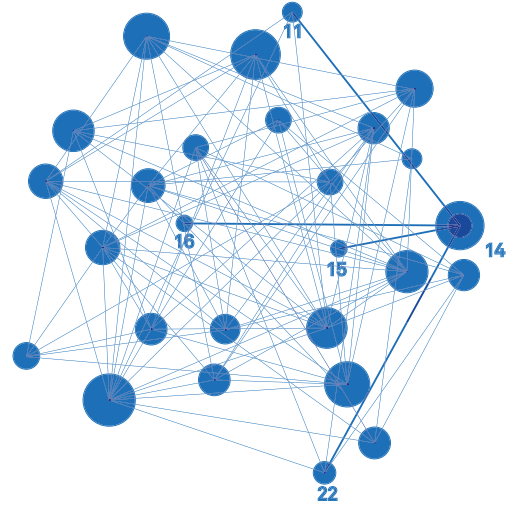
Riesgo 12



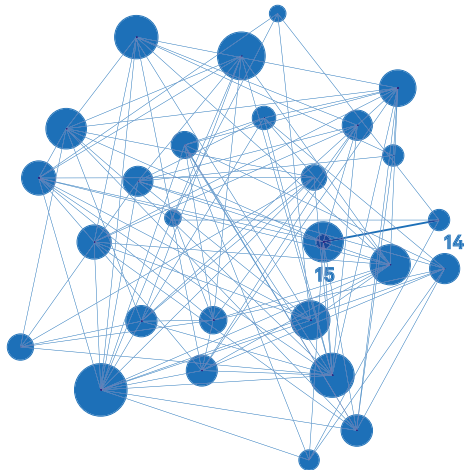
Riesgo 13



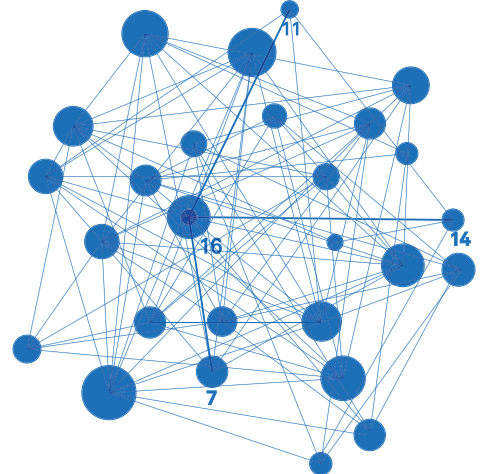
Riesgo 14



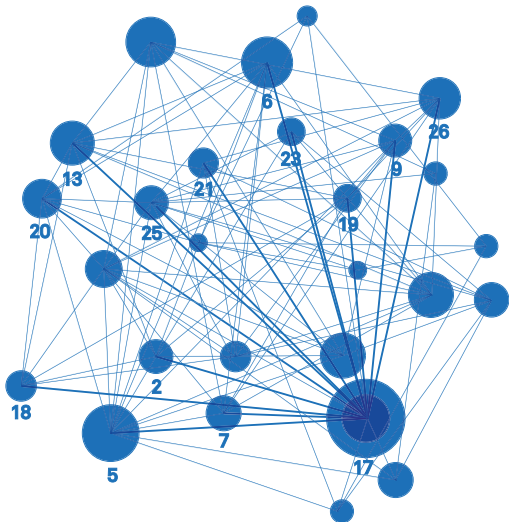
Riesgo 15



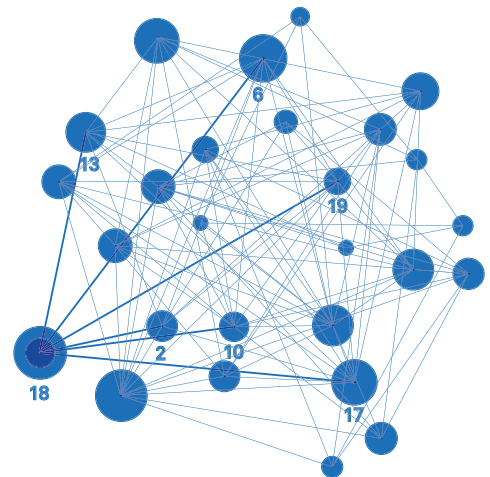
Riesgo 16



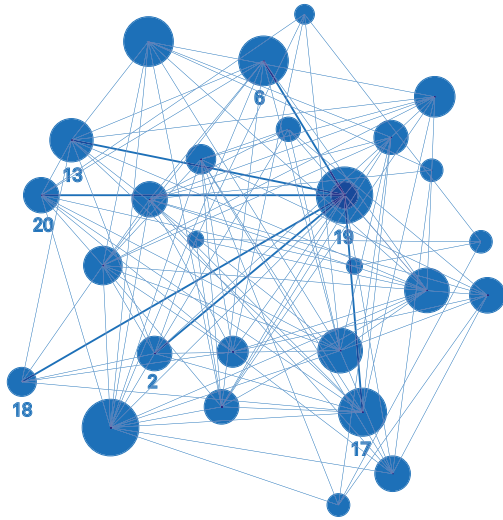
Riesgo 17



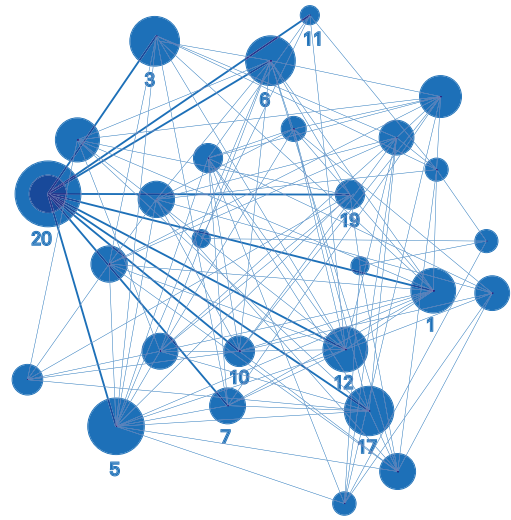
Riesgo 18



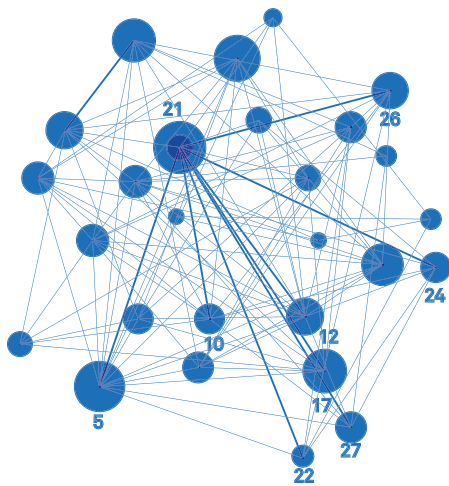
Riesgo 19



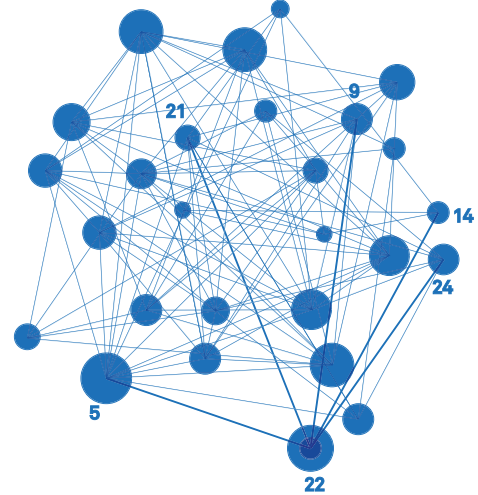
Riesgo 20



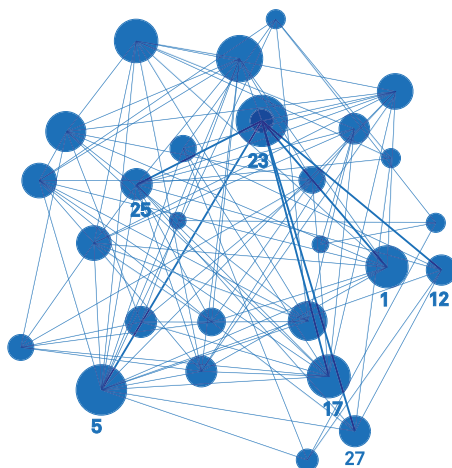
Riesgo 21



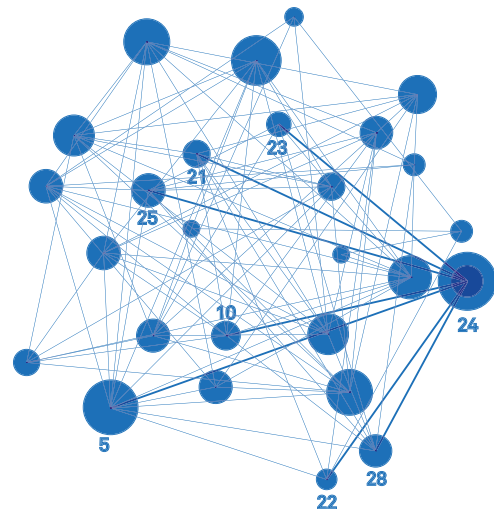
Riesgo 22



Riesgo 23



Riesgo 24



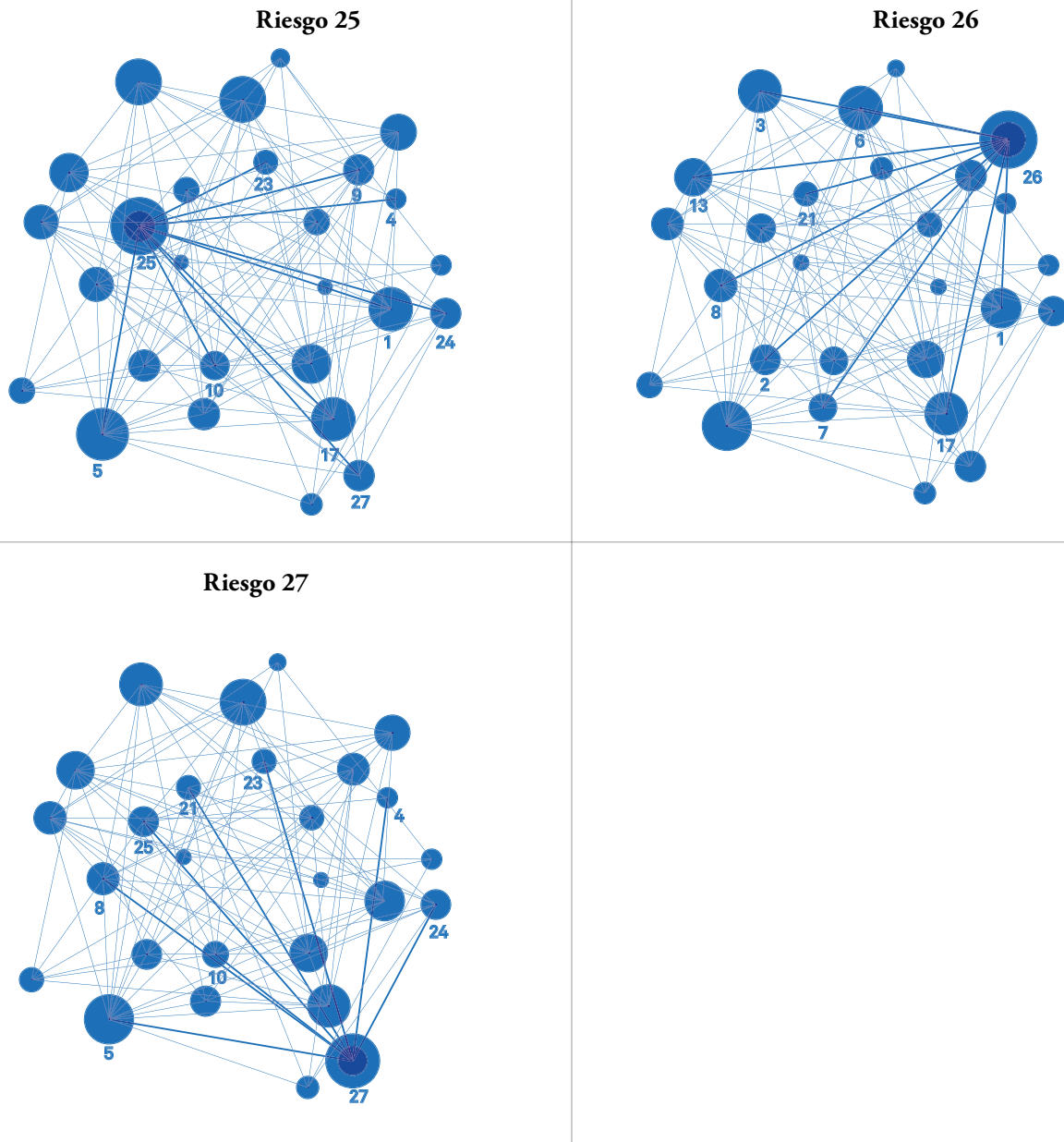


Figura 129 – Visualización de las relaciones entre riesgos (elaboración propia).

La importancia de disponer de herramientas para la visualización de la información radica en la facilidad de comunicación de los resultados, tanto a la alta dirección como a todos aquellos trabajadores involucrados en el proceso. La comunicación del riesgo es parte de una gestión eficaz del riesgo para garantizar a toda la organización el reconocimiento de los mismos (AENOR 2014b, p. 25).

5.7 Valoración y resultados

Este estudio de caso permite trabajar conjuntamente la gestión de riesgos con la gestión de documentos, en una organización real. Se cumple así el primer objetivo propuesto, que pretendía aplicar el proceso de gestión del riesgo a la gestión documental. Se desarrollan las distintas fases de dicho proceso: desde la identificación hasta la propuesta de revisión del tratamiento, pasando por la documentación. Para ello, se aplican distintas metodologías propias de la gestión de riesgos, evidenciando que son perfectamente aplicables al ámbito de la gestión documental y, a su vez, obteniendo resultados que permiten planificar acciones para la prevención y para la mejora del funcionamiento global de la Organización X.

Las mejoras de la gestión documental a través de la gestión de riesgos se evidencian a partir de las propuestas de tratamiento de las situaciones identificadas que pueden derivar en consecuencias negativas. Sin la puesta en práctica del proceso de gestión de riesgos, lo más probable es que estas situaciones de riesgo no se identifiquen y, por tanto, no se traten a tiempo para prevenirlas. De este modo, gracias a las acciones preventivas y al tratamiento de los riesgos se consigue una mejora de la gestión documental, de manera indirecta pero igualmente efectiva. De esto se deduce que la integración de la metodología de gestión de riesgos en la gestión documental conlleva beneficios y mejoras en esta última.

Lo mismo ocurre en sentido inverso, esto es, incluyendo la gestión documental en la gestión de riesgos se perciben mejoras en esta última. Cabe recordar la importancia que dan los estándares internacionales a la documentación del proceso, siendo fundamental disponer de información y evidencias de las diferentes etapas del proceso para una toma de decisiones fundamentada. Es sobre todo en este ámbito en el que la gestión documental contribuye a la mejora de la gestión de riesgos en este estudio. Una adecuada gestión de este tipo de información puede conseguirse mediante la inclusión de procesos e instrumentos de gestión documental en la metodología de gestión de riesgos. De este modo, se facilitará la gestión de las evidencias del proceso permitiendo una mayor efectividad y eficiencia del mismo. Por tanto, la relación entre ambas metodologías es recíprocamente positiva, ambas aportan beneficios y son más eficientes si se trabajan de manera conjunta.

En el caso estudiado, se ha puesto de manifiesto la escasa comunicación entre el área de prevención de riesgos laborales y la de gestión documental y archivo. Esta cuestión es significativa puesto que la segunda necesita de los conocimientos y metodología implantada de la primera para tener éxito en la gestión de riesgos documentales. Al analizar el contexto, se evidencia la existencia de una metodología de gestión de riesgos con cierto recorrido en la Organización X, que se aprovecha en el estudio de caso incluyendo ciertas cuestiones ya trabajadas en el desarrollo del proceso de gestión de riesgos, como por ejemplo las tipologías de acciones de tratamiento. Para poder mantener la gestión de riesgos documentales en la organización, resultará fundamental.

Se cumple el segundo objetivo, demostrando la estrecha vinculación entre una adecuada gestión documental y los procesos de rendición de cuentas. Quizás la mayor evidencia de ello se puede hallar en el análisis de riesgos mediante la técnica de la pajarita, donde se identifican distintas consecuencias de riesgos documentales, dentro de las cuales la mayoritaria es la imposibilidad de rendir cuentas. Con la inclusión de la gestión de riesgos documentales y los mecanismos de prevención implícitos, se consigue aumentar la capacidad de las organizaciones de rendir cuentas y de ser más transparentes, disminuyendo el porcentaje de fallos e incidencias en estos procesos.

En esta misma línea, el estudio de caso evidencia cómo una adecuada gestión documental puede servir como un mecanismo de prevención de riesgos en las organizaciones. Tras el análisis realizado y a partir de los mecanismos preventivos ya existentes en la organización, se ven reducidos los valores de algunos riesgos que tienen consecuencias negativas para la organización más allá de las relacionadas directamente con la gestión de los documentos. Así se reduce la probabilidad de que sucedan y lo mismo ocurre para las consecuencias. Si, además, se ponen en práctica los tratamientos propuestos, con el tiempo se verán aún más reducidas las probabilidades de cada uno de los riesgos identificados. De este modo, se consigue evitar consecuencias negativas en las organizaciones a partir de la mejora de la gestión de documentos.

Este es un argumento de peso para los profesionales de la gestión documental a la hora de presentar resultados y de poder conseguir mayores recursos en las organizaciones. La gestión de documentos no solo afecta a los propios documentos, sino que su adecuada administración repercute de manera general en los objetivos de la organización, en el ahorro de costes, la eficiencia y eficacia en la resolución de trámites, entre otros.

Otra cuestión destacable en el caso estudiado es la percepción de que la mayoría de riesgos documentales identificados pueden ser fácilmente extrapolables a otras organizaciones. Esto es así debido al contexto de transformación digital que se está viviendo en la actualidad a nivel estatal. Lo que no es extrapolable es el análisis y la posterior evaluación de riesgos a partir de los que se determinan los tratamientos, puesto que estas fases sí son específicas en función de cada realidad. Pero desde el punto de vista global, los riesgos identificados pueden coincidir con situaciones que se están viviendo en la mayoría de organismos públicos del país.

Esta percepción puede, con el tiempo, derivar en el desarrollo de un modelo normalizado de gestión de riesgos documentales, más allá de estándares generales centrados en el proceso, y siguiendo lo ya apuntado por Bearman el año 2006 (Bearman 2006, p. 25). Siendo esto posible, se facilitaría enormemente la integración de esta metodología en el día a día de la gestión documental, si bien para ello sería necesario incluir estos aspectos en la formación existente sobre archivística y gestión de documentos. Para ello, antes es necesaria una reflexión previa del colectivo profesional en el contexto estudiado en línea con la evolución de la profesión.

En cualquier caso, como última reflexión, se destaca la percepción positiva que de la gestión de riesgos documentales tienen las personas que han participado activamente en este estudio de caso, por parte de la Organización X. Todas ellas han manifestado en varias ocasiones la voluntad de incorporarla, así como los aspectos positivos que se conseguirían en la corporación si se decidiese trabajar de acuerdo a esta metodología. Entre ellos, se encuentran:

- Mejora en el conocimiento de los factores externos e internos que afectan a la apreciación y al tratamiento de riesgos documentales.
- Mejora en el conocimiento de la metodología de gestión del riesgo y certeza de que esta puede aplicarse a la gestión de los documentos y la información.
- Identificación de los riesgos más relevantes que afectan a la gestión documental de la Organización X y que pueden incidir directamente en la no consecución de sus objetivos.
- Integración de los riesgos documentales en el proceso general de gestión del riesgo de la Organización X.

- Mejora en el trabajo multidisciplinar a la hora de prevenir efectos no deseados.
- Garantía a la hora de disponer de documentos auténticos, íntegros, fiables y accesibles para los casos en que se necesiten en procesos de rendición de cuentas.

El estudio de caso, por tanto, se finaliza con una sensación positiva, si bien cabe tener en cuenta que se trata de un primer paso en el camino de la gestión de riesgos documentales. Serán necesarios estudios similares, de aplicación práctica de la metodología analizada, para obtener más resultados y disponer así de argumentos objetivos para entablar diálogo con los profesionales de la gestión documental.

Conclusiones

Esta investigación planteaba tres hipótesis en su inicio, una general y dos específicas. Para poder demostrarlas, se fijaron una serie de objetivos que se fueron trabajando a medida que se avanzaba en el tiempo. La hipótesis general planteaba que la integración de la metodología de gestión del riesgo en la gestión de documentos podía contribuir de manera indirecta a mejorar los procesos de rendición de cuentas pública. De esta, se derivaban las dos específicas. La primera hipótesis específica planteaba que la gestión documental podía mejorar a través de la integración de la metodología de gestión del riesgo. La segunda hipótesis específica planteaba que la gestión de riesgos podía mejorar a través de la metodología archivística y de gestión documental.

La gestión de documentos en las organizaciones es una práctica transversal al funcionamiento de las mismas. De ella depende, en gran medida, la consecución de los objetivos y el cumplimiento con las obligaciones. Como consecuencia, la integración de la gestión de riesgos en esta práctica influye de manera notable en su desempeño y puede proporcionar mejoras considerables para la organización. Esta integración puede producirse en cualquier momento de la implantación de un sistema de gestión documental, si bien a partir de la experiencia de esta investigación lo más recomendable sería incorporarla desde el principio, o desde las fases iniciales de la implementación. En cualquier caso, puede integrarse en cualquier momento y en cualquier fase. De hecho, el estudio de caso se ha desarrollado sobre una organización con el sistema de gestión documental implantado y en funcionamiento desde hacía unos años y, pese a ello, ha resultado muy provechoso. Lo fundamental es tener presente que, una vez incorporado, el proceso es cíclico y constante, lo que implica revisiones y actualizaciones continuas, que deberán operar conjuntamente con la gestión de los documentos y su ciclo de vida.

Gestionar los riesgos documentales es una manera eficaz de anticiparse a lo que puede salir mal y prevenirlo mediante las acciones de tratamiento. Esto comporta ventajas y mejoras directas en la gestión documental, a partir de la actuación sobre las causas de lo que aún no ha pasado.

Debido a su transversalidad, los riesgos documentales no solo se relacionan con la gestión de documentos, sino que influyen en otros ámbitos organizacionales. Por ejemplo, en la gestión de tecnologías, en el ámbito jurídico, en el desarrollo de procesos o en la gestión de proyectos, entre otros. Prevenirlos y tratarlos, por tanto, repercutirá en ellos, contribuyendo a una mejora global de la gestión en las organizaciones. Además, permitirá un mayor conocimiento sobre los procesos y los instrumentos de gestión documental, sobre cómo se generan los documentos, la gestión del ciclo de vida de los mismos, sobre su acceso o sobre su eliminación, entre otros aspectos, puesto que el análisis de riesgos permite estudiarlos desde una perspectiva distinta y complementaria.

Durante la realización del estudio de caso, se pudo observar que, integrando el proceso de gestión de riesgos en la gestión de documentos, se identificaban debilidades importantes en la organización que podían derivar en consecuencias graves, como, por ejemplo, incumplimientos legales, pérdidas económicas o la falta de garantía de derechos ciudadanos. Por el contrario, sin la aplicación de esta metodología no se habría podido detectar a tiempo estas situaciones y no se habría podido plantear un tratamiento de prevención adecuado. De hecho, estos riesgos no estaban identificados por los responsables de gestión documental ni por los trabajadores entrevistados. Salieron a la luz en la fase de identificación, mediante la aplicación de las técnicas seleccionadas.

De este modo, a través de la prevención se logran mejoras, en algunos casos significativas, al integrar ambas metodologías. Por ejemplo, esto se aprecia analizando algunas de las propuestas de tratamiento que se han planteado para actuar sobre algunas de las causas de riesgo. Se puede observar cómo algunas de ellas consisten, en realidad, en el desarrollo o la actualización de instrumentos de gestión documental. Uno de los ejemplos de este tipo de acciones se encuentra en una de las propuestas de tratamiento de la causa número 1 (accesos no controlados). Se trata del desarrollo de un cuadro de roles y permisos, lo que aumentará el control sobre los accesos a la información, facilitará la trazabilidad sobre los mismos y permitirá disponer de datos fiables para las auditorías de información cuando sea necesario. Otro ejemplo se encuentra en el tratamiento de la causa número 9 (préstamos y consultas no controlados), que incluye, como una de las actuaciones, la revisión y actualización del procedimiento sobre préstamos y consultas de documentación. En este caso, esta actuación facilitará el control y el seguimiento de los accesos internos a la documentación, prevendrá el traslado no autorizado de expedientes y documentos del archivo a las oficinas, así como la inclusión de documentos a expedientes ya cerrados. Otro ejemplo se encuentra en el tratamiento sobre la causa número 14 (falta de requisitos documentales), para la que se deberán definir requisitos para crear y gestionar los documentos a través de los requerimientos legales y de negocio según el contexto. Esta actuación permitirá la generación de documentos con las características necesarias desde el inicio de la tramitación, así como la adaptación a las obligaciones normativas y legales. Estos tres ejemplos de acciones de tratamiento mejoran de manera directa el sistema de gestión documental, a la vez que contribuyen a prevenir riesgos. Se demuestra la primera hipótesis específica y se afirma que la gestión documental mejora a través de la integración de la metodología de gestión del riesgo.

Sin embargo, es importante mencionar que no por el mero hecho de prevenir, siempre se consigue eliminar el riesgo. Lo importante de seguir esta metodología es la disminución de las probabilidades de que ocurra (actuación sobre las causas), así como también el aumento de la capacidad de reacción en caso de ocurrir (actuación sobre las consecuencias). Es posible que muchas organizaciones deban aprender a convivir con múltiples riesgos, lo que no es algo pernicioso si estos han sido correctamente identificados y se mantiene un control y un seguimiento de los mismos. La gestión de riesgos, de hecho, es altamente beneficiosa en este sentido, puesto que permite focalizar la atención donde es realmente necesaria, así como priorizar la inversión de tiempo y dinero. Además, es una metodología completamente alineada con la mejora continua. También cabe destacar que permite identificar errores y fallos del sistema a partir de la detección de situaciones de riesgo para la organización. Por tanto, no implica solo prevención, sino que también ayuda a la detección precoz de problemáticas que podrían derivar en graves consecuencias, permitiendo su corrección inmediata.

En el estudio de caso también se ha trabajado la incorporación de la metodología de gestión documental al proceso de gestión de riesgos. Se ha podido apreciar la importancia que cobra disponer de información actualizada y accesible en el momento en que se necesita para tomar las decisiones. Por ejemplo, a la hora de priorizar las acciones de tratamiento, resultó de vital importancia disponer de la información obtenida en el análisis y la evaluación de riesgos. En este caso, no solo se necesitaba dicha información, sino que era importante que esta estuviese estructurada de manera que se pudiese recuperar fácilmente para trabajar con ella. Otro instrumento documental útil para la organización fueron las fichas de riesgos, donde quedó compilada toda la información relevante sobre cada uno de los riesgos documentales identificados, con la finalidad de realizar el seguimiento a lo largo del tiempo. La adecuada gestión de esta documentación resulta esencial a la hora de implantar la gestión de riesgos en cualquier organización. Tener en cuenta la metodología de gestión documental e integrarla en el funcionamiento de dicho proceso mejora de manera notable su desarrollo.

Asimismo, la documentación resulta igualmente eficaz para el intercambio de información con todas aquellas partes interesadas en el proceso, sean internas o externas. Documentar, y poder recuperar evidencias sobre reuniones, decisiones, análisis y evaluaciones de riesgos o sus tratamientos, ha facilitado enormemente la comunicación entre quien ha implementado la gestión de riesgos documentales y los profesionales involucrados de la organización estudiada. Además, la documentación de las distintas fases del proceso permite, a su vez, realizar el seguimiento de la implementación de las acciones de tratamiento, así como de la evolución de los niveles y valores de los riesgos a lo largo del tiempo. Por tanto, se demuestra la segunda hipótesis específica y se afirma que la gestión de riesgos mejora a través de la metodología archivística y de gestión documental.

Estas metodologías, por tanto, resultan complementarias. A través del trabajo realizado en la investigación, se considera que la gestión de riesgos documentales puede llevarse a cabo en cualquier organización, disponga de un sistema de gestión documental implantado o no. Los beneficios obtenidos en ambos casos probablemente no serán similares, debido a que el punto de partida no es el mismo. En organizaciones con una cierta trayectoria en la gestión de documentos, seguramente se obtendrán mejoras de su sistema y principalmente se llevarán a cabo actuaciones de tipo preventivo. En cambio, en organizaciones sin una gestión documental sistematizada, se obtendrá información sobre las carencias existentes que deberá servir para fijar los objetivos documentales a corto y medio plazo. En este caso, pese a incluir también cuestiones preventivas concretas, la gestión de riesgos documentales permitirá obtener una perspectiva global en relación con la necesidad de disponer de un sistema de gestión documental como un método de prevención de otro tipo de riesgos y consecuencias para la organización. Como se puede apreciar, la funcionalidad de una misma metodología puede aportar resultados distintos dependiendo de la madurez documental de cada organización.

Además, ambas metodologías pueden integrarse con mucha facilidad en otros sistemas de gestión, como, por ejemplo, sistemas de gestión de la calidad, de medio ambiente o de prevención de riesgos laborales, entre otros. De hecho, la gestión de riesgos documentales puede emplear la misma metodología que la gestión de riesgos laborales, tal y como se ha demostrado en el desarrollo del estudio de caso llevado a cabo en la Organización X. En algunas de las fases se ha empleado, exactamente, la misma metodología que la ya definida en la organización para la prevención de riesgos laborales, quedando patente que es posible esta complementariedad. La integración comporta una facilidad mayor para incluir los riesgos documentales en la gestión diaria de cualquier organismo, ampliando las posibilidades de prevención.

Una cuestión a destacar es que todas estas cuestiones son extrapolables a las organizaciones privadas, que también pueden beneficiarse de la integración de estas metodologías. Todos los organismos generan información y documentos, que deben gestionarse y controlarse. En la medida en que esto es así, será igualmente beneficioso incorporar la gestión de los riesgos documentales, que servirá como una oportunidad de mejora y prevención.

De las dos demostraciones anteriores se concluye que la integración de estas metodologías aporta beneficios destacables a ambas. Trabajarlas conjuntamente es el marco ideal, ya no solo en relación con la gestión de riesgos específicamente documentales, sino aplicando esta fusión a la gestión de riesgos, sean estos del tipo que sean. Esta complementariedad sería la idónea para una gestión eficiente en las organizaciones.

Otra cuestión que se ha puesto de manifiesto en esta investigación, sobre todo en el desarrollo del estudio de caso, es la estrecha relación entre la gestión de documentos y los procesos de rendición de cuentas. Se realiza una aproximación teórica al tema en el capítulo 3 de esta investigación, pero, al estudiar un caso real, se ha hecho

patente que sin una óptima gestión de los documentos no es posible dar respuesta adecuada a las obligaciones de rendición de cuentas en las administraciones públicas. Estos procesos se basan en la existencia de evidencias sobre las decisiones o actuaciones llevadas a cabo, para poder estudiarlas, debatir sobre ellas y juzgarlas. Además, el proceso debe documentarse y debe poder ser accesible cuando se requiera. Sin evidencias, por tanto, no puede haber rendición de cuentas. En cambio, con una gestión adecuada de la información y los documentos es posible rendir cuentas y hacerlo de manera confiable.

Esta relación también se puso de manifiesto en los *Focus Groups*, en los que se mostraron de acuerdo la mayoría de los participantes. Un 70 % de ellos afirmaba que existía una relación (fuese directa o indirecta) entre la gestión documental y la rendición de cuentas pública. Además, se consideraba un valor añadido incluir la gestión de riesgos documentales como un medio para el aumento de la confianza en la información.

Sin embargo, esto no quiere decir que por el mero hecho de disponer de documentos y de gestionarlos de manera adecuada se produzca la rendición de cuentas. Tal y como afirma Hood, el auge de la transparencia conlleva cambios en los requisitos legales, afectando a la desclasificación y a la gestión documental, pero no necesariamente es la base o sustenta cambios en el comportamiento o en los valores y creencias (Hood 2006a, p. 214). Que se dé la transparencia y que se lleven a cabo procesos de rendición de cuentas depende mayoritariamente de la voluntad política, no solo de las leyes o de la correcta gestión pública.

En cualquier caso, sí ha quedado demostrado que la gestión documental facilita y aumenta la capacidad de las administraciones públicas de rendir cuentas de manera ágil y a través de documentos íntegros. Esto se constata, sobre todo, en la etapa de análisis de riesgos del estudio de caso. En esta fase se identificaron distintas consecuencias posibles de los riesgos documentales, siendo la más recurrente y duplicando el valor medio de recurrencia, la imposibilidad de rendir cuentas. Este resultado pone de manifiesto lo expuesto anteriormente y permite demostrar que la gestión de documentos puede facilitar la rendición de cuentas. Si, además, se añade la gestión de riesgos documentales como parte de una gestión documental optimizada, teniendo en cuenta que la integración de ambas las mejora y permite aumentar el éxito de los procesos relacionados, se demuestra la hipótesis general de esta investigación. Se puede afirmar entonces que la integración de la metodología de gestión del riesgo en la gestión de documentos puede contribuir de manera indirecta a mejorar los procesos de rendición de cuentas pública.

Esta contribución se refiere sobre todo al aumento de la capacidad de los organismos públicos de llevar a cabo estos procesos de manera eficiente, eficaz y con información confiable. Cabe destacar que las mejoras son indirectas, puesto que no se trata de acciones que incidan directamente en los procesos de rendición de cuentas, sino que actúan sobre los procesos e instrumentos relacionados como, por ejemplo, la gestión de documentos.

De todo lo anterior se deduce que los tres ámbitos de estudio de esta investigación (gestión documental, gestión de riesgos y rendición de cuentas) trabajados de manera conjunta se refuerzan y se mejoran. Por lo tanto, la integración de estos procesos en las administraciones públicas puede aportar grandes beneficios de manera global. En la Figura 130 se aprecia cómo, a partir de la inclusión de la gestión de riesgos documentales en los sistemas de gestión documental, se dan afectaciones, en este caso positivas, tanto sobre la información y los documentos como sobre la transparencia de las administraciones públicas. Estas interrelaciones resultan en tres grandes beneficios, que son la mejora de la gestión documental, la mejora de la gestión de riesgos y la posibilidad de una rendición de cuentas confiable.

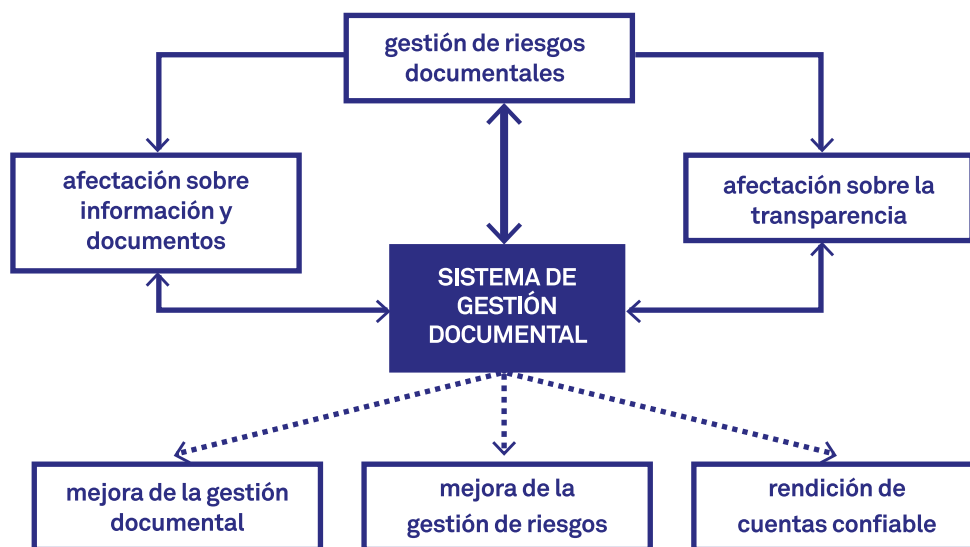


Figura 130 - Aportaciones de la gestión de riesgos documentales (elaboración propia).

Aportaciones de la investigación

A continuación, se explican las aportaciones de esta investigación para la archivística y la gestión documental, así como para los profesionales de este ámbito y perfiles afines.

1. Reposicionamiento de la gestión documental en las organizaciones.

La integración de la gestión de riesgos documentales en las organizaciones, sean públicas o privadas, permite reposicionar a la gestión documental y entenderla como algo esencial para el correcto funcionamiento de las mismas. Este planteamiento, que puede parecer normalizado en la actualidad, en realidad no suele ser habitual. En muchos casos, la gestión de documentos se desarrolla de un modo marginal y sectorial, siendo percibida más como un estorbo que como una oportunidad. Introducir soluciones a problemas concretos a través de la identificación de riesgos documentales ayuda a cambiar esta percepción y posiciona la gestión de documentos como una herramienta básica de prevención. Esta podría evitar, según los resultados del estudio de caso, consecuencias negativas como pueden ser, entre otras, pérdida de prestigio, incumplimientos legales, pérdida de litigios, filtraciones de información, pérdidas económicas o incumplimiento de objetivos. De este modo, la gestión de documentos se percibe como un instrumento para la prevención de riesgos en las organizaciones y se convierte en una oportunidad para la mejora del desempeño.

2. Potencial del lenguaje de riesgos para los profesionales de la gestión documental

Otro aspecto a considerar, relacionado con esta oportunidad, es el potencial que tiene el uso del lenguaje de riesgos para los profesionales de la gestión documental. Incluye términos y conceptos que los altos mandos y la dirección comprenden fácilmente. Introducirlo en su día a día, a través de la gestión de riesgos documentales, fortalece

la idea de la importancia de mejorar la gestión de documentos, con el valor añadido de evitar efectos perjudiciales para la organización. Además, emplear un lenguaje distinto al habitual de la archivística, pero complementario, permite hacerse entender entre perfiles que no tienen por qué conocer esta terminología. Esto favorece la comprensión de las necesidades de gestión documental y ayuda a su mejor posicionamiento, así como también al de los profesionales dentro de las organizaciones y dentro de la sociedad en general.

De hecho, en el desarrollo de los *Focus Groups* se apreció claramente cómo los participantes finalizaron los debates mucho más concienciados sobre la importancia de la gestión de riesgos documentales que al inicio de la conversación. No se había planteado como uno de los objetivos al preparar los debates y, sin embargo, ocurrió en ambos casos. Es un hecho remarcable y que pone de manifiesto la fuerza de la terminología, pero también la importancia del ámbito de estudio. Se habló de situaciones que habían desembocado en consecuencias negativas, se habló de prevención, de problemáticas diversas, pero, sobre todo, de buscar soluciones desde la gestión de los documentos.

Se considera fundamental dar conocimiento de estas posibilidades a los profesionales, ya que la incorporación de la gestión de riesgos a su quehacer les permite trabajar la gestión de la información y los documentos a nivel estratégico y de manera transversal, desde una óptica distinta a las habituales. Esta versatilidad puede contribuir a su reposicionamiento dentro de las organizaciones, dando mayor protagonismo a su función.

3. Adquisición de nuevas competencias y capacitación

El potencial existe, pero es necesario saber explotarlo y, para ello, se necesita capacitación. La gestión de riesgos documentales es un ámbito poco explorado y estudiado. Tal y como se ha comentado en el capítulo 4, y como se ha podido observar a través de las percepciones de los profesionales que participaron en los *Focus Groups*, la formación resulta fundamental para poder materializar este cambio de visión. Cabría plantearse si se está ante un nuevo perfil o si, por el contrario, tan solo es necesario incorporar esta metodología en los planes de estudio o en los cursos de especialización. Sea como fuere, se necesita mucha formación y, también, concienciación. Según los participantes en los debates llevados a cabo en esta investigación, se abre un campo de trabajo que permite ir más allá de lo tradicional y que llevará a los profesionales fuera de su zona de confort. Será necesario analizar este cambio de paradigma en el futuro más inmediato, lo que puede abrir nuevas líneas de investigación.

Los profesionales de la archivística y la gestión de documentos disponen de competencias y habilidades que les hacen únicos a la hora de realizar el proceso de gestión de riesgos documentales, debido al gran conocimiento que tienen de los documentos y la información en sus organizaciones, así como de la comprensión de los instrumentos y los procesos de la gestión documental que pueden contribuir a la prevención de los riesgos documentales. La causa principal de que este modo de trabajar no se esté implementando por estos profesionales es su desconocimiento. Ha quedado demostrado en el capítulo 4 que el tema interesa mucho. Prueba de ello son las sensaciones positivas y las ganas, por parte de los participantes en los debates llevados a cabo, de poner en práctica la metodología del 100%. Todos ellos se mostraban convencidos de que les aportaría beneficios y de que resultaba un instrumento útil y funcional para sus organizaciones. Les faltaba capacitación. Esta deberá tener un doble objetivo. En primer lugar, ampliar las competencias de los gestores de documentos y su ámbito de conocimiento y, en segundo lugar, servir como medida de difusión para dar a conocer las posibilidades que ofrece la integración de estas metodologías.

4. Empoderamiento de los profesionales de la gestión documental

Como factor añadido, la formación debe contribuir al empoderamiento de los archiveros y gestores de documentos mediante la ampliación de conocimientos y aptitudes. Se necesitará una inversión en la formación continua, el reciclaje y la actualización de las competencias adquiridas. En esta línea, cabe mencionar la importancia de la motivación y la proactividad entre los profesionales, ya que no es posible evolucionar si no hay una cierta voluntad como punto de partida. En cualquier caso, a partir de los resultados obtenidos en el capítulo 4, se destaca esta percepción de oportunidad y reposicionamiento profesional, añadiendo el optimismo a la ecuación. Este empoderamiento se consigue también gracias al reposicionamiento de la gestión documental en las organizaciones.

5. Afianzamiento de la gestión documental en las organizaciones

Otra oportunidad que aporta la gestión de riesgos documentales es la diseminación de la gestión documental en las organizaciones. Se puede aprovechar la coyuntura para ir introduciendo buenas prácticas en la gestión de documentos de manera progresiva e ir ampliando el ratio de acción. Es otro modo de afianzar la gestión documental, desde una nueva perspectiva que se ha demostrado que resulta útil. De hecho, cabe destacar que, a lo largo del desarrollo del estudio de caso, la Organización X decidió incluir la gestión de riesgos documentales en su plan estratégico de gestión para los próximos cuatro años. Esta decisión beneficiará a la gestión documental, haciéndola más visible y aumentando la percepción de los trabajadores sobre la necesidad de contar con esta metodología para el correcto funcionamiento y para la prevención de riesgos.

De este modo, se hace evidente que, tanto desde el punto de vista de los profesionales como desde el nivel estratégico de las administraciones públicas, la gestión de riesgos documentales se percibe como algo a explotar. Se deberá aprovechar esta oportunidad para continuar con el estudio de la metodología y analizar, a partir de múltiples experiencias, las posibles mejoras y desarrollos a implantar.

6. Primer paso para el desarrollo de nuevas investigaciones

Esta investigación debe entenderse como un primer paso para dar continuidad y protagonismo a un nuevo campo de trabajo y estudio en la archivística. Se ha demostrado la gran utilidad de la gestión de riesgos documentales, ya no solamente en relación con los procesos de rendición de cuentas, sino para la mejora continua en las organizaciones a través de la gestión de su información. Quedan muchos campos de aplicación no incluidos en el alcance de esta investigación y que pueden aportar mucho a la profesión. Por ejemplo, analizar las técnicas existentes de gestión de riesgos para comprobar su adaptación a la gestión de documentos, explorar nuevas técnicas o enfoques para la identificación de riesgos documentales, analizar las posibilidades de clasificación o tipificación de riesgos documentales, identificar patrones en los factores y causas de los riesgos, estudiar la influencia de la transformación digital en la gestión de riesgos, realizar un análisis comparativo de riesgos documentales en entornos clásicos, híbridos y electrónicos, entre muchos otros temas.

Un aspecto positivo que cabe mencionar para el futuro es el proyecto de revisión del informe técnico ISO/TR 18128, que se llevará a cabo durante los primeros meses del año 2019. En un primer momento, el objetivo de esta revisión se centraba en actualizar el informe según los cambios de la nueva versión de la norma ISO 31000, publicada a principios del año 2018. Sin embargo, este proyecto ha ido creciendo en envergadura y, desde el Comité Técnico de ISO responsable se plantea la posibilidad de convertir el informe técnico en un estándar internacional. Este cambio significaría un mejor posicionamiento para esta metodología, con mayor influencia entre los profesionales especializados y afines. Una vez publicado es posible que se den algunos cambios en el proceso de gestión de riesgos documentales, que se deberán tener en consideración para futuras investigaciones.

Otras posibilidades de investigación, más relacionadas con la rendición de cuentas, podrían incluir profundizar en el estudio de las estrategias de toma de conciencia de los trabajadores públicos sobre la importancia de la gestión de las evidencias documentales, o estudiar las posibilidades de concienciación de los propios teóricos de la transparencia y la rendición de cuentas en materia de gestión documental. En este sentido, es importante mencionar que queda mucho camino por recorrer en la multidisciplinariedad.

Esta investigación también pretende dar otro paso en el proceso de romper fronteras entre la ciencia archivística y otras ciencias o ámbitos de estudio. Cada vez más se aprecia que todo está interconectado y, por este motivo, no se debe estudiar la gestión de documentos de manera aislada, solamente dentro de su propio entorno, sino que se deben difuminar estas fronteras y buscar ámbitos afines, y no tan afines, para el desarrollo, pero sobre todo para el crecimiento de la archivística y la gestión documental. Se ha demostrado en esta investigación que la integración de tres ámbitos de estudio muy distintos conlleva grandes aportaciones. Los tres ámbitos se han beneficiado entre sí, se han complementado y han evolucionado hacia una mejor versión de sí mismos. Por este motivo, se anima a la comunidad a seguir en el futuro con esta filosofía de integración y crecimiento en positivo.

Bibliografía

- AENOR, 2006a. *UNE-ISO/TR 15489-2. Informació i documentació - Gestió documental - Part 2: Directrius*. 2006. Madrid: AENOR.
- AENOR, 2006b. *UNE-ISO 15489-1. Información y documentación. Gestión de documentos. Parte 1: Generalidades*. 2006. Madrid: AENOR.
- AENOR, 2008. *UNE-ISO/TR 26122 IN. Información y documentación. Análisis de los procesos de trabajo para la gestión de documentos*. 2008. Madrid: AENOR.
- AENOR, 2010. *UNE-ISO 31000: 2010. Gestión del riesgo. Principios y directrices*. 2010. Madrid: AENOR.
- AENOR, 2011a. *UNE-EN ISO/IEC 31010. Gestión del riesgo. Técnicas de apreciación del riesgo*. 2011. Madrid: AENOR.
- AENOR, 2011b. *UNE-ISO 30300. Información y documentación. Sistemas de gestión para los documentos. Fundamentos y vocabulario*. 2011. Madrid: AENOR.
- AENOR, 2011c. *UNE-ISO 30301. Información y documentación. Sistemas de gestión para los documentos. Requisitos*. 2011. Madrid: AENOR.
- AENOR, 2014. *UNE-ISO/TR 18128. Información y documentación. Identificación y evaluación de riesgos para sistemas de documentos*. 2014. Madrid: AENOR.
- AENOR, 2015a. *UNE-ISO 30302. Información y documentación. Sistemas de gestión para los documentos. Guía de implantación*. 2015. Madrid: AENOR.
- AENOR, 2015b. *UNE-EN ISO/IEC 17021-1. Evaluación de la conformidad. Requisitos para los organismos que realizan la auditoría y la certificación de sistemas de gestión. Parte 1: Requisitos*. 2015. Madrid: AENOR.
- AENOR, 2016. *UNE-ISO 15489-1. Información y documentación. Gestión de documentos. Parte 1: Conceptos y principios*. 2016. Madrid: AENOR.
- AGUILAR RIVERA, J.A., 2008. *Transparencia y democracia: claves para un concierto*. 2008. Ciudad de México: Instituto Federal de Acceso a la Información Pública (IFAI). ISBN 9685954283.
- ALBERCH I FUGUERAS, R., 2013. *Archivos: entender el pasado, construir el futuro*. Barcelona : Editorial UOC. ISBN 9788490297773.
- ALBERCH FUQUERAS, R., CASADESÚS DE MINGO, A., MAURI MARTÍ, A. y PERPINYÀ MOREIRA, R., 2014. ISO 30301 Certification for the Graduate School of Archive and Records Management: a Pioneering Initiative [en línea]. *Girona 2014: Arxius i Indústries Culturals*. Disponible en <http://www.girona.cat/web/ica2014/ponents/textos/id30-ESP.pdf>
- ALBORNOZ, F., ESTEBAN, J. y VANIN, P., 2009. Government Information Transparency [en línea]. DOI <http://dx.doi.org/10.2139/ssrn.1407162>. Disponible en: <https://ssrn.com/abstract=1407162>

- ALT, J.E., 2002. Credibility, transparency, and institutions: an exploration and an example [en línea]. *Estudios - Working papers / Instituto Juan March de Estudios e Investigaciones 2001/173*. Madrid: Centro de Estudios Avanzados en Ciencias Sociales. Disponible en: <http://digital.march.es/ceacs-ir/es/fedora/repository/ir%3A3797>
- AMUTIO GÓMEZ, M.Á., CANDAU, J. y MAÑAS, J.A., 2012. *MAGERIT - versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método* [en línea]. 2012. Madrid: Ministerio de Hacienda y Administraciones Públicas. Disponible en: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html.
- ANDREEVA, G., ANSELL, J. y HARRISON, T., 2014. Governance and Accountability of Public Risk. *Financial Accountability & Management*, vol. 30, no. 3, pp. 342- 361. ISSN 02674424. DOI 10.1111/faam.12036.
- ARMA INTERNATIONAL, 2009. *Evaluating and Mitigating Records and Information Risks. An ARMA International Guideline*. Overland Park: ARMA International. ISBN 9781931786867.
- ARMA INTERNATIONAL, 2014. Generally Accepted Recordkeeping Principles. [en línea], Disponible en: https://cdn.ymaws.com/www.arma.org/resource/resmgr/files/Learn/2017_Generally_Accepted_Reco.pdf.
- ASSOCIACIÓ D'ARXIVERS - GESTORS DE DOCUMENTS DE CATALUNYA, 2012. *Principis i requeriments funcionals per a documents en entorns d'oficina digital. Mòdul 1. Presentació general y declaració de principis*. Barcelona. ISBN 9788494020100. Associació d'Arxivers - Gestors de Documents de Catalunya.
- ARNULL, A. y WINCOTT, D., 2002. *Accountability and legitimacy in the European Union*. Oxford: Oxford University Press. ISBN 0199255601.
- BAK, G., 2016. Trusted by whom? TDRs, standards culture and the nature of trust. *Archival Science*, vol. 16, no. 4, pp. 373-402. ISSN 15737519. DOI 10.1007/s10502-015-9257-1.
- BALDWIN, R., BLACK, J. y O'LEARY, G., 2014. Risk Regulation and Transnationality: Institutional Accountability as a Driver of Innovation. *Transnational Environmental Law* [en línea], vol. 3, no. 02, pp. 373-390. ISSN 2047-1025. DOI 10.1017/S2047102514000120. Disponible en: http://www.journals.cambridge.org/abstract_S2047102514000120.
- BARATA, K., CAIN, P. y THURSTON, A., 1999. From Accounting to Accountability: Managing Accounting Records as a Strategic Resource [en línea]. *Report to the World Bank infoDEV Programme*, International Records Management Trust. Disponible en: http://www.irmt.org/documents/research_reports/accounting_recs/IRMT_acc_rec_background.PDF
- BEARMAN, D., 2006. Moments of risk: Identifying threats to electronic records [en línea]. *Archivaria*, vol. 62, no. 1, pp. 15-46. ISSN 03186954. Disponible en: <https://archivaria.ca/index.php/archivaria/article/view/12912/14148>
- BECK, U., 2006. *La Sociedad del riesgo global*. Madrid: Siglo Veintiuno de España. ISBN 8432312614.
- BELLO PAREDES, S.A., 2014. Gobernanza local y transparencia. *Revista jurídica de Castilla y León*, no. 33, pp. 7-28. ISSN 1696-6759.

- BELLVER, A. y KAUFMANN, D., 2005. Transparenting Transparency: Initial Empirics and Policy Applications. *SSRN Electronic Journal* [en línea], pp. 1-73. ISSN 1556- 5068. DOI 10.2139/ssrn.808664. Disponible en: <http://siteresources.worldbank.org/INTWBIGOVANTCOR/Resources/TransparentingTransparency171005.pdf>.
- BENTHAM, J., 2002. *Tácticas parlamentarias* [en línea]. 2002. Ciudad de México: Coordinación de los Diputados del Sector Popular del Partido Revolucionario Institucional. ISBN 8479430214. Disponible en: http://biblioteca.diputados.gob.mx/janium/bv/lviii/tac_parla_lviii.pdf
- BERLINER, D., 2014. The Political Origins of Transparency. *The Journal of Politics* [en línea], vol. 76, no. 2, pp. 479-491. ISSN 0022-3816. DOI 10.1017/S0022381613001412. Disponible en: <http://www.journals.uchicago.edu/doi/10.1017/S0022381613001412>.
- BERNSTEIN, P.L., 1996. *Against the gods: the remarkable story of risk*. New York: John Wiley & Sons, Inc. ISBN 9780471295631.
- BLANES CLIMENT, M.Á., 2014. *La transparencia informativa de las administraciones públicas: el derecho de las personas a saber y la obligación de difundir información pública de forma activa*. Cizur Menor: Aranzadi Thomson Reuters. ISBN 9788490593974.
- BONAL-ZAZO, J.L., 2012. Paradigmas de investigación en Archivística. En: OFICINA UNIVERSITARIA (ed.), *Estudios avanzados en Arquivologia* [en línea]. São Paulo: Cultura académica, pp. 69-90. ISBN 9788579832666. Disponible en: http://www.marilia.unesp.br/Home/Publicacoes/estudios_avancados_arquivologia.pdf.
- BOROWIAK, C.T., 2011. *Accountability and democracy the pitfalls and promise of popular control*. Oxford: Oxford University Press. ISBN 9780199778256.
- BOVENS, M., 2005. Public Accountability. En: E. FERLIE, L.J. LAURENCE y C. POLLIT (Eds.), *The Oxford Handbook of Public Management*. Oxford Handbooks, pp. 182-208. ISBN 0761964800.
- BOVENS, M., 2010. Two Concepts of Accountability: Accountability as a Virtue and as a Mechanism. *West European Politics*, vol. 33, no. 5, pp. 946-967. ISSN 0140- 2382. DOI 10.1080/01402382.2010.486119.
- BOVENS, M., SCHILLEMANS, T. y HART, P.T., 2008. Does public accountability work? An assessment tool. *Public Administration*, vol. 86, no. 1, pp. 225-242. ISSN 00333298. DOI 10.1111/j.1467-9299.2008.00716.x.
- BOVENS, M., CURTIN, D. y HART, P., 2010. *The Real world of EU accountability: what deficit?* New York: Oxford University Press. ISBN 9780199587803.
- BOWLES, N., HAMILTON, J.T. y LEVY, D.A.L. (Eds.), 2014. *Transparency in Politics and the Media. Accountability and Open Government*. New York: I.B. Tauris & Co. Ltd in association with the Reuters Institute for the Study of Journalism, University of Oxford. ISBN 9781780766768.
- BOVENS, M., GOODIN, R. E., SCHILLEMANS, T. (Eds.) , 2016. *The Oxford Handbook of Public Accountability*. Oxford: Oxford University Press. ISBN 9780198778479.
- BOVENS, M; SCHILLEMANS, T; GOODIN, R.E., 2016. Public Accountability. En: M. BOVENS, R.E. GOODIN y T. SCHILLEMANS (Eds.), *The Oxford Handbook of Public Accountability*. Oxford: Oxford University Press, ISBN 9780198778479.

- BRANDSMA, G.J. y SCHILLEMANS, T., 2013. The accountability cube: Measuring accountability. *Journal of Public Administration Research and Theory*, vol. 23, no. 4, pp. 953-975. ISSN 10531858. DOI 10.1093/jopart/muso34.
- BRIOSCHI, C.A. y GARZÓN, B., 2010. *Breve historia de la corrupción: de la Antigüedad a nuestros días*. Madrid: Santillana. ISBN 9788430607907.
- BRITISH STANDARDS INSTITUTION, 2008. *BS ISO/IEC 27001:2008 Information technology - Security techniques - Information security risk management*. British Standards Institution. ISBN 9780580545139.
- BRITO MARQUINA, A., 2015. La normalización como elemento de competitividad y de potencial exportador. *Economía Industrial (EI)*, vol. 396, pp. 33-42.
- BROWN, C., 2014. *Archives and recordkeeping: theory into practice*. London: Facet Publishing. ISBN 9781856048255.
- BROWN, I. y MARSDEN, C.T., 2013. *Regulating code: good governance and better regulation in the information age*. Cambridge: The MIT Press. ISBN 9780262018821.
- BRUNO, J.R., 2015. *Transparency Supplements*. 2015. Lugano: 4rd Global Conference os Transparency Research.
- BRYMAN, A., 2012. *Social Research Methods*. 4. New York: Oxford University Press. ISBN 9780199588053.
- BUSCO, C., FRIGO, M.L., RICCABONI, A. y QUATTRONE, P., 2015. *Integrated reporting. Concepts and Cases that Redefine Corporate Accountability*. London: Springer. ISBN 9783319021683.
- BUSTELO RUESTA, C., 2009. La Gestión de documentos y las evidencias en las organizaciones. Del plano operativo al plano estratégico: una propuesta desde la normalización. *Revista Española de Documentación Científica*, vol. 32, no. 4, pp. 157-161. ISSN 0210-0614.
- BUSTELO RUESTA, C., 2011. *Serie ISO 30300: Sistema de gestión para los documentos* [en línea]. Madrid: SEDIC. Asociación Española de Documentación e Información Científica. Documentos de trabajo. Disponible en: <https://www.sedic.es/wp-content/uploads/2011/01/serie-iso-30300.pdf>
- BUSTELO RUESTA, C., 2012. La normalización internacional en información y documentación: ¿una historia de éxitos? El caso de la normalización ISO en gestión de documentos. *Métodos de información*, vol. 3, no. 4, pp. 039-046. ISSN 11342838. DOI 10.5557/IIMEI2-N2-039046.
- BUSUIOC, M., 2012. European agencies and their boards: promises and pitfalls of accountability beyond design. *Journal of European Public Policy*, vol. 19, no. 5, pp. 719-736. ISSN 1350-1763. DOI 10.1080/13501763.2011.646785.
- CABEZAS MARDONES, C., 2014. Transparencia activa: Gestión de documentos electrónicos y datos en Chile. *Serie Bibliotecología y Gestión de Información*, no. 93, pp. 3-16. ISSN 07190832.
- CAPELL I GARRIGA, E. y COROMINAS I NOGUERA, M. (Eds.), 2009. *Manual d'arxivística i gestió documental*. Barcelona: Associació d'Arxivers de Catalunya. ISBN 9788492248292.
- CAPELLADES, A., CASADESÚS, A., LOPERA, S., MARIA, A. y MEINHARDT, C., 2016. *Model de maduresa en gestió documental per a la transparència i la publicitat activa*. Barcelona: Associació d'Arxivers-Gestors de Documents de Catalunya.

- CASADESÚS DE MINGO, A., 2015. Gestión de riesgos aplicada a la gestión de documentos: una metodología para garantizar una rendición de cuentas confiable. *I Jornadas Fundación Olga Gallego*, vol. 1, no. 1, pp. 119-135.
- CASADESÚS DE MINGO, A. y CERRILLO I MARTÍNEZ, A., 2018. El impacto de la gestión documental en la transparencia de las Administraciones públicas: la transparencia por diseño. *GAPP. Nueva Época*, no. 19, pp. 6-16. DOI 10.24965/gapp.voi19.10515.
- CASADESÚS DE MINGO, A., MAURI MARTÍ, A. y PERPINYÀ MORERA, R., 2016. Transparencia en riesgo: la gestión de documentos como estrategia de prevención. [en línea] VII Congreso *Internacional en Gobierno, Administración y Políticas Públicas GIGAPP*. Madrid. Disponible en: http://www.gigapp.org/administrator/components/com_jresearch/files/publications/2016-405.pdf
- CASADESÚS DE MINGO, A. y CERRILLO I MARTÍNEZ, A., 2018. Improving records management to promote transparency and prevent corruption. *International Journal of Information Management* [en línea], vol. 38, no. 1, pp. 256-261. ISSN 02684012. DOI 10.1016/j.ijinfomgt.2017.09.005. Disponible en: <http://linkinghub.elsevier.com/retrieve/pii/S0268401217306242>.
- CEA D'ANCONA, M.Á., 2001. *Metodología Cuantitativa. Estrategias y técnicas de investigación social*. Madrid: Editorial Síntesis, S.A. ISBN 8477384207.
- CERRILLO-I-MARTÍNEZ, A., 2012. The re-use of public sector information in Europe and its impact on transparency. *European Journal of Law*, vol. 18, no. 6, pp. 770- 792. DOI <http://doi.org/10.1111/eulj.12003>.
- CHAPMAN, R.A. y HUNT, M., 2006. *Open government in a theoretical and practical context*. Burlington, VT: Ashgate. ISBN 0754646424.
- CONDESSO, F., 2011. *Derecho a la información. Crisis del sistema político. Transparencia de los Poderes Públicos*. Preimpresi. Madrid : Dykinson. ISBN 9788499824192.
- COOK, T., 2001. Archival Science and Postmodernism: New Formulations for Old Concepts. *Archival Science*, vol. 1, no. 1, pp. 3-24. DOI <https://doi.org/10.1007/BF02435636>.
- COOK, T., 2002. Archives, Records, and Power: From (Postmodern) Theory to (Archival) Performance. *Archival Science*, vol. 2, no. 3-4, pp. 171-185. DOI <https://doi.org/10.1007/BF02435620>.
- COX, R.J., 2001. *Managing records as evidence and information*. Westport, Conn.: Quorum Books. ISBN 1567202314.
- CRESPO RODRÍGUEZ, M. y ZAFRA JIMÉNEZ, A., 2005. *Transparencia y buen gobierno: su regulación en España*. Madrid: La Ley. ISBN 84-9725-594-1.
- CRUZ MUNDET, J.R., 2005. *Manual de archivística*. Madrid: Fundación Germán Sánchez Ruipérez. ISBN 9788489384316.
- CRUZ MUNDET, J.R. (Dir.), 2011. *Administración de documentos y archivos. Textos fundamentales*. Madrid: Coordinadora de Asociaciones de Archiveros y Gestores de Documentos (CAA). ISBN 9788461551507.
- CRUZ MUNDET, J.R., 2012. *Archivística: gestión de documentos y administración de archivos*. Madrid: Alianza. ISBN 9788420609522.

- CRUZ REVUELTAS, J.C., 2009. Moral y Transparencia. Fundamento e implicaciones morales de la transparencia. [en línea]. Ciudad de México: Instituto Federal de Acceso a la Información Pública (IFAI). Cuadernos de transparencia, 15. Disponible en: http://www.resi.org.mx/icainew_f/images/Biblioteca/Cuaderno_transparencia/cuadernillo15.pdf.
- CUNNINGHAM, A., 2005. Memoria, pruebas y responsabilidad: enfoques australianos para gestionar el Records Continuum. *TABULA*, no. 8, pp. 103-119. ISSN 1098- 6596. DOI 10.1017/CBO9781107415324.004.
- CUNNINGHAM, A., 2011. The postcustodial archive. *The Future of Archives and Recordkeeping. A reader*. London: Facet Publishing, pp. 173-190.
- DAHL, R.A., 1999. *La Democracia: una guía para los ciudadanos*. Madrid: Taurus. ISBN 8430603425.
- DARBISHIRE, H., 2010. Proactive Transparency: The future of the right to information [en línea]. *World Bank Institute (Governance Working Paper Series)*. Disponible en: http://siteresources.worldbank.org/WBI/Resources/213798-1259011531325/6598384-1268250334206/Darbishire_Proactive_Transparency.pdf
- DAWES, S.S., 2010. Stewardship and usefulness: Policy principles for information-based transparency. *Government Information Quarterly*, vol. 27, no. 4, pp. 377- 383. ISSN 0740624X. DOI 10.1016/j.giq.2010.07.001.
- DEPARTAMENT DE CULTURA, 2015. Guia d'utilització del quadre de tipus documentals [en línea]. Barcelona: Departament de Cultura. pp. 1-55. (Arxivística i gestió documental. Eines; 8). Disponible en: http://cultura.gencat.cat/web/.content/dgpc/arxiu_i_gestio_documental/09_publicacions/altres_publicacions/Guia-de-tipus-documentals.pdf
- DERRIDA, J., 1997. *Mal de archivo. Una impresión freudiana*. 1997. Valladolid: Simancas Ediciones, S.A. ISBN 8481641332.
- DIETEL, J.E., 2003. Recordkeeping Integrity: assessing records' content after Enron. *The Information Management Journal*, no. May/June, pp. 43-51.
- DIRKS, J.M., 2004. Accountability, History, and Archives: Conflicting Priorities or Synthesized Strands? *Archivaria*, vol. 57, no. 1, pp. 29-49. ISSN 03186954.
- DONAHUE, J.D., 2002. Market-Based Governance and the Architecture of Accountability. En: J.D. DONAHUE y J.S. NYE (Eds.), *Market-Based Governance*. Brookings Institution Press, pp. 1-25.
- DOWDLE, M.W., 2006. *Public accountability: designs, dilemmas and experiences*. Cambridge: Cambridge University Press. ISBN 0521617618.
- DRAGHI, M., GIAVAZZI, F. y MERTON, R.C., 2003. *Transparency, risk management and international financial fragility*. London: Centre for Economic Policy Research. ISBN 1898128685.
- DUBNICK, M.J., 2003. Accountability and ethics: Reconsidering the relationships. *International Journal of Organization Theory and Behavior*, vol. 6, no. 3, pp. 405- 441. ISSN 10934537. DOI doi:10.1201/NOE1420052756.ch3.
- DUBNICK, M.J., 2006. Accountability and the Evil of Administrative Ethics. *Administration & Society*, vol. 38, no. 2, pp. 236-267. ISSN 0095-3997. DOI 10.1177/0095399705285999.

- DUBNICK, M.J., 2016. Accountability as a Cultural Keyword. En: R.E. BOVENS, M; SCHILLEMANS, T.; GOODIN (Eds.), *The Oxford Handbook of Public Accountability*. Oxford: Oxford University Press, pp. 23-38. ISBN 9780198778479.
- DUFF, W.M., JOHNSON, C.A. y CHERRY, J.M., 2013. Reaching out, reaching in: A preliminary investigation into archives' use of social media in Canada. *Archivaria*, no. 75, pp. 77-96. ISSN 03186954.
- DUPLÁ DEL MORAL, A., 2005. *Manual de archivos de oficina para gestores. Comunidad de madrid*. Madrid: Marcial Pons, Ediciones Jurídicas y Sociales, S.A. ISBN 9788472484672.
- DURANTI, L., 2008. El concepto de documento archivístico en entornos experienciales, interactivos y dinámicos: ensayo de discusión. *InterPARES 2*.
- DURANTI, L., 2009. From digital diplomatics to digital records forensics. *Archivaria*, vol. 68, no. Fall 2009, pp. 39-66. ISSN 03186954.
- DURANTI, L. y FRANKS, P.C. (Eds.), 2015. *Encyclopedia of archival science*. Plymouth: Rowman. ISBN 9780810888111.
- DURANTI, L. y MICHETTI, G., 2016. The archival method. *Research in the archival multiverse*. Clayton: Monash University Publishing, pp. 75-95. ISBN 9781876924676.
- DYRBERG, P., 2002. Accountability and Legitimacy: What is the Contribution of Transparency? En: A. ARNULL y D. WINCOTT (Eds.), *Accountability and Legitimacy in the European Union*. S.l.: Oxford University Press, pp. 81-96. ISBN 0199257108.
- EASTWOOD, T. y MACNEIL, H. (Eds.), 2010. *Currents of Archival Thinking*. Santa Barbara: ABC-CLIO, LLC. ISBN 9781591586562.
- EGBUJI, A., 1999. Risk management of organisational records. *Records Management Journal*, vol. 9, no. 2, pp. 93-116. ISSN 0956-5698. DOI 10.1108/EUM0000000007245.
- ELSTER, J., 2006. *Rendición de cuentas: la justicia transicional en perspectiva histórica*. Buenos Aires: Katz. ISBN 987128330X.
- EUROPEAN COMMISSION, 2005. *Report on archives in the enlarged European Union. Increased archival cooperation in Europe: action plan*. Belgium: European Communities. ISBN 9279008706.
- EVANS, J., REED, B., LINGER, H., GOSS, S., HOLMES, D., DROBIK, J., WOODYAT, B. y HENBEST, S., 2014. Winds of change: A recordkeeping informatics approach to information management needs in data-driven research environments. *Records Management Journal*, vol. 24, no. 3. ISSN 0956-5698. DOI 10.1108/RMJ-01-2014-0006.
- FEHRLER, S. y HUGHES, N., 2018. How Transparency Kills Information Aggregation: Theory and Experiment. *American Economic Journal: Microeconomics*, vol. 10, no. 1, pp. 181-209. DOI 10.1257/mic.20160046.
- FERNÁNDEZ RAMOS, S., 1997. *El Derecho de acceso a los documentos administrativos*. Madrid: Marcial Pons. ISBN 8472484750.
- FINEL, B.I. y LORD, K.M., 1999. The Surprising Logic of Transparency. *International Studies Quarterly* [en línea], vol. 43, no. 2, pp. 315-339. ISSN 00208833. DOI 10.2307/2600758. Disponible en: <http://www.jstor.org/stable/2600758>

- FLORENSA ORTIGA, H. y LORENTE LÓPEZ, A., 2004. El Sistema de Gestió Documental: una responsabilitat compartida. *Lligall, Revista Catalana d'Arxivística* [en línea], no. 22, pp. 421-445. Disponible en: <https://arxiv.org/index.php/documents/publicacions/revista-lligall-1/lligall-22-1/160-14-el-sistema-de-gestio-documental-una-responsabilitat-compartida-1/file>
- FRANCESCUTTI, L.P., 2012. Wikileaks: Transparencia total. Límites y posibilidades de una demanda utópica. *Estudios Sobre el Mensaje Periodístico*, vol. 18, no. 1, pp. 89-100. ISSN 11341629. DOI 10.5209/rev_ESMP.2012.v18.n1.39356.
- FRØLICH, N., 2011. Multi-layered accountability. Performance-based funding of universities. *Public Administration*, vol. 89, no. 3, pp. 840-859. ISSN 00333298. DOI 10.1111/j.1467-9299.2010.01867.x.
- FUNG, A., GRAHAM, M. y WEIL, D., 2007. *Full Disclosure. The Perils and Promise of Transparency*. New York: Cambridge University Press. ISBN 9780521699617.
- GARCÍA RUIPÉREZ, M., 2015. La denominación de tipos, series y unidades documentales en España. Aportación a la teoría archivística (I). *Documenta & Instrumenta*, no. 13, pp. 53-87. DOI 10.5209/REV_DOCU.2015.V13.49740.
- GARSON, G.D., 2006. *Public information technology and e-governance: managing the virtual state*. Raleigh: Jones and Bartlett Publishers. ISBN 0763734683.
- GAVENTA, J. y MCGEE, R., 2013. The impact of transparency and accountability initiatives. *Development Policy Review*, vol. 31, no. 1, pp. 3-28. ISSN 09506764. DOI 10.1111/dpr.12017.
- GHAURI, P., 2004. Designing and Conducting Case Studies in International Business Research. En: R. MARSCHAN-PIEKKARI y C. WELCH (Eds.), *Handbook of Qualitative Research Methods for International Business*. Northampton, Massachusetts: Edward Elgar Publishing, Inc., pp. 109-124. ISBN 1843760835.
- GILBERT, J., 2000. Access denied: The Access to Information Act and Its effect on public records creators. *Archivaria*, vol. 49, no. 1, pp. 84-123. ISSN 03186954.
- GILLILAND, A., 2014. *Conceptualizing 21st-Century Archives*. Chicago: Society of American Archivists. ISBN 1931666687.
- GILLILAND, A.J., MCKEMMISH, S. y LAU, A.J. (Eds.), 2016. *Research in the Archival Multiverse*. Clayton: Monash University Publishing. ISBN 9781876924676.
- GIMÉNEZ-CHORNET, V., 2012. Acceso de los ciudadanos a los documentos como transparencia de la gestión pública. *El Profesional de la Información*, vol. 21, no. 5, pp. 504-508. ISSN 1386-6710. DOI 10.3145/epi.2012.sep.09.
- GONZÁLEZ ALONSO, L.N. y MANGAS MARTÍN, A., 2002. *Transparencia y acceso a la información en la Unión Europea*. Madrid: COLEX. ISBN 8478797602.
- GONZÁLEZ HERNÁNDEZ, S., 2006. *Archivos desorganizados fuente de corrupción administrativa*. Bogotá: Imprenta Nacional de Colombia. ISBN 9588242029.
- GREILING, D. y HALACHMI, A., 2012. Public private partnerships: accountability and governance. *Public Administration Quarterly*, vol. 36, no. 2, pp. 134-139. ISSN 07349149.

- GRIFFIN, A., 2004. Records Management Capacity Assessment System (RMCAS). *Archival Science*, vol. 4, no. 1-2, pp. 71-97. ISSN 13890166. DOI 10.1007/s10502-005-6991-9.
- GRIMMELIKHUIJSEN, S., PORUMBESCU, G., HONG, B. y IM, T., 2013. The effect of transparency on trust in government: A cross-national comparative experiment. *Public Administration Review*, vol. 73, no. 4, pp. 575-586. ISSN 00333352. DOI 10.1111/puar.12047.
- GRUPO DE DIFUSIÓN DEL CTN 50-SC1, 2012. Normalización en el sector documental. *Revista Española de Documentación Científica* [en línea], vol. 35, no. 1, pp. 175-178. ISSN 0210-0614. Disponible en: <http://redc.revistas.csic.es/index.php/redc/article/view/728/808>
- GRUPO DE TRABAJO SOBRE CALIDAD EN LOS ARCHIVOS UNIVERSITARIOS, 2013. *Guía para la evaluación de archivos universitarios con el modelo EFQM de excelencia* [en línea]. 2013. Madrid: CRUE - CAU Conferencia de Archiveros de las Universidades Españolas. Disponible en: http://cau.crue.org/wp-content/uploads/GUIA_EVALUACION_EFQM_V_6_2013.pdf
- GUICHOT, E., 2011. *Transparencia y acceso a la información en el Derecho Europeo*. Sevilla: Derecho global. ISBN 9788493634933.
- GUICHOT, E. y BARRERO RODRÍGUEZ, C., 2014. *Transparencia, acceso a la información pública y buen gobierno: estudio de la Ley 19/2013, de 9 de diciembre*. Madrid: Tecnos. ISBN 9788430961665.
- HAGEN SATASLAATTEN, O., 2014. The Norwegian Noark Model requirements for EDRMS in the context of open government and access to governmental information. *Records Management Journal* [en línea], vol. 24, no. 3, pp. 189-204. ISSN 0956-5698. DOI 10.1108/RMJ-09-2014-0041. Disponible en: <http://www.emeraldinsight.com/doi/10.1108/RMJ-09-2014-0041>
- HARRIES, S., 2009. Managing records, making knowledge and good governance. *Records Management Journal* [en línea], vol. 19, no. 1, pp. 16-25. ISSN 0956-5698. DOI 10.1108/09565690910937218. Disponible en: www.emeraldinsight.com/10.1108/09565690910937218.
- HAY-GIBSON, N., 2008. A river of risk: a diagram of the history and historiography of risk management. *Interdisciplinary Studies in the Built and Virtual Environment*, vol. 1, no. 2. ISSN 1756-2473.
- HAY-GIBSON, N., 2011. *Risk and records management: investigating risk and risk management in the context of records and information management in the electronic environment*. Doctoral Thesis. Northumbria University Newcastle.
- HAZELL, R. y WORTHY, B., 2010. Assessing the performance of freedom of information. *Government Information Quarterly*, vol. 27, no. 4, pp. 352-359. ISSN 0740624X. DOI 10.1016/j.giq.2010.03.005.
- HEALD, D., 2006. Varieties of transparency. En: C. HOOD y D. HEALD (Eds.), *Transparency: the Key to Better Governance?* Oxford: Oxford University Press, pp. 25-43. ISBN 9780197263839.
- HOFMAN, H., 2006. Standards: Not 'One Size Fits All'. *The Information Management Journal*, vol. May/June. DOI 10.1080/19496591.2015.1067224.
- HOOD, C., 2006a. Beyond Exchanging First Principles? Some Clonsing Comments. En: C. HOOD y D. HEALD (Eds.), *Transparency: the Key to Better Governance?* Oxford: Oxford University Press, pp. 211-226. ISBN 9780197263839.

- HOOD, C., 2006b. Transparency in Historical Perspective. En: C. HOOD y D. HEALD (Eds.), *Transparency: the Key to Better Governance?* Oxford: Oxford University Press, pp. 3-24. ISBN 9780197263839.
- HOOD, C., 2010. Accountability and Transparency: Siamese Twins, Matching Parts, Awkward Couple? *West European Politics* [en línea], vol. 33, no. 5, pp. 989-1009. ISSN 0140-2382. DOI 10.1080/01402382.2010.486122. Disponible en: <http://www.tandfonline.com/doi/abs/10.1080/01402382.2010.486122>.
- HOOD, C., ROTHSTEIN, H. y BALDWIN, R., 2006. *El Gobierno del riesgo: aproximación a los regímenes de regulación de riesgos*. Barcelona: Escola de Prevenió i Seguretat Integral. ISBN 8434440059.
- HUGHES, O.E., 2012. *Public management and administration: an introduction*. Houndmills, Basingstoke: Palgrave Macmillan. ISBN 9780230231252.
- IACOVINO, L., 2010. Archives as Arsenals of Accountability. En: T. EASTWOOD y H. MACNEIL (Eds.), *Currents of Archival Thinking*. Oxford: ABC-CLIO, LLC, pp. 181-212. ISBN 9781591586562.
- INSTITUTO NACIONAL DE SEGURIDAD E HIGIENE EN EL TRABAJO, 1998. *NTP 471: La vigilancia de la salud en la normativa de prevención de riesgos laborales*. 1998. Madrid: Ministerio de Trabajo y Asuntos Sociales.
- ISAZA ESPINOSA, C., 2015. El diseño institucional para la rendición de cuentas. Una valoración del caso colombiano. *Gestión y Política Pública*, vol. XXIV, no. 2, pp. 339-375.
- ISO, 2009. *ISO Guide 73. Risk management. Vocabulary*. 2009. Geneva: ISO.
- JANG, Y.S., CHO, M. y DRORI, G.S., 2014. National transparency: Global trends and national variations. *International Journal of Comparative Sociology* [en línea], vol. 55, no. 2, pp. 95-118. ISSN 0020-7152. DOI 10.1177/0020715214534949. Disponible en: <http://cos.sagepub.com/cgi/doi/10.1177/0020715214534949>.
- JIMERSON, R.C., 2005. Archival Priorities: Ten Critical Issues for the Profession. *Provenance, Journal of the Society of Georgia Archivists* [en línea], vol. 23, no. 1- Article 5, pp. 57-70. Disponible en: <https://digitalcommons.kennesaw.edu/provenance/vol23/iss1/5>.
- JOHARE, R., 2006. *The development of a model for education and training in electronic records management*. Doctoral thesis, Northumbria University.
- JONES, J.A., 2005. *An Introduction to Factor Analysis of Information Risk (FAIR): a framework for understanding*. Draft. Risk Management Insight, 59 + [13] p. Disponible en: <https://theartofservicelab.s3.amazonaws.com/All%20Toolkits/The%20Information%20risk%20management%20Toolkit/Act%20-%20Recommended%20Reading/Risk%20Management%20Insight.pdf>
- JULNES, P.D.L., 2012. Accountability Unbound. *Public Administration Review*, vol. 72, no. 4, pp. 615-622. ISSN 1540-6210. DOI 10.1111/j.1540-6210.2012.02611.x.Book.
- KAMARCK, E.C. y NYE, J.S., 2002. *Governance.com: democracy in the information age*. Washington, D.C.: Brookings Institution Press. ISBN 0815702167.
- KANT, I., 2013. *La paz perpetua*. Madrid: Editorial Tecnos. ISBN 9788430955824.
- KASSEL, D.S., 2008. Performance, accountability, and the debate over rules. *Public Administration Review*, vol. 68, no. 2, pp. 241-252. ISSN 00333352. DOI 10.1111/j.1540-6210.2007.00859.x.

- KETELAAR, E., 2010. Ten Years of Archival Science. *Archival Science*, vol. 10, no. 4, pp. 345-352. DOI <https://doi.org/10.1007/s10502-011-9137-2>.
- KINNUCAN-WELSCH, K., ROSEMARY, C.A. y GROGAN, P.R., 2006. Accountability by Design in Literacy Professional Development. *The Reading Teacher*, vol. 59, no. 5, pp. 426-435. ISSN 00340561. DOI 10.1598/RT.59.5.2.
- KOENIG-ARCHIBUGI, M. y HELD, D., 2005. *Global governance and public accountability*. Oxford: Blackwell. ISBN 1405126787.
- KOPPELL, J.G.S., 2005. Pathologies of accountability: ICANN and the challenge of "Multiple Accountabilities Disorder". *Public Administration Review*, vol. 65, no. 1, pp. 94-108. ISSN 1540-6210. DOI 10.1111/j.1540-6210.2005.00434.x.
- KOSACK, S. y FUNG, A., 2014. Does Transparency Improve Governance? *Annual Review of Political Science* [en línea], vol. 17, no. 1, pp. 65-87. ISSN 1094-2939. DOI doi:10.1146/annurev-polisci-032210-144356. Disponible en: <http://www.annualreviews.org/doi/abs/10.1146/annurev-polisci-032210-144356>.
- KRUEGER, R.A., 1998. *Analyzing & Reporting Focus Group Results*. Thousand Oaks: SAGE Publications. International Educational and Professional Publisher.
- KUZUCUOĞLU, A.H., 2014. Risk Management in Libraries, Archives and Museums. *IIB International Refereed Academic Social Sciences Journal*, vol. 5, no. Sep, pp. 277-294.
- LAPPIN, J., 2010. What will be the next records management orthodoxy? *Records Management Journal*, vol. 20, no. 3, pp. 252-264. ISSN 0956-5698. DOI 10.1108/09565691011095283.
- LEINO, P., 2014. Transparency, Participation and EU Institutional Practice: An Inquiry into the Limits of the 'Widest Possible'. *EUI Working papers* [en línea], no. 03. ISSN 0717-6163. DOI 10.1007/s13398-014-0173-7.2. Disponible en: <http://cadmus.eui.eu/handle/1814/30580>.
- LEMIEUX, V., 2001. Let the ghosts speak: An empirical exploration of the «nature» of the record. *Archivaria*, vol. 51, no. 1, pp. 81-111. ISSN 03186954. DOI 10.2307/809582.
- LEMIEUX, V., 2004a. *Managing Risks for Records and Information*. Lenexa, Kansas: ARMA International. ISBN 1931786186.
- LEMIEUX, V., 2004b. Two Approaches to Managing Information Risks. *ManagementWise*, no. Sept./Oct., pp. 56-61.
- LEMIEUX, V., 2010. The records-risk nexus: exploring the relationship between records and risk. *Records Management Journal*, vol. 20, no. 2, pp. 199-216. ISSN 0956-5698. DOI 10.1108/09565691011064331.
- LEMIEUX, V., 2016. Trusting records: is Blockchain technology the answer? *Records Management Journal* [en línea], vol. 26, no. 2, pp. 110-139. ISSN 0956-5698. DOI 10.1108/RMJ-12-2015-0042. Disponible en: <http://www.emeraldinsight.com/doi/10.1108/RMJ-12-2015-0042>.
- LEWIN, L., 2007. *Democratic Accountability: Why Choice in Politics Is Both Possible and Necessary*. Cambridge: Harvard University Press. ISBN 9780674024755.

- LINDBERG, S.I., 2013. Mapping accountability: core concept and subtypes. *International Review of Administrative Sciences* [en línea], vol. 79, no. 2, pp. 202- 226. ISSN 0020-8523. DOI 10.1177/0020852313477761. Disponible en: <http://ras.sagepub.com/content/79/2/202.abstract>.
- LINK, A.N. y SCOTT, J.T., 2010. Historical Perspectives on Public Accountability. En: A.N. LINK y J.T. SCOTT (Eds.), *Public Goods, Public Gains: Calculating the Social Benefits of Public R&D*. Oxford: Oxford University Press.
- LIU, S., ZHANG, J., LIU, Y. y CHEN, T., 2009. Evaluating and mitigating information systems development risk through Balanced Score Card. *Proceedings - 2009 International Symposium on Information Engineering and Electronic Commerce*, IEEC 2009, pp. 111-115. DOI 10.1109/IEEC.2009.28.
- LLAURADÓ, J.M., 2000. *Democràcia digital: informació, participació, transparència*. Palma: Universitat de les Illes Balears. ISBN 84-7632-592-4.
- LOMAS, E., 2010. Information governance: information security and access within a UK context. *Records Management Journal*, vol. 20, no. 2, pp. 182-198. ISSN 0956-5698. DOI 10.1108/09565691011064322.
- LÓPEZ FERNÁNDEZ, I., 2012. *Transparencia focalizada a la Contraloría Social y Rendición de Cuentas*. Veracruz: Contraloría General - Gobierno del Estado de Veracruz. ISBN 9786077527466.
- LÓPEZ GÓMEZ, P. y GALLEGO DOMÍNGUEZ, O., 2007. *El documento de archivo: un estudio*. A Coruña: Universidade da Coruña Servizo de publicacións. ISBN 9788497492522.
- LOSADA LÓPEZ, J.L. y LÓPEZ FEAL, R., 2002. *Métodos de investigación en ciencias humanas y sociales*. Madrid: Thomson. ISBN 8497321901.
- LOWRY, J. y WAMUKOYA, J., 2014. *Integrity in Government thorough Records Management. Essays in Honour of Anne Thurston*. Farnham: Ashgate Publishing Limited. ISBN 9781472428455.
- LÜDERS, M., FOLSTAD, A. y WALDAL, E., 2014. Expectations and experiences with MyLabourParty: From right to know to right to participate? *Journal of Computer- Mediated Communication*, vol. 19, no. 3, pp. 446-462. ISSN 10836101. DOI 10.1111/jcc4.12047.
- LUJÁN, J.L. y ECHEVERRÍA, J., 2009. *Gobernar los riesgos: ciencia y valores en la sociedad del riesgo*. Madrid : Organización de Estados Iberoamericanos. ISBN 9788497429382.
- MACNEIL, H., 2002. Providing grounds for trust II: The findings of the authenticity task force of interPARES. *Archivaria*, vol. 54, no. 1, pp. 24-58. ISSN 03186954.
- MANCINI, D., VAASSEN, E.H.J. y DAMERI, R.P., 2013. *Accounting Information Systems for Decision Making*. London: Springer. ISBN 9783642357602.
- MANIN, B., STOKES, S.C. y PRZEWORSKI, A., 1999. *Democracy, accountability, and representation*. New York: Cambridge University Press. ISBN 0521646162.
- MARTÍNEZ GARCÍA, C., 2009. *Gestión integral de riesgos corporativos como fuente de ventaja competitiva: cultura positiva del riesgo y reorganización estructural*. Madrid: Fundación Mapfre. ISBN 9788498441567.
- MATAS I BALAGUER, J., 2015. Notes sobre les lleis de transparència. *Lligall, Revista Catalana d'Arxivística*, vol. 38, pp. 22-44.

- MATHEUS, R. y JANSSEN, M., 2013. Transparency of civil society websites: Towards a model for evaluation websites transparency. *7th International Conference on Theory and Practice of Electronic Governance, ICE-GOV 2013* [en línea], pp. 166- 169. DOI 10.1145/2591888.2591915. Disponible en: <https://dl.acm.org/citation.cfm?id=2591915>.
- MCCARTHY, D.R. y FLUCK, M., 2016. The concept of transparency in International Relations: Towards a critical approach. *European Journal of International Relations* [en línea], ISSN 1354-0661. DOI 10.1177/1354066116651688. Disponible en: <http://ejt.sagepub.com/cgi/doi/10.1177/1354066116651688>.
- MCGEE, R., 2013. Aid Transparency and Accountability: 'Build It and They'll Come'? *Development Policy Review* [en línea], vol. 31, no. 1, pp. 107-124. DOI <https://doi.org/10.1111/dpr.12022>. Disponible en: <http://onlinelibrary.wiley.com/doi/10.1111/dpr.12022/abstract>.
- MCKEMMISH, S., 2001. Placing records continuum theory and practice. *Archival Science*, vol. 1, no. 4, pp. 333-359. ISSN 1389-0166. DOI 10.1007/BF02438901.
- MCKEMMISH, S. y UPWARD, E., 1993. *Archival Documents. Providing Accountability Through Recordkeeping*. Clayton: Ancora Press. ISBN 0868620173.
- MCKEMMISH, S. y GILLILAND, A., 2013. Archival and recordkeeping research: Past, present and future. En: K. WILLIAMSON y G. JOHANSON (Eds.), *Research Methods: Information, Systems, and Contexts*. Pahrán, Victoria: Tilde University Press, pp. 79-112. ISBN 9788861293915.
- MCLEOD, J., 2012. Thoughts on the opportunities for records professionals of the open access, open data agenda. *Records Management Journal*, vol. 22, no. 2, pp. 92-97. ISSN 0956-5698. DOI 10.1108/09565691211268711.
- MEIJER, A., 2001. Accountability in an information age: Opportunities and risks for records management. *Archival Science*, vol. 1, no. 4, pp. 361-372. ISSN 1389-0166. DOI 10.1007/BF02438902.
- MEIJER, A., 2005. Risk maps on the Internet: Transparency and the management of risks. *Information Polity: The International Journal Of Government & Democracy In The Information Age*, vol. 10, pp. 105-113. ISSN 15701255.
- MEIJER, A., 2013. Understanding the Complex Dynamics of Transparency. *PAR. Public Administration Review*, vol. 73, no. 3, pp. 429-439. DOI 10.1111/puar.12032.
- MEIJER, A., 2014. Transparency. En: R.E. BOVENS, M; SCHILLEMANS, T.; GOODIN (Eds.), *The Oxford Handbook of Public Accountability*. Oxford: Oxford University Press, pp. 507-524.
- MEIJER, A.J., HART, P. y WORTHY, B., 2015. Assessing Government Transparency: An Interpretive Framework. *Administration & Society* [en línea], pp. 1-26. ISSN 0095-3997. DOI 10.1177/0095399715598341. Disponible en: <http://aas.sagepub.com/cgi/doi/10.1177/0095399715598341>.
- MENDO CARMONA, C., 2004. Consideraciones sobre el método en Archivística. *Documenta & Instrumenta* [en línea], vol. 1, pp. 35-46. DOI http://dx.doi.org/10.5209/rev_DOCU.2004.v1.20093. Disponible en: <http://revistas.ucm.es/index.php/DOCU/article/view/DOCU0404110035A>.
- MENDOZA NAVARRO, A.L., 2004. *Transparencia vs Corrupción. Los archivos: Políticas para su protección*. Lima: Perú Textos Editores. ISBN DL-1501012004- 8073.

- MILLAR, L., 2006. Touchstones: Considering the relationship between memory and archives. *Archivaria*, vol. 61, no. 1, pp. 105-126. ISSN 03186954.
- MILLAR, L.A., 2017. *Archives: Principles and Practices*. London. Facet Publishing. ISBN 1783302070.
- MORGAN, D.L., 1998a. *Planning Focus Groups*. Thousand Oaks: SAGE Publications. International Educational and Professional Publisher. ISBN 9780761908173.
- MORGAN, D.L., 1998b. *The Focus Group Guidebook*. Thousand Oaks: SAGE Publications. International Educational and Professional Publisher. ISBN 9780761908180.
- MORGAN, D.L., KRUEGER, R.A. y KING, J.A., 1998. *Developing Questions for Focus Group*. Thousand Oaks: SAGE Publications. International Educational and Professional Publisher. ISBN 0761908161.
- MORO CABERO, M., 2011. Certificación de calidad en los archivos. Análisis y prospectiva. *Revista Española de Documentación Científica*, vol. 34, no. 3, pp. 447-460. ISSN 0210-0614. DOI 10.3989/redc.2011.3.815.
- MORO CABERO, M., 2012. La evaluación en Archivos: Alcance e Instrumentos de Medición. En: OFICINA UNIVERSITARIA (Ed.), *Estudios avanzados en Arquivología* [en línea]. São Paulo: Cultura académica, pp. 27-54. ISBN 9788579832666. Disponible en: https://www.marilia.unesp.br/Home/Publicacoes/estudios_avancados_arquivologia.pdf.
- MORO CABERO, M. y LLANES PADRÓN, D., 2018. La importancia de la normalización para el ejercicio profesional del archivista. *Investigación Bibliotecológica: archivonomía, bibliotecología e información* [en línea], vol. 32, no. 74, pp. 193. ISSN 2448-8321. DOI 10.22201/iibi.24488321xe.2018.74.57919. Disponible en: <http://rev-ib.unam.mx/ib/index.php/ib/article/view/57919>.
- MOYANO COLLADO, J., 2015. Gestión documental en un marco de transparencia y reutilización de la información. *Lligall, Revista Catalana d'Arxivística*, no. 38, pp. 45-63.
- MULGAN, R., 1997. The Processes of Public Accountability. *Australian Journal of Public Administration*, vol. 56, no. 1, pp. 25-36. ISSN 0313-6647. DOI 10.1111/j.1467-8500.1997.tb01238.x.
- MULGAN, R., 2000. «Accountability»: An ever expanding Concept? *Public Administration*, vol. 78, no. 3, pp. 555-573. ISSN 0033-3298. DOI 10.1111/1467-9299.00218.
- NEAZOR, M., 2007. Recordkeeping professional ethics and their application. *Archivaria*, vol. 64, no. 1, pp. 47-87. ISSN 03186954.
- NESMITH, T., 1999. Still Fuzzy, But More Accurate: Some Thoughts of the «Ghosts» of Archival Theory. *Archivaria*, vol. 47, no. Spring 1999, pp. 136-150. ISSN 1923-6409.
- NGULUBE, P., 2014. Fostering Accountability and Justice: Opportunities for Records Managers in Changing Societies. *ESARBICA Journal*, no. 23, pp. 23-32. ISSN 0717-6163. DOI 10.1007/s13398-014-0173-7.2.
- NODAC, 2007. *Norma de Descripción Archivística de Cataluña (NODAC) 2007*. Generalitat de Catalunya. ISBN 9788439374466.
- NONELL, R., 2006. *Transparencia y buen gobierno: la rendición de cuentas (accountability) en una sociedad avanzada*. Barcelona: Icaria. ISBN 8474266165.

- NÚÑEZ FERNÁNDEZ, E., 2007. *Archivos y normas ISO*. Gijón: Ediciones Trea. ISBN 9788497043137.
- O'TOOLE, J., 2004. Archives and historical accountability: Toward a moral theology of archives. *Archivaria*, vol. 58, no. 1, pp. 3-19. ISSN 03186954.
- ÖBERG, L.-M. y BORGLUND, E., 2006. What are the Characteristics of Records? *International Journal of Public Information Systems*, vol. 1, pp. 55-76.
- OFICINA ANTIFRAUDE DE CATALUNYA, 2013. Derecho de acceso a la información pública y transparencia. Aspectos clave en su regulación. *Estudis IntegriCat*, 04.
- OLIVER, G., 2014. International records management standards: the challenges of achieving consensus. *Records Management Journal*, vol. 24, no. 1, pp. 22-31. ISSN 0956-5698. DOI 10.1108/RMJ-01-2014-0002.
- PAGE, S., 2004. Measuring accountability for results in interagency collaborates. *Public Administration Review*, vol. 64, no. 5, pp. 591-606. ISSN 00333352. DOI 10.1111/j.1540-6210.2004.00406.x.
- PALERMO, T., 2014. Accountability and Expertise in Public Sector Risk Management: A Case Study. *Financial Accountability & Management*, vol. 30, no. 3, pp. 267- 4424. ISSN 02674424. DOI 10.1111/faam.12039.
- PAPADOPOULOS, Y., 2010. Accountability and Multi-level Governance: More Accountability, Less Democracy? *West European Politics* [en línea], vol. 33, no. 5, pp. 1030-1049. ISSN 0140-2382. DOI 10.1080/01402382.2010.486126. Disponible en: <http://www.tandfonline.com/doi/abs/10.1080/01402382.2010.486126>.
- PARLAMENTO DE CATALUÑA, 2001. Ley 10/2001, de 13 de julio, de archivos y documentos. Barcelona: Parlamento de Cataluña.
- PARTRIDGE, H. y HALLAM, G., 2004. The double helix: A personal account of the discovery of the structure of [the Information Professional's] DNA. *ALIA Biennial Conference* [en línea]. Disponible en: <http://eprints.qut.edu.au/1215/>.
- PEARCE-MOSES, R., 2005. *A Glossary of Archival and Records Terminology* [en línea]. Chicago: The Society of American Archivists. ISBN 1931666148. Disponible en: <http://files.archivists.org/pubs/free/SAAGlossary-2005.pdf>
- PICKARD, A.J., 2013. Case studies. *Research Methods in Information*. London: Facet Publishing, pp. 101-110. ISBN 9781856048132.
- POLLACK, D., 2009. Legal risk, accountability and transparency in social work. *International Social Work*, vol. 52, no. 6, pp. 837-842. ISSN 0020-8728. DOI 10.1177/0020872809342663.
- POMED SÁNCHEZ, L.A., 1989. *El Derecho de acceso de los ciudadanos a los archivos y registros administrativos*. Madrid: Instituto Nacional de Administración Pública. Ministerio para las Administraciones Públicas. ISBN 8470884824.
- PRAT, A., 2006. The More Closely We Are Watched, the Better We Behave? En: C. HOOD y D. HEALD (Eds.), *Transparency: the Key to Better Governance?* Oxford: Oxford University Press, pp. 91-106. ISBN 9780197263839.
- PUCHTA, C. y POTTER, J., 2004. *Focus Group Practice*. London: SAGE Publications. International Educational and Professional Publisher. ISBN 9780761966913.

- PUIG-PEY SAURÍ, A. de P., FONTANET AMBRÓS, M., GUIU RIUS, P.J., MAURI MARTÍ, A. y PER-PINYÀ I MORERA, R., 2015. *Análisis de procedimientos administrativos para la simplificación documental en la administración local* [en línea]. 2015. Escola Superior d'Arxivística i Gestió de Documents. Disponible en: <https://ddd.uab.cat/record/132988>.
- PULLEN, T. y MAGUIRE, H., 2007. The information management risk construct: Identifying the potential impact of information quality on corporate risk. *International Journal of Information Quality*, vol. 1, no. 4, pp. 412-443. DOI 10.1504/IJIQ.2007.016716.
- QUARCHIONI, S. y TROVARELLI, F., 2013. Approaching Risk Management from a New Integrated Perspective. En: C. BUSCO, M. FRIGO, A. RICCABONI y P. QUATTRONE (Eds.), *Integrated Reporting. Concepts and Cases that Redefine Corporate Accountability* [en línea]. Springer, pp. 159-170. ISBN 9783319021676. Disponible en: https://link.springer.com/chapter/10.1007/978-3-319-02168-3_10
- RAMÍREZ ACEVES, M., 2013. Los Archivos: el marco propicio para el acceso a la información. Apuntes sobre sus orígenes. *Revista Interamericana de Bibliotecología*, vol. 36, no. 2, pp. 139-149.
- RAMS RAMOS, L., 2011. *Los documentos de archivo. Cómo se accede a ellos*. Gijón: Ediciones Trea. ISBN 9788497046008.
- RAMS RAMOS, L. y MARTÍN-RETORTILLO BAQUER, L., 2008. *El Derecho de acceso a archivos y registros administrativos*. Madrid: Editorial Reus. ISBN 9788429015386.
- RED DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN, 2014. Modelo de Gestión de Documentos y Administración de Archivos para la Red de Transparencia y Acceso a la Información. [en línea], Disponible en: <http://mgd.redrta.org/modelo-de-gestion-de-documentos-y-administracion-de-archivos-para-la-red-de-transparencia-y-acceso-a-la-informacion/mgd/2015-01-23/093820.html>.
- REED, B., 2005. Reading the records continuum: interpretations and explorations. *Archives and Manuscripts* [en línea], vol. 33, no. 1. Disponible en: http://66.29.157.249/pdf/Reading_the_Records_Continuum.pdf.
- REED, B., 2010. Managing record keeping risk. *Keeping Good Companies* [en línea], no. 2, pp. 84-88. ISSN 1444-7614. Disponible en: <http://www.records.com.au/pdf/Chartered%20Secretaries%20-%20Managing%20Risk%20Paper.pdf>.
- RIDENER, J., 2009. *From Polders to Postmodernism. A Concise History of Archival Theory*. Duluth MN: Litwin Books, LLC. ISBN 9780980200454.
- ROBERTS, A., 2005. Spin control and freedom of information: Lessons for the United Kingdom from Canada. *Public Administration*, vol. 83, no. 1, pp. 1-23. ISSN 00333298. DOI 10.1111/j.0033-3298.2005.00435.x.
- ROBERTS, A., 2006. Dashed Expectations: Governmental Adaptation to Transparency Rules. En: C. HOOD y D. HEALD (Eds.), *Transparency: the Key to Better Governance?* New York: Oxford University Press, pp. 197-126. ISBN 9780197263839.
- ROBERTS, A., 2012. WikiLeaks: the illusion of transparency. *International Review of Administrative Sciences* [en línea], vol. 78, no. 1, pp. 116-133. ISSN 0020-8523. DOI 10.1177/0020852311429428. Disponible en: <http://ras.sagepub.com/content/78/1/116.abstract>.
- RODRÍGUEZ ZEPEDA, J., 2008. Estado y Transparencia: Un paseo por la filosofía política. Ciudad de México: Instituto Federal de Acceso a la Información Pública (IFAI). Cuadernos de transparencia, 04.

- ROTHSTEIN, H., BORRAZ, O. y HUBER, M., 2013. Risk and the limits of governance: Exploring varied patterns of risk-based governance across Europe. *Regulation and Governance*, vol. 7, no. 2, pp. 215-235. ISSN 17485983. DOI 10.1111/j.1748-5991.2012.01153.x.
- ROYO MONTANÉS, S., 2008. *El Gobierno electrónico en la rendición de cuentas de la administración local*. Madrid : Instituto de Estudios Fiscales. ISBN 9788480082617.
- RUNARDOTTER, M., MÖRTBERG, C. y MIRIJAMDOTTER, A., 2011. The Changing Nature of Archives: Whose Responsibility? *Electronic Journal of e-Government*, vol. 9, no. 1, pp. 68-78.
- SAFFADY, W., 2005. Risk Analysis and Control: Vital to Records Protection. *Information Management Journal*, vol. 39, no. 5, pp. 62-68.
- SALAZAR REBOLLEDO, G., 2016. La solidez del cristal: la importancia del tiempo para explicar la calidad de las leyes de acceso a la información. *Foro Internacional* 225, vol. LVI, no. 3, pp. 684-723.
- SALKIND, N.J. y VALDÉS SALMERÓN, V., 1999. *Métodos de investigación*. Ciudad de México: Prentice-Hall. ISBN 9701702344.
- SCHAUER, F., 2011. Transparency in three dimensions. *University of Illinois Law Review* [en línea], pp. 1339-1358. ISSN 02769948. Disponible en: <https://illinoislawreview.org/wp-content/ilr-content/articles/2011/4/Schauer.pdf>
- SCHEDLER, A., 2008. ¿Qué es la rendición de cuentas? Ciudad de México: Instituto Federal de Acceso a la Información Pública (IFAI). Cuadernos de transparencia, 03.
- SCHEDLER, A., DIAMOND, L. y PLATTNER, M.F., 1999. *The Self-Restraining State. Power and Accountability in New Democracies*. Boulder: Lynne Rienner Publishers, Inc. ISBN 9781555877743.
- SHELLENBERG, T., 1996. *Modern Archives. Principles and Techniques* [en línea]. Chicago: The Society of American Archivists. Reprint of the 1956 ed. ISBN 093182849X. Disponible en: <https://babel.hathitrust.org/cgi/pt?id=mdp.39015071452539;view=lup;seq=5>.
- SCHNACKENBERG, A., 2009. Measuring Transparency: Towards a Greater Understanding of Systemic Transparency and Accountability. Cleveland: Behavior Department, Working Paper 09-02, Case Western Reserve University.
- SCHWARTZ, J.M. y COOK, T., 2002. Archives, Records, and Power: The Making of Modern Memory. *Archival Science* [en línea], vol. 2, no. 1-2, pp. 1-19. DOI <https://doi.org/10.1007/BF02435628>. Disponible en: <https://www.nyu.edu/classes/bkg/methods/schwartz.pdf>.
- SECTION ON ARCHIVAL EDUCATION (SAE), 2012. *Multilingual Archival Terminology*. 2012. ICA - International Council of Archives.
- SEMPLE, J., 1993. Proposal and Contract II. *Bentham's Prison: A Study of the Panopticon Penitentiary*. Oxford: Oxford Scholarship Online, ISBN 9780199682676.
- SHEPHERD, E., 2006. Why are records in the public sector organizational assets? *Records Management Journal* [en línea], vol. 16, no. 1, pp. 6-12. ISSN 0956-5698. DOI 10.1108/09565690610654747. Disponible en: <http://www.emeraldinsight.com/doi/full/10.1108/09565690610654747>.

- SHEPHERD, E., 2012. An 'academic' dilemma: The tale of archives and records management. *Journal of Librarianship and Information Science*, ISSN 0961-0006. DOI 10.1177/0961000611427067.
- SHEPHERD, E. y YEO, G., 2003. *Managing Records. A Handbook of Principles and Practice*. London: Facet Publishing. ISBN 9781856043700.
- SHEPHERD, E., STEVENSON, A. y FLINN, A., 2010. Information governance, records management, and freedom of information: A study of local government authorities in England. *Government Information Quarterly*, vol. 27, no. 4, pp. 337-345. ISSN 0740624X. DOI 10.1016/j.giq.2010.02.008.
- SHIMELL, P., 2002. *The Universe of Risk. How Top Business Leaders Control Risk and Achieve Success*. London: Pearson Education Limited. ISBN 0273656422.
- SMYTH, Z.A., 2005. Implementing EDRM: has it provided the benefits expected? *Records Management Journal* [en línea], vol. 15, no. 3, pp. 141-149. ISSN 0956- 5698. DOI 10.1108/09565690510632328. Disponible en: <http://www.emeraldinsight.com/doi/10.1108/09565690510632328>.
- SOLER I JIMÉNEZ, J., 2009. *Del bit al logos. Preservar documents electrònics a l'Administració local*. Barcelona: Col·lecció Estudis. Diputació de Barcelona.
- SOTO LOSTAL, S., 2011. *El Derecho de acceso a la información, el estado social y el buen gobierno*. Valencia: Tirant lo Blanch. ISBN 9788490043080.
- STRAW, J.D., BENEDETTO, A.R. y NUSYNOWITZ, M., 1976. A simplified radiopharmaceutical accountability record-keeping system. *The Journal of Nuclear Medicine*, vol. 17, pp. 1015-1017.
- THOMAS, G., 2010. *How to do your case study: a guide for students*. London: Sage Publications Ltd. ISBN 9780857025630.
- THOMASSEN, T., 2001. A First Introduction to Archival Science. *Archival Science*, vol. 1, no. 4, pp. 373-385. DOI <https://doi.org/10.1007/BF02438903>.
- THURSTON, A., 2012. Public Records: Evidence for Openness. [en línea]. Institute of Commonwealth Studies. School of Advanced Study, University of London. International Records Management Trust. Disponible en: <https://asimplicidadedascoisas.files.wordpress.com/2012/08/public-records-evidence-for-openness.pdf>.
- THURSTON, A., 2015. Right to Information. Managing Records and Information for Transparent, Accountable, and Inclusive Governance in the Digital Environment: Lessons from Nordic Countries. *International Records Management Trust*, ISSN 1098-6596. DOI 10.1017/CBO9781107415324.004.
- UPWARD, F., 1996. Structuring the Records Continuum - Part One: Postcustodial principles and properties. *Archives and Manuscripts*, vol. 24, no. 2.
- UPWARD, F., 1997. Structuring the Records Continuum, Part Two: Structuration Theory and Recordkeeping. *Archives and Manuscripts*, vol. 25, no. 1.
- VÉLEZ IBARROLLA, R., RAMOS MÉNDEZ, E., HERNÁNDEZ MORALES, V., CARMENA YÁÑEZ, E. y NAVARRO FERNÁNDEZ, J., 2006. *Métodos Estadísticos en Ciencias Sociales*. Madrid: Ediciones Académicas. ISBN 9788496062825.

- VERGARA, R., 2008. La transparencia como problema. Ciudad de México: Instituto Federal de Acceso a la Información Pública (IFAI). Cuadernos de transparencia, 05.
- VILLANUEVA, E., 2006. *Derecho de acceso a la información en el mundo*. Ciudad de México. Miguel Ángel Porrúa. ISBN 9789707018228.
- WHEELER, E., 2011a. Formulating a Risk. En: E. WHEELER (Ed.), *Security Risk Management. Building an Information Security Risk Management Program from the Ground Up* [en línea]. Elsevier Inc., pp. 87-103. ISBN 9781597496155. Disponible en: <https://www.sciencedirect.com/science/book/9781597496155>.
- WHEELER, E., 2011b. Risk Assessment Techniques. En: E. WHEELER (Ed.), *Security Risk Management. Building an Information Security Risk Management Program from the Ground Up* [en línea]. Elsevier, pp. 189-212. ISBN 9781597496155. Disponible en: <https://www.sciencedirect.com/science/book/9781597496155>.
- WHEELER, E., 2011c. The Risk Management Lifecycle. En: E. WHEELER (Ed.), *Security Risk Management. Building an Information Security Risk Management Program from the Ground Up* [en línea]. Elsevier, pp. 43-60. ISBN 9781597496155. Disponible en: <https://www.sciencedirect.com/science/book/9781597496155>.
- WHEELER, E., 2011d. Risk Evaluation and Mitigation Strategies. En: E. WHEELER (Ed.), *Security Risk Management. Building an Information Security Risk Management Program from the Ground Up* [en línea]. Elsevier, pp. 147-162. ISBN 9781597496155. Disponible en: <https://www.sciencedirect.com/science/book/9781597496155>.
- WILLIAMS, S.P. y HARDY, C.A., 2011. Information Management Issues and Challenges in an Enterprise 2.0 Era: Imperatives for Action. *24th Bled eConference eFuture: Creating Solutions for the Individual, Organizations and Society*, vol. June 12, pp. 56-67.
- XIAOMI, A., 2003. An Integrated Approach to Records Management. *The Information Management Journal*, vol. 37, no. 4, pp. 24-30.
- YEO, G., 2007. Concepts of Record (1): Evidence, Information, and Persistent Representations. *The American Archivist* [en línea], vol. 70, no. 2, pp. 315-343. ISSN 0360-9081. DOI 10.17723/aarc.70.2.u327764v1036756q. Disponible en: <http://americanarchivist.org/doi/10.17723/aarc.70.2.u327764v1036756q>.
- YIN, R.K., 2014. *Case study research: design and methods*. Los Angeles: Sage. ISBN 9781452242569.

Anexo A.

Consentimiento Informado

Yo, _____ (nombre y apellidos del participante), manifiesto mi conformidad a participar en este proyecto de investigación sobre “La gestión del riesgo aplicada a la gestión de documentos y su impacto en la rendición de cuentas pública”, que está siendo desarrollado por la estudiante de doctorado Anahí Casadesús de Mingo, dentro del Programa de Doctorado en Historia Comparada, Política y Social de la Universidad Autónoma de Barcelona.

Entiendo que el objetivo de este estudio es llevar a cabo un debate en grupo sobre la temática de la investigación y que se espera que se debatan diferentes ideas generales sobre la gestión de riesgos documentales.

Entiendo que el estudio incluye un debate siguiendo la metodología del *Focus Group*, que tiene prevista una duración de dos horas o menos, y que éste será grabado.

Entiendo que mi participación en este estudio es totalmente voluntaria, y que si deseo abandonar el estudio o dejar el debate, puedo hacerlo en cualquier momento sin necesitar ninguna justificación o explicaciones para ello. Si decido abandonar el debate, entiendo que esto no tendrá ningún efecto en mi relación con la Universidad Autónoma de Barcelona ni con cualquier otra organización relacionada.

Entiendo que, a raíz de este estudio, podrían darse violaciones de mi privacidad. Para prevenir que esto pueda pasar, se me ha sugerido no comentar ningún aspecto relacionado con experiencias personales que considere demasiado personales o reveladoras.

Entiendo también que tengo la obligación de respetar la privacidad de los otros miembros del grupo de debate y que esto incluye no hacer pública ninguna información personal que ellos puedan compartir durante el debate.

Entiendo que la información que proporcione permanecerá confidencial en las líneas de lo marcado por la ley, y que los nombres de todas las personas de este estudio se mantendrán en la confidencialidad.

Entiendo que no recibiré ningún beneficio directo de la participación en este estudio, aunque mi participación sí puede ayudar a otras personas en el futuro.

Los miembros del equipo de investigación se han mostrado disponibles a contestar cualquier pregunta que pueda tener sobre el estudio, así como sobre lo que se espera de mí.

He leído y entendido esta información y estoy de acuerdo en formar parte del estudio.

Fecha y firma del participante

Anexo B.

Documento para la comunicación previa a las partes interesadas

Proyecto de análisis de la gestión de riesgos en la Organización X en el marco del desarrollo de una Tesis Doctoral de la Universidad Autónoma de Barcelona

En el marco del desarrollo de la tesis doctoral en gestión de riesgos aplicada a la gestión de la información y los documentos se ha escogido como prueba piloto de aplicación de la metodología y análisis de resultados a la Organización X.

Para llevar a cabo dicha prueba piloto se ha definido un alcance reducido que afecta a todo aquello relacionado con el desarrollo y puesta en funcionamiento de la administración electrónica. Es por este motivo que solicitamos tu colaboración para participar en la primera fase, a través de una entrevista sobre el conocimiento que en la organización se tiene de esta aplicación de la gestión de riesgos.

Previamente a la entrevista, se enviará un guión de los temas a tratar por si pudiera resultarte útil. Ten en cuenta que no se pretende evaluar los conocimientos técnicos ni evaluar a las personas implicadas, sino conocer el estado de la cuestión dentro del Ayuntamiento con el objetivo de realizar una investigación teórica dentro del desarrollo de una tesis doctoral.

En caso de que tengas alguna duda puedes contactar con nosotros en el correo electrónico: anahi.casadesus@uab.cat y estaré encantada de poder ayudarte así como de recibir tus sugerencias.

Recibe un cordial saludo,

Anahí Casadesús de Mingo

Anexo C.

Transcripción no literal de las entrevistas semiestructuradas

Se realizaron cinco entrevistas en el proceso de estudio del contexto y la identificación de riesgos:

ENTREVISTA	INTERLOCUTOR	FECHA
1	Entrevista al Jefe del Servicio de Atención Ciudadana de la Organización X	18/11/2016
2	Entrevista a uno de los responsables del Servicio de Prevención de Riesgos Laborales de la Organización X	28/11/2016
3	Entrevista con el responsable del Servicio de informática	28/11/2016
4	Entrevista al Responsable del Servicio de gestión documental y archivo	12/12/2016
5	Entrevista al Responsable del Servicio de Organización y Proyectos de Mejora, también responsable de Transparencia	29/03/2017

Figura 131 - Índice de entrevistas realizadas en la Organización X (elaboración propia).

A continuación se presenta la traducción no literal de cada una de las entrevistas, en el orden en que fueron realizadas.

Entrevista número 1

Jefe del Servicio de Atención Ciudadana de la organización X

Fecha: 18 de noviembre de 2016

Duración de la entrevista: 34 minutos

Las respuestas obtenidas se detallan a continuación:

1. ¿Qué es para ti un riesgo? ¿Y un riesgo documental o riesgo de gestión documental?

El entrevistado comenta que en el ámbito laboral siempre ha entendido los riesgos desde la perspectiva de riesgos laborales, de la prevención. Comenta que es la perspectiva desde la que siempre ha tratado el riesgo. En este sentido, afirma que en su departamento se dan algunos. Eso es así por el mero hecho de tratar con las personas ya que en ocasiones comenta que se dan conflictos.

Desde la perspectiva documental, el entrevistado explica que desde que empezó a trabajar con la Unidad de Gestión de la Población, con el Padrón de Habitantes, se le plantearon algunas dudas al ver cómo estaba organizada y conservada la documentación. Explica que el archivo de gestión no estaba en las condiciones que él consideraba las adecuadas, tanto a nivel de conservación de los documentos como a nivel de organización y ubicación. Comenta que esto le generó también dudas sobre las transferencias que efectuaban al archivo, como por ejemplo que se estuviesen enviando los documentos que debían enviar.

2. ¿A qué áreas de la organización crees que pueden afectar los riesgos documentales?

En relación a las instancias, los departamentos de mayor riesgo según el punto de vista del entrevistado son Espacio Público, Urbanismo, y Seguridad Ciudadana. Son áreas muy grandes y que prestan muchos servicios, por tanto también deben dar respuesta a muchas instancias. Pese a ello, no existe un procedimiento definido y no se gestionan las instancias de manera centralizada. Eso conlleva que dentro de un mismo departamento se realice el mismo procedimiento de maneras distintas.

3. ¿Crees que tu trabajo puede estar afectado por algún tipo de riesgo documental? ¿Puedes poner algún ejemplo?

Responde afirmativamente. Indica que las condiciones físicas del archivo del padrón de habitantes no son las adecuadas para la conservación de los documentos. Por ejemplo, explica que en el edificio hay goteras y que hace unas semanas, tras un episodio de lluvias fuertes se encontró el armario donde guarda los documentos de las gestiones del día a día con agua procedente de estas goteras. Como medida de prevención comenta que, cuando hay previsión de lluvia, desplazan los armarios y los alejan de la zona de riesgo. En cualquier caso, afirma que no se ha perdido ningún documento.

Comenta también que con el sistema de distribución interno que está funcionando en la organización se ha dado el caso de perder alguna instancia, no en el proceso de registro sino al derivarlas al departamento de gestión correspondiente.

También apunta a una falta de control de los documentos (según su experiencia, al menos las instancias) por parte de los departamentos que reciben las instancias y son responsables de realizar algún trámite o gestión al respecto. Para contextualizar este riesgo el entrevistado explica que ha intentado obtener información para elaborar estadísticas de respuesta y resolución de instancias y comenta que muchos son los departamentos que no han podido dar una información concreta al respecto ya sea por desconocimiento o por falta de seguimiento del trámite. Añade que, en caso de que se inicie expediente a partir de la instancia recibida, seguramente esta se conserve y las gestiones se realicen de manera adecuada pero también le plantea dudas si todas las instancias que él considera que deberían haber generado un expediente o actuación, se conservan. Comenta que quizás esta problemática se relacione con la cultura de la organización. El gran problema que tienen en los diferentes departamentos es que no son capaces de

localizar las instancias porque no saben dónde están, ni si se ha dado respuesta, ni quién o cuándo. Esto le hace pensar que no se deben clasificar y archivar de manera adecuada, lo que comporta riesgos.

Otra cuestión que comenta se refiere a la respuesta que se da al ciudadano después de presentar una instancia. El entrevistado ha constatado como en ocasiones no se genera ninguna evidencia documental sino que se llama por teléfono al ciudadano y se añade una nota manuscrita a la instancia indicando que se llamó por teléfono a la persona pero no se documenta la respuesta. Explica que no se dispone de un procedimiento normalizado de actuación frente a la recepción de instancias y que, por tanto, se dan muchas casuísticas distintas incluso dentro de un mismo departamento.

Otra situación que comenta se relaciona con la inaccesibilidad a algunos documentos debido al paso del tiempo. Explica que los documentos que ha ido generando a lo largo de su vida laboral se han conservado en versiones obsoletas y no ha podido recuperarlos. Cree que nadie se ha preocupado de actualizar las versiones y se han ido quedando inaccesibles. Eso sí, comenta que esta situación se da mayoritariamente con documentos de trabajo como, por ejemplo, documentos de análisis económicos o de análisis demográficos. No son documentos que formen parte de un expediente administrativo. Finalmente, añade que los destruyeron porque no tenían utilidad ni eran recuperables.

Se pregunta qué pasa con los documentos que no han llegado a formar parte de un expediente administrativo pero que han sido documentos de base para iniciar expedientes. Pone como ejemplo el documento de planificación de un proyecto. Explica un caso concreto: un plan de barrios. Se inicia con un diagnóstico, que puede hacerse tanto por personal de la organización como por personal externo: esto implica realizar un estudio social, económico, demográfico, urbano, etc. De este diagnóstico se entrega un documento base a la Organización X, para conocer los problemas a los que deberá darse solución. Posteriormente se desarrolla un plan y una memoria económica donde se enumera todo aquello detectado y se explica cómo se abordará, los plazos de ejecución y la valoración económica. A partir de aquí se inicia el proyecto y el primer paso podría ser, por ejemplo, la rehabilitación de viviendas. El entrevistado afirma que esto sí genera uno o varios expedientes, pero todo lo anteriormente explicado, según su experiencia, deja de existir. Añade que si alguien quiere conocer las actuaciones llevadas a cabo por la organización lo podrá hacer sin problemas pero que no podrá saber cómo se gestionó el proceso previo, ya que la documentación explicada no forma parte de los expedientes administrativos. El entrevistado, además, cree que no se conserva.

4. ¿Sabes si en el Ayuntamiento existe alguna metodología para prevenir o tratar los riesgos? ¿Se te ha explicado alguna vez dicha metodología?

Sí que ha oído hablar de prevención de riesgos laborales y considera que se ha hecho muy buena gestión y formación sobre ello. Se le ha explicado el funcionamiento y comenta que se realiza formación de manera periódica.

También menciona la existencia de un Plan de seguridad, a nivel tecnológico, y la realización periódica de auditorías de riesgos tecnológicos, cree. No conoce muy bien qué se audita pero sí considera que existe preocupación por el control de los riesgos informáticos. No se le ha explicado el funcionamiento y supone que esto es así debido a que es una cuestión propia del departamento informático.

5. En caso de que la respuesta anterior sea afirmativa, ¿te parece adecuada también para el control de los documentos que generas y gestionas en tu día a día?

Conoce el funcionamiento de la prevención de riesgos laborales pero sin una adaptación a la gestión documental. En relación a temas de seguridad menciona que se trata más bien de una cuestión interna del departamento informático y desconoce las implicaciones que en su área podría tener.

6. ¿En tu departamento lleváis a cabo algún control sobre los posibles riesgos documentales? En caso de que no, ¿consideras que sería necesario?

El entrevistado afirma que no se llevan a cabo controles sobre riesgos documentales en su departamento. En cambio, sí considera necesario disponer de una metodología apropiada.

Explica que están trabajando con los responsables de gestión documental en la simplificación de trámites con la finalidad de no generar tantos documentos. Considera que esto puede ser una medida preventiva ya que, desde su punto de vista, cuanto menos “papeles” archiven en el departamento más se minimizan los riesgos. Con este criterio lo que están intentando es simplificar los procedimientos.

7. ¿Consideras que existe un mayor riesgo al trabajar con documentos electrónicos? ¿Por qué sí/no?

Considera que en el entorno electrónico existe menor riesgo y que trabajando con documentos electrónicos se minimizan los riesgos, ya que no se exponen los documentos a pérdidas o a degradaciones. En caso de perderse o destruirse una base de datos siempre existen réplicas y copias de seguridad, por lo que el riesgo es menor. Cree, por tanto, que el entorno electrónico es más seguro siempre y cuando se gestione de manera adecuada.

Considera el paso al registro electrónico como prioritario y está convencido de que se generarán muchos menos errores que en papel, además de ganar agilidad en la tramitación.

Entrevista número 2

Entrevista a uno de los responsables del Servicio de Prevención de Riesgos Laborales de la Organización X

Fecha: 28 de noviembre de 2016

Duración de la entrevista: 80 minutos

Las respuestas obtenidas se detallan a continuación:

1. ¿Qué es para ti un riesgo? ¿Y un riesgo documental o riesgo de gestión documental?

El entrevistado explica que en su contexto de trabajo la definición de riesgo viene fijada por la legislación, en concreto por la Ley de Prevención. En relación a la gestión documental se pregunta en base a qué normativa podrían identificarse los riesgos concretos, si existen parámetros o valores definidos para realizar la identificación de riesgos que estén publicados y aprobados.

Añade que a nivel de riesgos laborales se dispone del soporte técnico del Instituto de Seguridad e Higiene en el Trabajo, que es un organismo técnico científico que publica normativa y directrices de manera regular. Comenta que algunas de las publicaciones se refieren a la gestión de documentos en un servicio de prevención⁸⁷. Explica que estas notas técnicas marcan la documentación que debe custodiarse de manera obligatoria por un servicio de prevención, sobre todo en relación a los procesos de inspección o auditoría a los que puede someterse el servicio. Esto es así debido a la gran cantidad de documentación que se genera en la prevención de riesgos laborales, con la finalidad de facilitar la gestión.

En su caso particular, un riesgo documental puede ser por ejemplo no encontrar un documento de evaluación de un colectivo de un trabajador porque el servicio de prevención está sometido a un control externo, como puede ser una inspección de trabajo. Por tanto, explica que siempre debe tener toda la información bien custodiada y bien definida.

2. ¿A qué áreas de la organización X crees que pueden afectar los riesgos documentales?

El entrevistado considera que los riesgos documentales pueden afectar a todas las áreas de la organización, desde distintos ámbitos, ya sea desde la vertiente tecnológica, legal, de transparencia u otras. Considera que en función de las consecuencias de los riesgos identificados se actuará de una manera u otra. Por ejemplo se dará mayor prioridad a aquellas áreas que trabajan directamente con los ciudadanos.

⁸⁷ – Se refiere a la *Nota Técnica de Prevención (NTP) 484: Documentación del sistema de prevención de riesgos laborales (I)*, la *NTP 485: Documentación del sistema de prevención de riesgos laborales (II)* y la *NTP 591: Documentación del sistema de prevención de riesgos laborales (III): registros documentales*. Están disponibles a través del siguiente enlace de la página web del Instituto Nacional de Seguridad e Higiene en el Trabajo, del Ministerio de Empleo y Seguridad Social: http://www.insht.es/portal/site/Insht/menuitem.1f1a3bc79ab34c578c2e8884060961ca/?vgnextoi_d=72abae6588c35410VgnVCM1000008130110aRCRD&vgnextchannel=db2c46a815c83110Vg_nVCM-100000dc0ca8coRCRD (consultado el 02/08/2018).

Define la organización X como “un reino de taifas” y, en ocasiones, además con una casuística muy específica por departamento. Comenta que hay mucha diversidad, a nivel legal, a nivel de dimensiones de las áreas, entre otras cuestiones.

3. ¿Crees que tu trabajo puede estar afectado por algún tipo de riesgo documental? ¿Puedes poner algún ejemplo?

Explica que en la Organización X se tienen cajas de documentación en algunos depósitos sin identificar, que pueden contener documentos que pueden estar accesibles a personas que no deberían tener acceso. Añade que tampoco están definidos los procesos en relación con la conservación o preservación. Pone el ejemplo de depósitos en los que ha visto insectos.

Comenta también que en el servicio de prevención se cuenta con un área médica que genera documentación sensible que está sujeta a un régimen especial de protección de datos. Tienen los documentos antiguos en papel, en un armario bajo llave. La llave está custodiada por el médico que debe realizar la gestión y seguimiento de los expedientes. Comenta que han externalizado la gestión de este tipo de documentación y que ahora se conserva en la nube. Lo ve como un aspecto positivo.

Afirma que tienen una asignatura pendiente en el tema de la documentación. No hay criterios sobre qué documentación es la esencial y qué documentación debe formar parte de un expediente. No disponen de directrices sobre qué se puede eliminar y qué deben conservar. Explica que se han reunido con el responsable de gestión documental pero todavía no se han dedicado a ello por falta de recursos y tiempo en el servicio de prevención. Considera fundamental tener criterios establecidos.

Otro riesgo identificado por el entrevistado es la transformación digital. En este caso se refiere a esta situación como un riesgo de carga mental para las personas derivado de una mala gestión del cambio, por tanto no se trata de un riesgo documental propiamente. Explica que se debería tratar el paso a la administración electrónica como un cambio cultural de la organización, como un proceso que debe trabajarse con tiempo suficiente y dando la formación necesaria a todas las personas implicadas y con buena pedagogía. Además, añade que la formación está siendo insuficiente y muchas personas desconocen cómo trabajar con las nuevas aplicaciones, por ejemplo la facturación electrónica. Esto supone otro tipo de riesgos documentales que para el entrevistado son importantes.

Otro de los riesgos que apunta se relaciona con el sistema de trabajo en red compartida. Por ejemplo, para el entrevistado la eliminación o manipulación incorrecta de documentos serían riesgos, aunque añade que se realizan copias de seguridad que permiten recuperar los documentos eliminados si se detecta a tiempo. Con relación a estos riesgos, comenta que deberían definirse mejor los permisos de acceso a las carpetas compartidas para evitar riesgos.

Con relación al entorno en papel, sobre todo hace referencia a las condiciones de conservación y al control físico de acceso a la documentación. No se realiza ningún control sobre las consultas de expedientes, con lo que puede darse la situación de que un técnico coja prestado un expediente de una unidad de instalación para consultarla en su despacho y se olvide de devolverlo o se archive mal al devolverlo.

Comenta que han realizado eliminaciones de documentos. Concretamente explica el caso de los documentos generados para el cobro de la paga por productividad de los trabajadores de la organización según convenio. Explica que se trataba de documentación no vigente, con el trámite cerrado y sin posibilidad de reclamación y es por ello que se decidió eliminarla. No se solicitó autorización al departamento de gestión documental ni se siguió ningún procedimiento reglado o normalizado de destrucción.

4. ¿Sabes si en la organización existe alguna metodología para prevenir o tratar los riesgos? ¿Se te ha explicado alguna vez dicha metodología?

La metodología que conoce es la relacionada con la prevención de riesgos laborales, que se deriva de la normativa laboral. Disponen de una metodología para realizar la evaluación de los riesgos que pueden afectar a un trabajador en su día a día. Da una especial importancia al seguimiento de las medidas preventivas y a la posibilidad de eliminar los riesgos, en caso de que sea posible.

Desconoce si existen otras metodologías de gestión de otro tipo de riesgos.

5. En caso de que la respuesta anterior sea afirmativa, ¿te parece adecuada también para el control de los documentos que generas y gestionas en tu día a día?

El entrevistado considera adecuada la metodología existente de prevención de riesgos para aplicar a la gestión documental. Los pasos de identificar, analizar, tratar y realizar el seguimiento son perfectamente aplicables. Explica que en el caso de los riesgos laborales existe mucha normativa en la que se indican los aspectos a considerar y que en gestión documental se podría partir también de la legislación aplicable.

Considera que algunos aspectos pueden resultar útiles y funcionales para la gestión de riesgos documentales, como algunas de las tipologías de riesgos, que se podrían aprovechar a la hora de analizar riesgos documentales.

No sólo le parece adecuada la metodología sino que, añade, “me parece urgente y necesaria”.

6. ¿En tu departamento lleváis a cabo algún control sobre los posibles riesgos documentales? ¿Consideras que sería necesario?

En el departamento tienen implantada la norma UNE-ISO 9001: 2008 y, por tanto, siguen los procedimientos establecidos en relación a dicha norma. Esto implica definir la documentación que se genera para cada proceso, el tiempo de conservación y el régimen de acceso. Comenta que pese a que en muchas ocasiones la retención está fijada en 5 años, en realidad no se realiza eliminación de documentos en el departamento.

Considera muy importante disponer de unas mínimas directrices sobre gestión documental. El entrevistado comenta que no conoce si existen pautas o normativa. Por tanto, en el servicio se actúa de buena fe pero con criterios propios en función de sus necesidades.

7. ¿Consideras que existe un mayor riesgo al trabajar con documentos electrónicos? ¿Por qué sí/no?

El entrevistado percibe un mayor riesgo en el entorno electrónico que en el entorno papel. Para contextualizar su respuesta explica una incidencia con la validación de una factura electrónica que se ha hecho por desconocimiento del funcionamiento de la aplicación. Posteriormente se ha comprobado que era una factura correcta pero ya se había hecho la validación previamente.

Otra causa de esta percepción es el desconocimiento del funcionamiento de las nuevas aplicaciones para la transformación digital, relacionado también con una mala gestión del cambio. Comenta la inseguridad que supone la desinformación y la falta de formación.

Entrevista número 3

Entrevista con el responsable del Servicio de informática

Fecha: 28 de noviembre de 2016

Duración de la entrevista: 18 minutos

Las respuestas obtenidas se detallan a continuación:

1. ¿Qué es para ti un riesgo? ¿Y un riesgo documental o riesgo de gestión documental?

Define el riesgo como la posibilidad o la probabilidad de que pase algo que ponga en peligro los sistemas de la organización. En principio el entrevistado lo percibe como algo negativo puesto que nadie quiere estar expuesto a riesgos, aunque también explica que los riesgos deben verse como una oportunidad de mejora. Estos se pueden compensar, prever, planificar o estudiar pero no se pueden evitar.

Al hablar de riesgos documentales el entrevistado, en primer lugar, hace una diferenciación entre los documentos en papel y los electrónicos, pese a que el primer riesgo que identifica es la pérdida de un documento y afirma que afectaría a ambos entornos. Su percepción es de que existe un riesgo mucho más elevado trabajando en entorno en papel. Otro ejemplo de riesgo que explica es la fuga de información⁸⁸ o también las filtraciones de contenido, derivándose consecuencias relacionadas con incumplimientos de la ley de protección de datos personales. También incluye las amenazas sobre la tecnología, como por ejemplo los virus o también los dispositivos de almacenaje de información, que pueden fallar. Comenta que todo lo explicado puede afectar a cualquier tipología de documento, entendiendo como tipologías los vídeos, fotografías, documentos en formato Word o formato PDF. Continúa con los riesgos asociados a la obsolescencia tecnológica explicando que existe la posibilidad de perder documentos si no se actualiza su formato. En relación a esta última situación de riesgo añade que la obsolescencia puede también afectar a la firma electrónica.

Un aspecto que considera importante es no hacer públicos los riesgos a los que se exponen ya que eso les haría más vulnerables de cara al exterior. Considera que ya se es vulnerable sin publicar las vulnerabilidades.

2. ¿A qué áreas de la organización crees que pueden afectar los riesgos documentales?

Afirma que todas las áreas de la Organización X están expuestas a riesgos documentales. Añade que el archivo puede estar más expuesto a temas de conservación de los documentos en papel y necesitará disponer de una infraestructura dedicada a la preservación de las condiciones adecuadas. También el departamento de informática está más expuesto, por ser responsable de la administración electrónica, del mantenimiento de los servidores, y de la

⁸⁸ – Con fuga de información el entrevistado explica que se refiere a que los trabajadores pueden extraer información de la organización (sea con buena o mala intención) y ésta puede acabar expuesta a un mal uso por un tercero.

seguridad y acceso a la información. Pero repite que todos los departamentos trabajan con documentos y gestionan información. De hecho, son quienes gestionan dicha información y los riesgos asociados a los documentos les afectan directamente.

3. ¿Crees que tu trabajo puede estar afectado por algún tipo de riesgo documental? ¿Puedes poner algún ejemplo?

Responde afirmativamente. Añade que le afectan todos los riesgos relacionados con la conservación y con la seguridad del sistema, con el control y el acceso a los datos, con la recuperación tras un fallo del sistema, la gestión de copias de seguridad, la gestión de antivirus, entre otros. En este punto añade la metodología del Esquema Nacional de Seguridad (ENS), que da soporte a toda esta casuística y establece las medidas de seguridad que se deben tomar en cada caso. Hay un Comité de Seguridad en la organización, del que el entrevistado forma parte, que tiene la labor de detectar los riesgos e implementar las medidas necesarias para tratarlos, realizando también el seguimiento de dichas medidas.

También comenta que el servicio de informática tiene un papel muy importante en el control de la ley de protección de datos personales y los riesgos asociados.

4. ¿Sabes si en la organización X existe alguna metodología para prevenir o tratar los riesgos? ¿Se te ha explicado alguna vez dicha metodología?

Responde afirmativamente. Añade que se está trabajando con el ENS y que se ha contratado a una empresa especializada para ayudar con el proceso. Además se ha realizado una auditoría, un plan de trabajo a seguir y evaluar.

Desconoce si existe otra metodología en la organización para la gestión de riesgos. Añade que, debido a su cargo dentro de la organización, conoce la existencia de una aplicación informática de prevención de riesgos laborales pero comenta que no se le ha explicado la metodología que siguen.

5. En caso de que la respuesta anterior sea afirmativa, ¿te parece adecuada también para el control de los documentos que generas y gestionas en tu día a día?

La metodología del ENS le parece adecuada para ser aplicada a la gestión de documentos. Explica que pone unos límites y orienta sobre cómo gestionar los riesgos. Añade que, probablemente, sería mejorable pero que es un buen comienzo.

6. ¿En tu departamento lleváis a cabo algún control sobre los posibles riesgos documentales? ¿Consideras que sería necesario?

Responde afirmativamente. Explica que se aplican en la medida de lo posible los controles que sugiere el ENS: controles de acceso por contraseña, realización y recuperación de copias de seguridad, entre otros. En cualquier caso, considera que es mejorable y explica que en las auditorías que han pasado siempre se detectan aspectos que pueden mejorarse, pero se lleva a cabo un control para evitar situaciones de riesgo en relación con los documentos.

Considera que disponer de esta metodología es algo necesario.

7. ¿Consideras que existe un mayor riesgo al trabajar con documentos electrónicos? ¿Por qué sí/no?

Explica que en la organización no están trabajando con la administración electrónica y esto es un problema muy grave debido a que los documentos en papel se trasladan entre departamentos y en ocasiones se pierden. Esto es un riesgo importante y, por tanto, la administración electrónica para el entrevistado es un tema muy prioritario. A partir de esta explicación afirma que los documentos en papel tienen riesgos mucho mayores que los documentos electrónicos. Pone varios ejemplos: en la firma de un documento en papel que consta de varias páginas puede darse el caso de que tan sólo se firme la última página y que el resto del documento pueda modificarse posteriormente; en caso de que se firmen todas las páginas del documento no puede garantizarse que se hayan firmado el mismo día y tampoco que no se hayan realizado modificaciones a posteriori. Estos serían, según el entrevistado, ejemplos de riesgos que afectan a los documentos en papel y que, en cambio, no afectan a los documentos electrónicos.

Añade además, la falta de trazabilidad en las acciones que se realizan sobre los documentos en papel.

Al trabajar con documentos electrónicos se gana en seguridad respecto al entorno papel. De hecho, se está exigiendo más seguridad de la que se exigía en los entornos tradicionales en papel. Por tanto, para el entrevistado, con la implantación de la administración electrónica se da un salto abismal en la seguridad y en el control de los documentos. Considera la administración electrónica como “la estrategia de prevención de riesgos”: trazabilidad, acceso, usabilidad, integridad,... tiene numerosas ventajas en relación a los documentos, además de otras relacionadas con la velocidad de la tramitación, la optimización de procesos y la mejora de los tiempos de gestión. Concluye afirmando que se consigue ser más ágil a la vez que se es más seguro.

Entrevista número 4

Entrevista al Responsable del Servicio de gestión documental y archivo

Fecha: 12 de diciembre de 2016

Duración de la entrevista: 29 minutos

Las respuestas obtenidas se detallan a continuación:

1. ¿Qué es para ti un riesgo? ¿Y un riesgo documental o riesgo de gestión documental?

El entrevistado entiende como riesgo cualquier situación que se debe tener en cuenta y prever con el fin de poder valorar las afectaciones que puede tener y cómo actuar en caso de que ocurra. Lo resume como todo aquello que se debe tener en cuenta antes de empezar cualquier proyecto. Explica que, para él, la connotación del término riesgo es más negativa que positiva, aunque añade que en caso de que se pueda prever, será positivo.

Como riesgo documental incluye de todo este tipo de situaciones, que podrían afectar a la gestión de documentos. Según su punto de vista, un ejemplo típico sería la no localización de un documento. Menciona, además, que en el entorno electrónico un riesgo que le preocupa es cómo asegurar la autenticidad de los documentos, considera que no se ha trabajado suficiente el tema.

2. ¿A qué áreas de la organización crees que pueden afectar los riesgos documentales?

Afirma que afectan a todas las áreas productoras de documentos. Añade que, desde el momento en que se genera un documento o se debe realizar algún trámite o gestión con un documento, se podrían dar riesgos. Por tanto, afirma que afecta a todas las áreas de la organización.

3. ¿Crees que tu trabajo puede estar afectado por algún tipo de riesgo documental? ¿Puedes poner algún ejemplo?

Responde afirmativamente. Comenta que, una vez que la custodia de los documentos en papel se transfiere al archivo, si los procesos no se controlan de manera adecuada se pueden generar riesgos. Como ejemplo explica que por falta de recursos actualmente no están pudiendo llevar a cabo la verificación de las transferencias (comprobar que los documentos que las áreas dicen que están transfiriendo al archivo se corresponden realmente con los documentos transferidos). Otra situación de riesgo que les afecta es que, también por falta de recursos, no pueden realizar el control de los expedientes que se prestan a las unidades gestoras para su consulta. Por este motivo no se puede garantizar que cuando se devuelve el expediente desde la unidad que solicitó el préstamo al archivo, este esté completo y contenga todos los documentos. Además explica que los expedientes no están foliados ni contienen índice, con lo que la dificultad de control es aún mayor.

A esto se suma el desconocimiento de los trabajadores sobre el procedimiento administrativo y el concepto de expediente. Explica que se han encontrado casos de expedientes devueltos de un préstamo a los que se habían añadido nuevos documentos, ya que los trabajadores entienden los expedientes como su dossier de seguimiento del asunto a tramitar. Considera que este es un riesgo muy grave. El problema principal para el entrevistado es la falta de definición de lo que es un expediente en la organización.

Añade el riesgo del poco control que se tiene en la organización sobre los archivos de gestión, ni desde el departamento de archivo (indica que por falta de tiempo y recursos) ni desde las propias áreas de gestión. No conoce cuánta documentación se tiene en las áreas y añade que no se sigue el calendario de transferencias, sino que éstas se realizan a petición de las áreas de gestión en función de los criterios que consideran oportunos.

Otro aspecto que destaca es que la Organización X dispone de varios edificios localizados por la ciudad en la que se encuentra, que están separados físicamente. Comenta que el envío de documentos en papel entre departamentos de edificios distintos puede generar riesgos, como por ejemplo el retraso en la tramitación administrativa. También se han dado casos de pérdida de documentos, aunque el entrevistado no considera que sea destacable puesto que no suele ocurrir.

Con relación a los depósitos, menciona tener problemas con la climatización, puesto que tan sólo tienen control sobre la temperatura pero no sobre la humedad. Esto implica tener que disponer de deshumidificadores y controles manuales, cosa que puede poner en riesgo la conservación preventiva. Además, añade que el sistema no funciona bien y hay algunos depósitos sin garantías de conservación de las condiciones de humedad y temperatura adecuadas. Comenta que han informado en numerosas ocasiones pero que la solución pasa por cambiar el sistema de climatización de todo el edificio y actualmente no es viable.

También en relación con los depósitos de archivo, explica que han tenido incidencias con goteras y añade que pasa de manera periódica. Eso sí, no ha habido afectación sobre los documentos por humedad.

4. ¿Sabes si en el Ayuntamiento existe alguna metodología para prevenir o tratar los riesgos? ¿Se te ha explicado alguna vez dicha metodología?

No conoce si existe alguna metodología pero deduce que a nivel de riesgos laborales sí debe existir. Afirma que no se le ha explicado, aunque sí comenta que recibió una formación sobre cómo actuar en caso de emergencia y sobre la evacuación del edificio donde trabaja. En cualquier caso, afirma que no se le ha explicado la metodología de gestión de riesgos, ni ha recibido formación al respecto.

5. En caso de que la respuesta anterior sea afirmativa, ¿te parece adecuada también para el control de los documentos que generas y gestionas en tu día a día?

No aplica.

6. ¿En tu departamento lleváis a cabo algún control sobre los posibles riesgos documentales? En caso de que no, ¿consideras que sería necesario?

Explica que lo que se intenta desde su departamento es hacer pedagogía sobre la gestión documental. También están trabajando con las áreas con las que más incidencias tienen, en la definición de los expedientes: por ejemplo, cuándo debe cerrarse un expediente, que una vez cerrados los expedientes no deben incluirse más documentos, entre otras cuestiones. Comenta que todos estos conceptos se transmiten también en las diferentes acciones formativas que llevan a cabo. Las formaciones se realizan tanto de manera puntual como en promociones internas.

Comenta que la inexistencia de mecanismos para tener controlada la documentación facilita las situaciones de riesgo. Cuando detectan una situación de este tipo lo primero que hacen es hablar con el área implicada para solucionarlo. El entrevistado destaca como una situación de riesgo importante el hecho de no detectar estas situaciones, porque no puede darse solución.

En relación a la segunda pregunta, considera que disponer de una metodología de gestión de riesgos referida a la administración electrónica resultaría muy útil para identificar problemáticas y prioridades. No han desarrollado ninguna metodología y considera que sería muy difícil desarrollarla debido a los pocos recursos que tienen. En cualquier caso, sí lo considera necesario.

7. ¿Consideras que existe un mayor riesgo al trabajar con documentos electrónicos? ¿Por qué sí/no?

Considera que el entorno papel le genera mayor tranquilidad, sobre todo en temas de seguridad, por el mero hecho de tener los documentos almacenados en un único lugar bajo llave. El entorno electrónico no le genera esta tranquilidad, y explica que quizás sea por su desconocimiento tecnológico.

El entrevistado no cree que existan riesgos diferentes por el entorno sino que la manera de abordarlos es diferente. Explica que puede ser que exista el mismo riesgo en ambos entornos pero en el electrónico puede resultar más problemático o con mayores consecuencias que en el papel. Añade que la existencia de mayor o menor riesgo no depende tanto del entorno como del riesgo identificado. Pone como ejemplo los préstamos de documentos en papel a las oficinas gestoras, que implican riesgos que en cambio en un entorno electrónico no se darían.

También considera el paso a la administración electrónica como una oportunidad para poner orden y solucionar aspectos que ahora mismo no controlan en el entorno papel. Pero también apunta que existe un gran desconocimiento sobre qué implica el cambio.

Otro de los aspectos que destaca es la necesidad de colaboración interdepartamental y multidisciplinar en el proceso hacia la administración electrónica, cosa que para el entrevistado implica mayores dificultades. Concluye afirmando que los riesgos dependerán de cómo se diseñe el sistema, más que de si se trabaja en un soporte o en otro.

Entrevista número 5

Entrevista al Responsable del Servicio de Organización y Proyectos de Mejora, también responsable de Transparencia

Fecha: 29 de marzo de 2017

Duración de la entrevista: 22 minutos

Las respuestas obtenidas se detallan a continuación:

1. ¿Qué es para ti un riesgo? ¿Y un riesgo documental o riesgo de gestión documental?

El entrevistado define el riesgo como la posibilidad o las probabilidades de que algo vaya mal. En relación a la gestión documental, considera como riesgos la imposibilidad de encontrar la documentación cuando se necesite, que no esté bien clasificada, bien ordenada, que no pueda localizarse o que se haya perdido. También que no pueda garantizarse que un documento que se sube al portal de transparencia es auténtico y es íntegro.

Para el entrevistado, la Ley de Transparencia⁸⁹ pone en evidencia cómo las organizaciones tienen los sistemas de información y cómo tienen organizada la documentación. Explica que hasta ahora, la gestión de documentos se quedaba en el ámbito interno pero desde el momento en que el ciudadano tiene la posibilidad de solicitar acceso a alguna información, no ser rápidos dando respuesta o no proporcionarla con las suficientes garantías pone en evidencia a la administración. Esto ha ayudado a poner sobre la mesa cómo se gestiona y ordena la información. Según su opinión, se consigue que la gestión documental deje de ser una asignatura pendiente para pasar a ser una obligación y a convertirse en una prioridad. Lo considera positivo, ya que se han conseguido mejoras pero también expone el trabajo que queda por hacer.

2. ¿A qué áreas de la organización X crees que pueden afectar los riesgos documentales?

Considera que afectan a cualquier área que sea productora de documentos. Afecta a las áreas gestoras de procesos (por ejemplo deportes, cultura), a servicios centrales, al archivo o al departamento con responsabilidades en gestión documental. Por tanto, para él afecta a todas las áreas que produzcan documentos, que los gestionen y a los responsables sobre su futura conservación.

⁸⁹ – Se refiere a la *Ley 19/2014, de 29 de diciembre, de transparencia, acceso a la información pública y buen gobierno*, disponible en: <https://www.boe.es/buscar/pdf/2015/BOE-A-2015-470-consolidado.pdf> (consultado el 02/08/2018).

3. ¿Crees que tu trabajo puede estar afectado por algún tipo de riesgo documental? ¿Puedes poner algún ejemplo?

Sí puede estar afectado su trabajo por riesgos documentales. Como ejemplos expone nuevamente el riesgo de que la documentación que se publique en el portal de transparencia sea auténtica, sea la versión final, que esté firmada, etc. Comenta que cuando se trata de documentos administrativos es fácil comprobar que son auténticos, ya que están firmados. En cambio, cuando se trata de publicar información o datos, es más difícil garantizarlo. En relación a la transparencia pasiva, explica que es más sencillo puesto que se da en expedientes cerrados y trámites finalizados.

Otro riesgo para el entrevistado sería la falta de criterios sobre qué documentación es accesible y cuál no, a la hora de dar respuesta al ciudadano en una solicitud de acceso a información pública.

Considera que la administración electrónica evitará mala praxis a la hora de gestionar los documentos en la administración y comportará una mejora ya que será más restrictiva, estará reglada mediante protocolos claros y no se podrán incluir en los expedientes documentos que no formen parte del expediente o borradores, documentos de trabajo, etc. Considera que para la gestión de documentos en papel se debería haber contado con protocolos de gestión desde el principio, tal y como ahora las administraciones se están preocupando de desarrollarlos para la gestión electrónica. Esto lo relaciona con el cambio de visión sobre la gestión documental vista ahora como una prioridad, y no solo como un proceso finalista.

4. ¿Sabes si en la organización existe alguna metodología para prevenir o tratar los riesgos? ¿Se te ha explicado alguna vez dicha metodología?

El entrevistado explica que seguramente debe existir un protocolo de prevención de riesgos laborales pero afirma desconocerlo. Cree que es una obligación legal disponer de este protocolo pero lo desconoce completamente. A nivel de gestión documental explica que no existen protocolos de asesoramiento o acompañamiento a los trabajadores, incluso de formación.

5. En caso de que la respuesta anterior sea afirmativa, ¿te parece adecuada también para el control de los documentos que generas y gestionas en tu día a día?

No aplica.

6. ¿En tu departamento lleváis a cabo algún control sobre los posibles riesgos documentales? ¿Consideras que sería necesario?

A nivel de prevención, intentan concienciar a los trabajadores en el mantenimiento de los protocolos a lo largo de todo el ciclo de vida de los documentos, explicando conceptos básicos para que los vayan incorporando en su día a día y sean conscientes de su importancia. Esto se realiza dentro de las sesiones formativas que se programan, no tienen un protocolo establecido de prevención o control de riesgos pero sí llevan a cabo estas pequeñas acciones de prevención desde la concienciación.

Sí, considera necesario integrar la prevención de riesgos dentro de los protocolos propios de cada ámbito en la organización. Por ejemplo, en relación con el portal de transparencia, su idea es desarrollar un protocolo de gestión de dicho portal que ahora no existe. El entrevistado explica que la gestión de riesgos estaría incluida en este protocolo, donde se contemplarían aspectos tecnológicos, de responsabilidades, entre otros, y también de gestión documental. Aquí es donde entraría la prevención: pone ejemplos sobre qué elementos tener en cuenta antes de subir un documento al portal, qué documentos se pueden subir, en qué condiciones, en qué formatos, cómo se ejecuta, etc. Es decir, que no contemplan un protocolo específico de gestión de riesgos documentales.

Sobre la transparencia pasiva, la gestión de riesgos la entiende dentro de la política de gestión documental de la organización. Esto es así porque en este caso lo que se materializa es el acceso a expedientes administrativos y, por tanto, se relaciona directamente con esta política. Quien es responsable de mantener las características de los expedientes administrativos en su fase inactiva es el departamento de gestión documental y, por tanto, entiende que debe incorporarse en sus protocolos y políticas. Remarca que no considera necesario disponer de un protocolo de gestión de riesgos documentales específico, sino que la prevención la entiende a través de los procedimientos, protocolos, políticas e instrumentos de gestión documental de la organización. Lo justifica explicando que de esta manera tendrá más peso que si se desarrolla un instrumento a parte. Cuanto más incorporado en los pilares de la organización, más efectivo.

El entrevistado afirma que entiende la gestión documental como un instrumento de prevención de riesgos en sí dentro de la organización.

7. ¿Consideras que existe un mayor riesgo al trabajar con documentos electrónicos? ¿Por qué sí/no?

Afirma que los riesgos en un entorno u otro son diferentes, pero no está seguro de si realmente existe mayor riesgo en un entorno o en otro. Según la experiencia del entrevistado, los documentos en papel se pierden más a menudo de lo que parece y es por este motivo que considera que hay riesgos importantes también en este entorno. Comenta el caso de los envíos por correo interno y de la falta de conciencia y formación de las personas que tienen la responsabilidad del traslado. Muchas veces, estas personas no son conscientes de la importancia de la información que están trasladando, existe falta de sensibilidad. Para el entrevistado esta situación es un riesgo muy importante.

En entorno electrónico existen otros riesgos. Comenta el tema de la seguridad y explica que desconoce cómo se gestiona esta cuestión en su organización.