Escola Superior d'Arxivística i Gestió de Documents
Adscrita a la UAB

PROPUESTA METODOLÓGICA PARA LA IDENTIFICACIÓN DE RIESGOS ASOCIADOS A LA GESTIÓN DOCUMENTAL

Claudia Cecilia Castillo Segura

Director del trabajo: Anahí Casadesús

Año: 2016

Máster en Gestión Documental, Transparencia y Acceso a la Información

Escuela Superior de Archivística y Gestión de Documentos

Colección: Trabajos fin de máster y de posgrado

Como citar este trabajo: Castillo Segura, Claudia Cecilia. (2016) *Propuesta metodológica para la identificación de riesgos asociados a la gestión documental*. Trabajo de Investigación del Máster en Gestión Documental, Transparencia y Acceso a la Información de la Escuela Superior de Archivística y Gestión de Documentos de la Universidad Autónoma de Barcelona. (Trabajos fin de máster y de posgrado). Http://... (consultado el ...)

Título: Propuesta Metodológica para la Identificación de Riesgos Asociados a la Gestión Documental

Resumen

La Propuesta Metodológica para la Identificación de Riesgos Asociados a la Gestión Documental, tiene como fin brindar una orientación a las entidades públicas en Colombia para la identificación de los riesgos que pueden afectar a los documentos o archivos electrónicos, con la consecuencia de perder sus atributos de autenticidad, fiabilidad, integridad, usabilidad y accesibilidad, y amenazar su preservación a largo plazo, disminuyendo la capacidad de una organización para el logro de sus objetivos.

En este trabajo se articulan metodologías y modelos relacionados con la gestión del riesgo, teniendo como marco general de referencia el proceso de apreciación del riesgo establecido en la norma técnica UNE-ISO/TR 18128: 2014 IN *Información y documentación. Apreciación del riesgo en procesos y sistemas de gestión documental,* a partir del cual se desarrolla específicamente el subproceso de identificación del riesgo.

Palabras clave: riesgo**,** gestión del riesgo, gestión documental, procesos de gestión documental, sistemas de gestión documental, conservación, riesgos de los documentos, identificación del riesgo, preservación digital.

Títol: Proposta Metodològica per a la Identificació de Riscos Associats a la Gestió Documental

Resum

La Proposta Metodològica per a la Identificació de Riscos Associats a la Gestió Documental, té com a fi brindar una orientació a les entitats públiques a Colòmbia per a la identificació dels riscos que poden afectar els documents o arxius electrònics, amb la conseqüència de perdre els seus atributs d' autenticitat, fiabilitat, integritat, usabilitat i accessibilitat, i amenaçar la seva preservació a llarg termini, disminuint la capacitat d'una organització per a l'assoliment dels seus objectius. En aquest treball s'articulen metodologies i models relacionats amb la gestió del risc, tenint com a marc general de referència el procés d'apreciació del risc que estableix la norma tècnica UNE-ISO / TR 18128: 2014 IN Informació i documentació. Apreciació del risc en processos i sistemes de gestió documental, a partir del qual es desenvolupa específicament el subprocés d'identificació del risc.

Paraules clau: risc, gestió del risc, gestió documental, processos de gestió documental, sistemes de gestió documental, conservació, riscos dels documents, identificació del risc, preservació digital.

Abstract

The Proposed Methodology for Identifying Risks Associated with Document Management aims to provide guidance to public entities in Colombia for identifying risks that may affect any documents or electronic archives, with the consequence of losing their attributes authenticity, reliability, integrity, usability and accessibility, and threaten its long-term preservation, diminishing the ability of an organization to achieve its objectives.

In this work methodologies and models related to risk management are articulated, having as a general framework the risk assessment process established in technical standard UNE- ISO / TR 18128: 2014 IN K *Risk evaluation process and document management systems,* from which the thread identification process is developed specifically risk.

Keywords: risk, risk management, document management, document management processes, document management systems, document storage, document risks, risk identification, digital preservation.

SUMARIO

INDICE DE FIGURAS

INDICE DE TABLAS

1. INTRODUCCIÓN

En el ámbito de la administración pública en Colombia, la gestión del riesgo adquiere cada vez mayor importancia debido a los constantes cambios que se presentan tanto en el contexto interno como externo de las organizaciones, lo cual crea incertidumbres respecto del cumplimiento de sus objetivos.

Cambios en el contexto externo como nuevas políticas públicas, legislación, introducción de nuevas tecnologías, nuevos modelos de negocio y cambios en el contexto interno como por ejemplo reestructuraciones de las entidades, ajustes presupuestales, competencias del personal, entre otros, crean incertidumbres e implican un esfuerzo importante por parte de las organizaciones para adaptarse rápidamente a nuevas situaciones y cumplir con el desarrollo de políticas y aplicación de modelos de gestión desarrollados por la administración pública.

En este contexto, la gestión documental se ha desarrollado en Colombia siguiendo lineamientos y directrices establecidos en la normativa legal principalmente y de manera paulatina a través de estándares internacionales para la gestión de documentos, que se han venido adoptando con la intención de normalizar tanto los procesos de la gestión documental, como los sistemas de gestión documental, lo cual sería muy difícil sin una adecuada gestión del riesgo que permita anticiparse a aquello que podría afectar los documentos y en consecuencia el logro de los objetivos de una organización.

De manera general, la gestión del riesgo en Colombia tiene un enfoque organizacional basado en los procesos establecidos en la norma ISO 31000:2009 *gestión del riesgo – principios y directrices* y en legislación colombiana referente al Modelo de Gestión y Planeación en la Administración Pública, pero no un enfoque de la gestión de los riesgos relacionados específicamente con la gestión documental, procesos y sistemas de gestión documental; y aunque recientemente se ha homologado por el ICONTEC la norma ISO/TR 18128:2014 *apreciación del riesgo en procesos y sistemas de gestión documental*, es evidente la escasez de referencias o instrumentos metodológicos para su aplicación.

Frente a esta problemática, el objetivo de la *Propuesta Metodológica para la Identificación de Riesgos Asociados a la Gestión Documental* es brindar una orientación para reconocer los riesgos que pueden afectar positiva o negativamente la capacidad de los documentos para satisfacer las necesidades de una organización y está dirigida principalmente a los

responsables de la gestión documental y áreas de tecnologías de la información de las entidades de la administración pública en Colombia.

Las etapas de realización de este trabajo incluyen la recopilación de información para la elaboración del marco teórico de referencia sobre gestión del riesgo aplicable a los procesos y sistemas de gestión documental; el análisis de la gestión del riesgo en el contexto colombiano basado en referentes legales, modelos y metodologías relacionados con la gestión del riesgo, y el estudio de aspectos metodológicos relacionados con la identificación del riesgo.

El resultado de esta investigación es una propuesta metodológica para la identificación de riesgos asociados a la gestión documental, que contiene una estructura flexible, alineada con la norma UNE–ISO/TR 18128:2014 *Información y documentación. Apreciación del riesgo en procesos y sistemas de gestión documental* y con la metodología de administración del riesgo establecida para las entidades públicas en Colombia por el Departamento Administrativo de la Función Pública - DAFP, y es una propuesta metodológica que puede actualizarse fácilmente de acuerdo con los cambios que se presenten en el contexto de una organización o cuando esté generando o actualizando sus procesos y procedimientos.

2. MARCO TEÓRICO Y ESTADO DE LA CUESTIÓN

Sobre la gestión del riesgo en procesos y sistemas de gestión documental, son pocas las referencias teóricas que existen en la actualidad; en cambio, existen varias normas técnicas que abordan la gestión del riesgo como uno de los elementos fundamentales para normalización y estandarización de los procesos relacionados con la gestión documental. En la figura a continuación se presentan los referentes teóricos y técnicos que han sido considerados para el desarrollo de esta investigación, seguido de una breve descripción de cada uno:

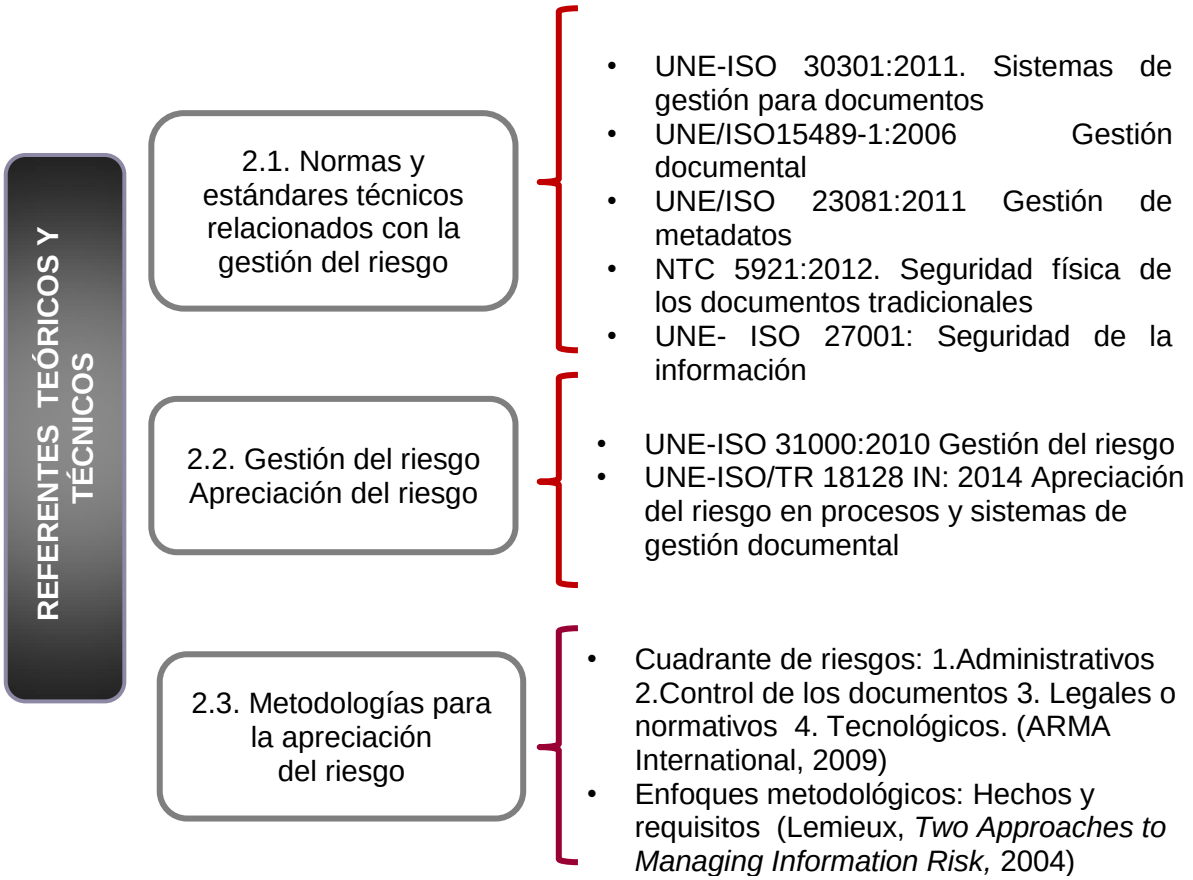

Figura 1. Referentes teóricos y técnicos
(Fuente: Elaboración propia, 2016**)**

2.1. Normas y estándares técnicos relacionados con la gestión del riesgo y con sistemas y procesos de gestión documental

La normalización[1] en archivística y gestión de documentos ha experimentado un incremento notable en los últimos años, que se da paralelo al crecimiento del campo de la información y al alto impacto de las tecnologías de la información en la producción y gestión de documentos.

Los objetivos principales de la normalización, son reducir los modelos existentes en la materia para adoptar únicamente los más necesarios y de esta manera lograr la simplificación de procesos; permitir el intercambio a nivel internacional y con ello unificar requisitos, conceptos o procesos; evitar errores de identificación creando un lenguaje claro y preciso que conlleve a una especificación u objetividad para el manejo de un vocabulario científico (Lobato Domínguez, 2009, pág. 4). Según Lobato Domínguez, las principales características de las normas técnicas y científicas son:

- **Carácter Unificador:** dado que su elaboración es producto del consenso de un grupo de profesionales, se consiguen normas que facilitan la compatibilidad e intercambiabilidad, entre sistemas y productos.
- **Seguridad Fiabilidad**: parte de principios y métodos universales, de patrones o modelos probados y para ello debe integrar diversas experiencias, para crear normas comunes y estables, y generar un clima de fiabilidad.
- **Necesidad:** sirve para intereses colectivos generales y demandas de la sociedad, está orientada a los usuarios.
- **Carácter finalista:** las normas están orientadas a resolver problemas, establecer metodologías y en general facilitar la vida (calidad) y economizar gastos.
- **Accesibilidad:** la norma debe difundirse y conocerse para poder ser aplicada.
- **Comprensibilidad (sencillez):** El aspecto lingüístico es un factor esencial en la normalización internacional. Deben incluir términos precisos con relaciones unívocas entre los idiomas más extendidos.
- **Tolerancia:** La norma no debe ser inmutable y fosilizar el ámbito de aplicación. Debe estar abierta a revisiones y cambios, pero también gozar de cierta estabilidad.

[1] La Organización Internacional de Normalización ISO define la Normalización como “la actividad que tiene por objeto establecer, ante problemas reales o potenciales, disposiciones destinadas a usos comunes y repetidos, con el fin de obtener un nivel de ordenamiento óptimo en un contexto dado, que puede ser tecnológico, político o económico.”

En Colombia el proceso de normalización en el campo de la gestión documental y archivística es relativamente reciente y de manera general tiene como referencia las normas técnicas emitidas por organismos internacionales como la Organización Internacional de Normalización - ISO. A través del Instituto Colombiano de Normas Técnicas y Certificación - ICONTEC[2], se realiza el proceso de generación y adopción de normas y estándares, que son de aplicación voluntaria y se expiden para que las organizaciones interesadas puedan establecer requisitos y buenas prácticas que apoyen la gestión documental.

Si bien la aplicación de normas y estándares técnicos no tienen carácter obligatorio, es muy importante reconocer las características de la normalización y cómo sirve de apoyo al cumplimiento de la legislación nacional referente a la archivística y gestión de documentos, que sí es de obligatorio cumplimiento por parte de las entidades de ámbito de aplicación de las normas legales colombianas.

Metodológicamente, se han tomado como referencia las normas técnicas UNE emanadas del organismo certificador en España Asociación Española de Normalización y Certificación - AENOR para el desarrollo de este trabajo, sin detrimento de la aplicación de las normas técnicas colombianas equivalentes que han sido homologadas en el contexto Colombiano. Por ello, se presenta a continuación una tabla de equivalencia entre las normas UNE/ISO y las NTC/ISO, que se describen más adelante:

UNE	NTC
UNE-ISO 30301:2011 *Información y documentación. Sistemas de gestión de documentos. Requisitos*	**NTC-ISO 30301:** *Información y documentación. Sistemas de gestión de registros. Requisitos.*
UNE/ISO15489-1:2006 *Información y documentación. Gestión de documentos Parte 1: Generalidades*	**NTC/ISO15489:2010** *información y documentación. Gestión de documentos. Parte 1. Generalidades*
UNE/ISO 23081:2011 *Información y documentación. Procesos de gestión de documentos. Metadatos para la gestión de documentos. Parte 2: Elementos de implementación y conceptuales.*	**NTC-ISO 23081-2:2011** *Información y documentación. Procesos de gestión de documentos. Metadatos para la gestión de documentos. Parte 2: Elementos de implementación y conceptuales.*

[2] Instituto Colombiano de Normas Técnicas y Certificación - ICONTEC. Es el Organismo Nacional de Normalización de Colombia.

UNE	NTC
UNE-ISO/IEC 27001:2014 *Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información (SGSI). Requisitos*	**NTC-ISO-IEC 27001:2006** *tecnología de la información. Técnicas de seguridad*. *Sistemas de Gestión de la Seguridad de la Información -SGSI-*
UNE-ISO/IEC 27002:2009 *Tecnología de la Información Técnicas de seguridad. Código de buenas prácticas para la gestión de la seguridad de la información.*	**NTC-ISO-IEC 27002:2007** *Tecnología de la información. Técnicas de seguridad. código de práctica para la gestión de la seguridad de la información*
UNE-ISO 31000:2010 *Gestión del riesgo. Principios y directrices*, es una norma que brinda los principios y directrices.	**NTC 31000:2011** *Gestión del riesgo. Principios y directrices.*
UNE-ISO/TR 18128 IN: 2014 *información y documentación. Apreciación del riesgo en procesos y sistemas de gestión documental*.	**NTC-ISO/TR 18128: 2016** *información y documentación. Evaluación del riesgo en procesos y sistemas de registros*.
ISO-11799:2003 *Información y documentación. Requisitos de almacenamiento de documentos para los materiales de archivos y bibliotecas.*	**NTC-5921:2012** *Información y documentación. Requisitos para el almacenamiento de material documental.*

Tabla 1. Equivalencia entre las normas UNE-ISO / NTC-ISO
(Fuente: Elaboración propia, 2016)

2.1.1 UNE-ISO 30301:2011. Sistemas de gestión para documentos

La UNE-ISO 30301:2011 *Información y documentación. Sistemas de gestión de registros. Requisitos*, tiene un enfoque estratégico y se encuentra dentro de la familia de las normas de sistemas para la gestión de documentos. Los requisitos de esta norma, relacionados con las acciones para el tratamiento de riesgos y oportunidades, se describen en el apartado 6.1. del capítulo 6, que se centra en la planificación alrededor de los riesgos estratégicos, asociados al aseguramiento de que el Sistema de Gestión Documental – SGD, alcance los resultados

previstos; de esta manera, el éxito en la implementación de un SDG requiere de la identificación, análisis y evaluación de los riesgos, que como subprocesos de la gestión del riesgo, se basan en la comprensión de la organización y su contexto teniendo en cuenta factores externos e internos de la organización (4.1.), así como los requisitos de negocio, legales y reglamentarios que debe cumplir. Así es como se definen los objetivos de la gestión documental y se identifican las acciones necesarias para alcanzar dichos objetivos (6.2); operativamente, estas acciones deberían incorporarse a los procesos del SGD (Capítulo 8).

2.1.2. UNE/ISO15489-1:2006. Gestión documental

La UNE/ISO15489-1:2006, *Información y documentación. Gestión de documentos Parte 1: Generalidades,* es una norma orientada hacia los procesos, en donde la gestión documental es un proceso transversal a toda la organización e integra la gestión de los documentos con los sistemas y procesos de trabajo, de tal manera que los documentos que han sido creados o recibidos por una organización en desarrollo de sus funciones, adquieren un valor probatorio o evidencial, atribuible por el cumplimiento de cuatro cualidades o requisitos desde el momento de su creación; estos requisitos están definidos en la norma y se resumen a continuación:

- **Autenticidad.** Documento auténtico es aquél del que se puede probar: que es lo que afirma ser; que ha sido creado o enviado por la persona de la cual se afirma que lo ha creado o enviado; y que ha sido creado o enviado en el momento que se afirma.
- **Fiabilidad.** Documento fiable es aquél cuyo contenido puede ser considerado una representación completa y precisa de las operaciones, las actividades o los hechos de los que da testimonio.
- **Integridad.** Documento íntegro es el que hace referencia a su carácter completo e inalterado. Es decir, un documento que no ha sufrido modificaciones no autorizadas.
- **Disponibilidad.** Documento disponible es aquel que puede ser localizado, recuperado, presentado e interpretado.

De manera general, la aplicación de la norma contribuye a reducir los riesgos a los que puede estar expuesta la organización, a través de la definición de procesos y controles para la gestión de documentos.

2.1.3. UNE/ISO 23081:2011. Gestión de metadatos

UNE/ISO 23081:2011 *Información y documentación. Procesos de gestión de documentos. Metadatos para la gestión de documentos. Parte 2: Elementos de implementación y conceptuales,* es otra de las normas de referencia relacionada con la gestión del riesgo.

Establece que a través de la adaptación de los esquemas de metadatos, una organización puede cumplir los requisitos que sean necesarios para evitar los riesgos, partiendo de la especificación de los elementos que deben incluirse para que los documentos conserven sus características de autenticidad, fiabilidad e integridad.

Entonces, al hacer el análisis de las estrategias para la implementación de un esquema de metadatos, la organización debe identificar los riesgos que existen y el grado de riesgo que estos implican, para asegurarse que la estrategia de implementación proporcionará acceso a los sistemas de gestión esenciales a lo largo del tiempo, cumplirá los requisitos legales de autenticidad y fiabilidad y podrá mantenerse a través del tiempo.

2.1.4. UNE- ISO 27000. Seguridad de la información

A nivel de normalización la seguridad de la información es una de las disciplinas que cuenta con sus propias normas y una relación directa con los sistemas de gestión de la organización; así, las normas ISO de la familia 27000, constituyen el modelo de referencia de las organizaciones para la implementación de un sistema de seguridad de la información.

En este modelo se asume que la información es un activo**,** que al igual que otros activos comerciales, es esencial para el negocio[3] de una organización y por lo tanto merece ser protegida de forma adecuada.

La información puede estar almacenada de forma digital, como por ejemplo archivos de datos almacenados en medios magnéticos u ópticos o de forma física o analógica como por ejemplo en papel, así como la información que está relacionada con el conocimiento de los empleados, y ser transmitida a través de diferentes medios. En cualquier caso siempre se necesitará de una protección adecuada.

[3] Dentro de la norma se entiende “negocio” como aquellas actividades que son esenciales para la existencia de la organización. une-ISO/IEC 27001

Las normas de seguridad de la información, giran en torno a tres dimensiones principales definidas a partir de tres propiedades de los activos de información**:**

- **Confidencialidad**: propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
- **Disponibilidad:** propiedad que la información sea accesible y utilizable por solicitud de una entidad autorizada.
- **Integridad:** propiedad de salvaguardar la exactitud y estado completo de los activos.

La seguridad de la información consiste en la aplicación y gestión de las medidas de seguridad apropiadas, que implica la identificación y análisis de un conjunto amplio de amenazas y la aplicación de controles seleccionados a través del proceso de gestión del riesgo. Para esto impone como requisito general de la organización, establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un Sistema de Gestión de la Seguridad de la información – SGSI documentado, en el contexto de las actividades globales de negocio de la organización y de los riesgos que enfrenta.

El proceso usado en la norma para el establecimiento del SGSI se basa en el modelo de proceso PHVA[4] o ciclo Deming, que consiste en una secuencia lógica de cuatro pasos: planear, hacer, verificar y actuar, en donde la evaluación de los riesgos forma parte del ejercicio cíclico. Dicha evaluación de los riesgos asociados a los activos de información de una organización, contempla tres variables: las amenazas a los activos de información; los factores de vulnerabilidad ante la probabilidad de que la amenaza se materialice y afecte los activos de información; y el impacto potencial de cualquier incidente de seguridad de la información sobre los activos de información.

2.1.5. NTC 5921:2012. Seguridad física de los documentos tradicionales

Una de las mejores prácticas para la seguridad y mantenimiento de los documentos físicos se establece en la norma NTC-5921:2012 que es una adopción modificada de la norma ISO 11799:2003 *Información y documentación. Requisitos de almacenamiento de documentos para*

[4] Planear o Planificar: consiste en definir los objetivos y los medios para conseguirlos; Hacer: Se refiere al acto de implementar la visión preestablecida; Verificar: Implica comprobar que se alcanzan los objetivos previstos con los recursos previamente asignados; Actuar: Se refiere a analizar y corregir las posibles desviaciones detectadas, así como también se debe proponer mejoras a los procesos ya empleados.

los materiales de archivos y bibliotecas. La norma establece los requisitos para las áreas de almacenamiento y mobiliario y describe los componentes de la planificación de desastres.

En esta norma las amenazas que ponen en riesgo los documentos, provienen del ambiente externo y están relacionadas con las condiciones de almacenamiento y la utilización y manipulación durante el procesamiento de los documentos.

Aunque la norma está enfocada hacia la seguridad física de los documentos en soporte papel, incluye algunas recomendaciones para el almacenamiento a largo plazo de documentos en otros soportes como medios magnéticos y medios ópticos.

Las acciones de gestión del riesgo recomendadas giran en torno a la formulación de políticas que incluyen el control del entorno de almacenamiento, control de acceso físico, la planificación de desastres, el cuidado y manejo de los documentos, así como la utilización de materiales que aseguren la permanencia de los documentos a través del tiempo.

Esta norma está relacionada con la normativa legal, específicamente con los Acuerdos 049 y 050 de 2000, expedidos por el Archivo general de la Nación de Colombia, en los cuales se establecen los requisitos que deben cumplir los edificios y locales destinados a archivos y la prevención de deterioro de los documentos de archivo y situaciones de riesgo, respectivamente.

2.2. Normas y estándares sobre gestión del riesgo

En materia de normalización, la línea base para la gestión del riesgo se establece en la UNE-ISO 31000:2010 *Gestión del riesgo. Principios y directrices* y el enfoque sobre la gestión del riesgo en procesos y sistemas de gestión documental se especifica en la UNE-ISO/TR 18128 IN: 2014 *Información y documentación. Apreciación del riesgo en procesos y sistemas de gestión documental*.

La línea metodológica que se plantea en estas normas debe ser aplicada en una organización de manera conjunta y articulada con otras normas técnicas relacionadas con la gestión de documentos, tanto para la definición de las actividades o procesos, como de los controles que pueden aplicarse para minimizar los riesgos en esta materia y de esta manera apoyar el cumplimiento de la normativa legal existente en el ámbito colombiano. A continuación se profundiza en los aspectos más relevantes de cada una de estas normas.

2.2.1. UNE-ISO 31000:2010. Gestión del riesgo.

La norma UNE-ISO 31000:2010 *Gestión del riesgo. principio y directrices*, es una norma que brinda los principios y directrices genéricas para la gestión de riesgo; su espectro es bastante amplio y tiene como alcance cualquier organización, bien sea una empresa pública, privada o comunitaria, asociación grupo o individuo y el rango de actividades incluye estrategias y decisiones, operaciones, procesos, funciones proyectos, productos, servicios y activos, y aplica a cualquier tipo de riesgo, de cualquier naturaleza bien sea que tenga consecuencias positivas o negativas.

En esta norma el riesgo se define como el "efecto de incertidumbre sobre los objetivos"; el efecto puede ser una desviación positiva o negativa respecto de lo esperado y la incertidumbre el estado de deficiencia de información relativa a la comprensión o conocimiento de un suceso o evento, de sus consecuencias o de su probabilidad. Los objetivos pueden hacer referencia a diferentes aspectos organizacionales tales como financieros, salud, seguridad, medio ambientales, entre otros y establece que el riesgo se caracteriza por la referencia a sucesos o eventos potenciales y a sus consecuencias o a una combinación de ambos y se expresa como una combinación de las consecuencias de un suceso o evento y de su probabilidad (UNE-ISO 31000, 2010).

- **Marco de referencia UNE-ISO 31000: 2010**

Según esta norma, la gestión del riesgo son aquellas actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Uno de los elementos clave para la gestión del riesgo es el marco de referencia, que ha de brindar las bases y disposiciones que se tendrán en cuenta en todos los niveles de la organización y trae como beneficios que ayuda a la gestión eficaz del riesgo a través de la aplicación de este proceso en todos los niveles y contextos específicos de la organización, garantizando de este modo, que la información derivada se reporte de manera adecuada y se utilice como base para la toma de decisiones y la rendición de cuentas en todos los niveles de la organización. De acuerdo con la (UNE-ISO 31000, 2010) los cuatro componentes del marco de referencia para la gestión del riesgo son:

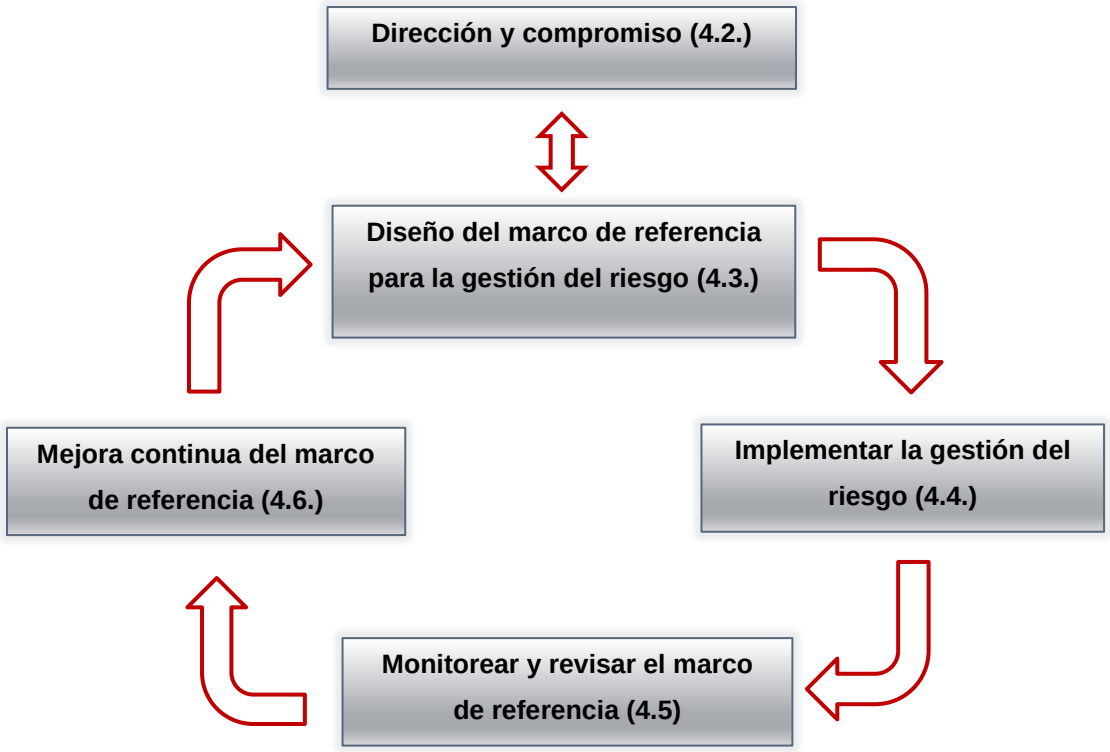

Figura 2. Componentes del marco de referencia para la gestión del riesgo (Fuente: UNE- ISO 31000, 2010)

La introducción del riesgo en una entidad requiere del compromiso fuerte y sostenido de la alta dirección de la organización (4.2), así como la planificación estratégica y rigurosa para lograr el compromiso a todo nivel. Dentro de las actividades propias de la dirección se encuentra la definición de la política para la gestión del riesgo, la cual debería estar alineada con la cultura organizacional y los objetivos de la gestión del riesgo deben alinearse con los objetivos y las estrategias de la organización. Otros aspectos como indicadores de desempeño de la gestión del riesgo, conformidad legal y reglamentaria, asignación de obligaciones, responsabilidades y recursos, deben tenerse en cuenta, así como la comunicación de los beneficios de la gestión del riesgo y la adopción de mecanismos que permitan garantizar que el marco de referencia sigue siendo el adecuado para la organización.

Entender a la organización y su contexto implica la evaluación de su contexto interno y externo, dada la influencia de estos aspectos en la construcción del marco de referencia (4.3). Según la norma, la evaluación del contexto externo incluye, entre otros, aspectos como: Ambiente social,

cultural y político, legal, reglamentario, financiero, tecnológico, económico, natural y competitivo, que pueden ser del ámbito, internacional, nacional, regional o local; impulsores clave que pueden tener impacto en los objetivos en la organización; relaciones con las partes involucradas externas y sus percepciones y valores.

En cuanto al contexto interno algunos elementos que pueden incluirse están relacionados con gobierno, estructura organizacional, funciones y obligaciones; políticas, objetivos y estrategias, capacidades entendidas como recursos y conocimiento, sistemas de información, flujos de información y procesos de toma de decisiones, cultura organizacional, normas y directrices adoptados por la organización, relaciones contractuales, entre otros.

La implementación de la gestión del riesgo requiere de una política (4.4) que debería establecer los objetivos y compromiso de la organización para la gestión del riesgo y para garantizar la eficacia del desarrollo de este proceso; así mismo, la organización debería medir su desempeño y revisar periódicamente tanto el marco de referencia como la política y el plan para la gestión del riesgo (4.5); de este modo, con los resultados obtenidos, tomar las decisiones pertinentes para la mejora continua del este proceso (4.6).

De manera general, la norma sugiere que se deben abordar los siguientes aspectos:

1. Justificación para la gestión del riesgo.
2. Alineación entre los objetivos, políticas organizacionales y la política de gestión del riesgo.
3. Obligaciones y responsabilidades para gestionar el riesgo
4. La manera de tratar los conflictos e intereses
5. Compromiso para poner a disposición los recursos necesarios con el fin de ayudar a los responsables de la gestión del riesgo y de rendir cuentas con respecto a ésta
6. La forma de medir y reportar el desempeño de la gestión del riesgo.
7. Compromiso para revisar y mejorar periódicamente la política, el marco de la gestión del riego, en respuesta a un evento o cambio en las circunstancias.
8. Comunicar de manera adecuada la política.

Así mismo, la entidad debería garantizar que existe responsabilidad, autoridad y competencia adecuada para gestionar el riesgo incluyendo la implementación y mantenimiento del proceso,

garantizando la idoneidad, eficacia y eficiencia de todos los controles y con ello la rendición de cuentas.

Deberían identificarse los propietarios del riesgo, quien debe dar cuentas por el desarrollo y mantenimiento del marco para la gestión del riesgo, identificación de otras responsabilidades en el proceso para la gestión del riesgo; estableciendo la medición del desempeño y procesos de escalamiento y reporte externo e interno. Adicionalmente, garantizando niveles adecuados de reconocimiento.

La gestión del riesgo debe estar incluida en todas las prácticas y los procesos de la organización. Debería existir un plan para la gestión del riesgo, que garantice que se implementa la política de la gestión del riesgo en toda la organización.

- **Procesos para la Gestión del Riesgo**

La UNE-ISO 31000:2010 describe lo que se conoce como la *gestión del riesgo empresarial* que significa que la gestión del riesgo se asumen como una parte integral de todos los procesos de la organización, es un parte esencial de la toma de decisiones y aporta valor a la organización.

Siguiendo la norma UNE-ISO 31000:2010 *Gestión del riesgo. Principios y directrices,* a continuación se describe el conjunto de actividades que conforman el proceso para la gestión de riesgos:

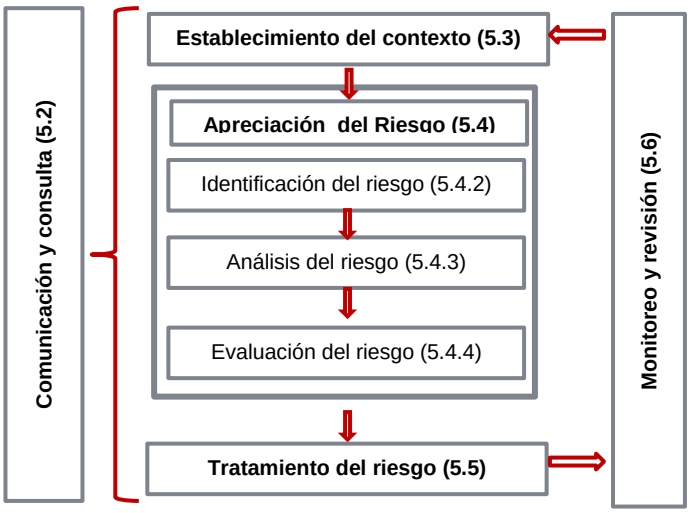

Figura 3. Esquema del proceso para la gestión del riesgo
(Fuente: UNE-ISO 31000, 2010)

- **Comunicación y consulta (5.2)**

Son aquellos procesos continuos y reiterativos que una organización lleva acabo para suministrar, compartir u obtener información de las partes involucradas con la gestión del riesgo, es decir con una persona u organización que puede afectar o verse afectada por una decisión o actividad dentro de la organización.

- **Establecimiento del contexto (5.3)**

Contempla los parámetros internos y externos que se han de tomar en consideración para gestionar el riesgo y para establecer el alcance y los criterios del riesgo para la política de gestión del riesgo. Estos parámetros están relacionados con el contexto o ambiente externo y/o interno respectivamente, en el cual la organización busca alcanzar sus objetivos.

- **Apreciación del riesgo (5.4)**

Es el proceso total de identificación del riesgo, análisis del riesgo y evaluación del riesgo.

  - **Identificación del riesgo (5.4.2).** Es el proceso para encontrar reconocer y describir el riesgo. Implica la identificación de la fuentes de riesgo, que puede ser tangible o intangible; los eventos que pueden ser ocurrencias con varias causas, ser algo que no está sucediendo, hacer referencia a un incidente o accidente o un evento sin consecuencia; y sus causas y consecuencias potenciales que son el resultado de un evento que afecta los objetivos.
  - **Análisis del riesgo (5.4.3).** Es el proceso que permite comprender la naturaleza del riesgo y determinar su nivel, es decir su magnitud o de una combinación de riesgos que se expresa en términos de la combinación de las consecuencias y su probabilidad. El análisis es la base para la evaluación del riesgo y las decisiones sobre el tratamiento de los riesgos e incluye la estimación del riesgo.
  - **Evaluación del riesgo (5.4.4).** Es el proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables. Esta evaluación permite la toma de decisiones sobre el tratamiento del riesgo.

- **Tratamiento del riesgo (5.5.)**

Es el proceso para modificar el riesgo. Implica acciones como evitar el riesgo decidiendo no continuar con la actividad que lo originó; tomar e incrementar el riesgo con el fin de perseguir una oportunidad; retirar la fuente del riesgo; cambiar la probabilidad; cambiar las consecuencias; compartir el riesgo con una o varias de las partes involucradas y retener el riesgo a través de la decisión informada.

Puede hacer referencia a los tratamientos del riesgo relacionados con consecuencias negativas como mitigación del riesgo, eliminación del riesgo, prevención del riesgo, y reducción del riesgo. Así mismo, el tratamiento de los riesgos puede dar lugar a generación de riesgos nuevos o modificar los ya existentes.

- **Monitoreo y revisión (5.6.)**

El monitoreo es la verificación, supervisión, observancia critica o determinación continua del proceso con el fin de identificar cambios respecto del nivel de desempeño exigido o esperado. Este proceso puede aplicar al marco de referencia para la gestión del riesgo, al proceso para la gestión del riesgo o al control. La revisión es la acción que se emprende para determinar la idoneidad, conveniencia y eficacia de la materia en cuestión para lograr los objetivos establecidos.

El proceso descrito en la norma UNE-ISO 31000:2010 es cíclico y está diseñado para ser parte de las prácticas de gestión generales de una organización. De estas actividades algunas son comunes a cualquier disciplina, como el establecimiento del contexto, la comunicación y consulta, y el seguimiento y revisión de los cuales se debe establecer un procedimiento o metodología que puede compartirse con cualquier campo de trabajo (Casadesús, 2015).

2.2.2. UNE-ISO/TR 18128:2014. Apreciación del riesgo en procesos y sistemas de gestión documental.

El marco conceptual para el desarrollo la norma UNE-ISO/TR 18128:2014 *Información y documentación. Apreciación del riesgo en procesos y sistemas de gestión documental* se encuentra en la norma UNE/ ISO 31000:2010 y se centra específicamente en el proceso de apreciación del riesgo y sus tres subprocesos: identificación, análisis y evaluación del riesgo.

La norma plantea cómo se pueden desarrollar estas tareas en relación con los procesos y sistemas de gestión documental y tiene como finalidad brindar apoyo a los profesionales de la gestión documental, para la apreciación de los riesgos, estableciendo directrices y ejemplos relacionados con el proceso de la gestión del riesgo que se presenta en la UNE- ISO 31000:2010 *Gestión del riesgo. Principios y directrices,* aplicados a los riesgos relacionados con los procesos y sistemas de gestión documental.

De manera general, la norma establece que los resultados del análisis del riesgo relacionados con los procesos y sistemas de gestión de documentos, deben incorporarse al marco general de la gestión del riesgo de una organización, de tal forma que pueda tener un mejor control de sus documentos, su calidad y uso según el propósito de una entidad u organización.

El objeto y campo de aplicación de esta norma, consiste en establecer un método de análisis para identificar los riesgos relacionados con los procesos y sistemas de gestión documental, proporcionar un método de análisis de los potenciales efectos de eventos adversos sobre los procesos y sistemas de gestión documental, proporcionar directrices para conducir la apreciación de los riesgos relacionados con los procesos y sistemas de gestión documental y proporcionar directrices para documentar los riesgos apreciados como desarrollo para la mitigación de los mismos.

Dentro del contexto de los procesos y sistemas de gestión documental, el subproceso de identificación del riesgo tiene como objetivo detectar, reconocer y registrar los posibles eventos y situaciones que pueden suceder y que afecten la capacidad de los documentos para la consecución de los objetivos propuestos por la organización y estructura esta actividad en tres categorías relacionadas con la creación y control de los documentos: contexto, sistemas y procesos.

Figura 4. Categorías del proceso de identificación del riesgo
(Fuente: elaboración propia, adaptado de UNE-ISO/TR 18128, 2014)

Así mismo, la norma explica que el análisis del riesgo, es un subproceso se realiza para determinar las consecuencias potenciales de los riesgos y la probabilidad de que ocurran, a partir de elementos de análisis como las áreas de incertidumbre, cuyo resultado de análisis permite establecer las consecuencias y los criterios de apreciación del riesgo que facilitan la definición del escalado de probabilidad del riesgo.

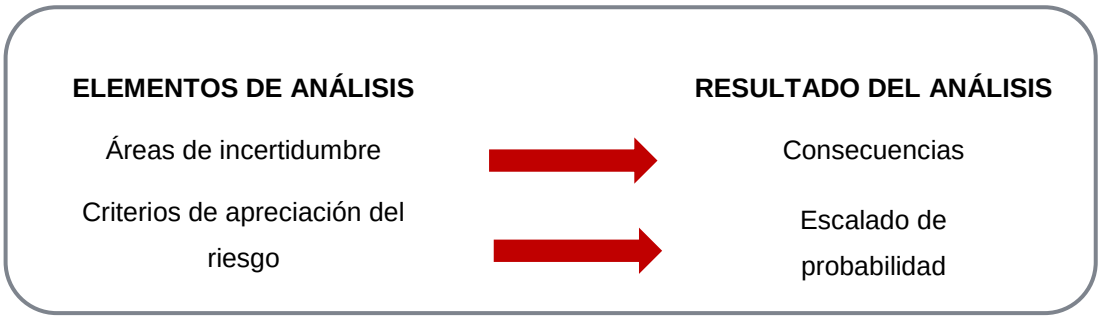

Figura 5. Elementos y resultados del subproceso de análisis del riesgo
(Fuente: elaboración propia, adaptado de UNE-ISO/TR 18128, 2014)

Por último, aborda la evaluación de los riesgos como un subproceso que implica comparar el nivel de riesgo detectado durante el subproceso de análisis, con los criterios de riesgo establecidos en ese contexto.

El análisis de los riesgos, es la base para considerar qué riesgos necesitan tratamiento y con qué prioridad. Así la evaluación de los riesgos ayuda en la toma de las decisiones que pueden ser:

- Si un riesgo necesita tratamiento
- Las prioridades para el tratamiento
- Si una actividad debería llevarse a cabo
- Cuál de las posibles opciones se debería adoptar

La apreciación del riesgo en procesos y sistema de gestión documental de la norma UNE-ISO/TR 18128: 2014, sigue el desarrollo de los procesos de gestión del riesgo establecidos en la norma UNE-ISO 31000:2010; específicamente es importante tener en cuenta el desarrollo del establecimiento del contexto, ya que en este apartado se incluye la definición de los criterios de riesgo, que serían aquellos criterios que aplican para evaluar la importancia del riesgo (Casadesús, 2015).

Dentro del subproceso de identificación del riesgo se establecen las capas de contexto de los documentos y procesos de gestión documental de una organización para la identificación de los factores tanto externos como internos. En su ítem (5.1) la norma ilustra las capas de contexto de los documentos y procesos de gestión documental así:

Figura 6. Capas de contexto de los documentos y los procesos de gestión documental (Fuente: UNE-ISO/TR 18128 IN, 2014)

En esta noma, la metodología para la identificación y el análisis de los riesgos relativos a los procesos y sistemas de gestión documental, se desarrolla teniendo en cuenta cuatro áreas de incertidumbre. Estas áreas, se constituyen en una guía para encontrar las causas de posibles riesgos en una organización. De manera general los aspectos relacionados con cada una de ellas son los siguientes:

- Contexto: factores externos (5.2.)

Los factores externos son áreas de incertidumbre que están por fuera del control de la organización, pero que afectan a los documentos y los sistemas donde se crean y gestionan.

- Contexto: factores internos (5.3.)

Los factores internos son áreas de incertidumbre que tienen un efecto inmediato en la gestión de los documentos. Están relacionados con los cambios del entorno económico, tecnológico y estructural de las organizaciones, para adaptarse a nuevas circunstancias.

- Sistemas de gestión documental (5.4.)

Los sistemas para crear y controlar documentos, cambian a lo largo del tiempo de acuerdo con el contexto externo e interno de la organización y por esto es necesario que la alta dirección esté informada y asuma la responsabilidad de respuesta de la organización ante posibles amenazas. La identificación de riesgos relacionados con los sistemas de gestión documental y otros sistemas de información, generalmente se realiza desde la perspectiva de la seguridad de la información. Sin embargo es necesario tener un enfoque más amplio para abordar diferentes problemáticas.

- Procesos documentales (5.5.)

En este caso la identificación de riesgos se centra en la creación de los documentos, en los procesos de control para gestionarlos y en los sistemas de gestión documental. Las referencias para el diseño de documentos y procesos documentales se encuentran en las normas ISO 15489, partes 1 y 2, e ISO 23081 partes 1, 2, y 3.

La metodología de la norma (UNE-ISO/TR 18128, 2014), se orienta hacia los requisitos que deben cumplir los documentos para identificar los riesgos que podrían afectarles y en este sentido, la identificación de riesgos relacionados con los procesos y sistemas de gestión

documental, es fundamental para detectar qué pasaría si los documentos dejan de ser auténticos y fiables y si estos no se mantienen íntegros, usables y accesibles por el tiempo que sea necesario, ya que esto puede afectar la capacidad de los documentos para satisfacer las necesidades de la organización (Casadesús, 2015).

2.3. Metodologías para la identificación de los riesgos asociados a la gestión de documentos

Además de la metodología propuesta en la norma (UNE-ISO/TR 18128, 2014), existen algunas metodologías para la identificación del riesgo en procesos de gestión documental, que pueden ser útiles y adaptarse a las diferentes necesidades y realidades de una organización. A continuación se relacionan dos de estas referencias metodológicas:

2.3.1. Guía de la organización internacional ARMA[5]

Evaluar y mitigar los riesgos de la información y los documentos (ARMA International, 2009), es un documento que proporciona un marco metodológico para la comprensión y evaluación del riesgo de una organización en relación con los archivos y la gestión de la organización. Esta metodología se basa en un cuadrante que sirve de herramienta para categorizar los riesgos y establecer un sistema de evaluación de riesgos en una organización. El cuadrante de riesgos (ARMA International, 2009), se estructura a partir de cuatro categorías de riesgos:

Figura 7. Cuadrante de riesgos ARMA
(Fuente: ARMA International, 2009)

[5] Association of records managers and administrators (ARMA) International. http://www.arma.org/

- **Riesgos administrativos**

  Se refiere a las amenazas de una organización que están relacionadas con el sistema de gestión documental. Esta categoría identifica las áreas de: Gobernanza de la información, Gestión del cambio y Gestión de emergencias.
- **Riesgos en el control de los documentos**

  Son los riegos relacionados con los procesos de gestión documental: clasificación, retención, disposición y almacenamiento, entre otros.
- **Riesgos legales o normativos**

  Esta categoría corresponde a los riesgos relacionados con el cumplimiento legal y reglamentario de la gestión documental, que enfrenta cualquier tipo organización, bien sea pública o privada.
- **Riesgos tecnológicos**

  Se refiere a los riesgos que existen en cualquier sistema de gestión documental en un entorno tecnológico y que están relacionados con la seguridad de la información, las comunicaciones electrónicas y control del software.

La guía de la organización internacional ARMA incluye una herramienta de evaluación del riesgo, que consiste en un cuestionario estructurado a partir de las cuatro categorías del cuadrante, el cual a su vez se divide en once áreas de incertidumbre. Al completar el cuestionario se calcula un valor numérico para cada cuadrante. Cuanto menor sea el valor resultante, menor será el riesgo potencial para la organización; y por el contrario los valores más altos indicaran un mayor riesgo potencial, lo que significa que la organización debe revisar su sistema de gestión documental con el fin de mitigar y reducir la exposición al riesgo. (ARMA International, 2009).

2.3.2. Enfoques metodológicos: Hechos y requisitos

Existen dos enfoques para el análisis de riesgos, propuestos por *Lemieux* (Lemieux, Two Approaches to Managing Information Risk, 2004): Uno es el enfoque tradicional basado en hechos, que consiste en la identificación y gestión de riesgos a partir de un hecho, acontecimiento o amenaza desencadenante.

El otro es el enfoque basado en requisitos, que consiste en la identificación de riesgos a partir del análisis de los requisitos aplicables, cuyo incumplimiento puede afectar los documentos. Estos requisitos se extraen del marco legal y normativo en el que la organización desarrolla sus

actividades, en donde el riesgo aparece cuando la organización falla en el cumplimiento de estos requisitos (Casadesús, 2015).

A continuación se relacionan algunas de las características sobre estos dos enfoques:

ENFOQUE	VENTAJAS	DESVENTAJAS	EJEMPLO
Hechos	Rápida identificación de estrategias de prevención o mitigación de los riesgos, ya que se centra en las amenazas y vulnerabilidades. Puede requerir menos tiempo y recursos Es más fácil la implementación de una estrategia para dar respuesta a una amenaza conocida.	No es útil para lograr un enfoque estratégico Se puede pasar por alto las Causas de los riesgos en los sistemas de gestión documental.	Una amenaza o condición latente derivada de la posible ocurrencia de un fenómeno físico de origen natural, socio-natural o antrópico no intencional, que puede causar daño: condiciones geográficas, climáticas, sociales, uso y estado de la edificación, entre otros.
Requisitos	Tiene un enfoque estratégico de la gestión del riesgo Facilita el análisis de los procesos de negocio para detectar fallos en los flujos de información. Analiza los requisitos de información y los documentos que la organización necesita para cumplir sus objetivos.	Implica mayores recursos y tiempo para su realización. En principio puede ser difícil su integración con la gestión del riesgo organizacional existente.	Requisitos establecidos las normas técnicas internacionales ISO o normas técnicas colombianas. Requisitos establecidos en el marco legal y normativo relacionado con la organización y la gestión documental.

Tabla 2. Enfoques metodológicos para la Identificación de riesgos
(Fuente: elaboración propia, adaptado de *Lemieux,* 2004)

2.4. Referentes para la identificación del riesgo en procesos y sistemas de gestión documental

Metodológicamente es necesario tener como referentes trabajos realizados por diferentes organizaciones, para apoyar el proceso de identificación de riesgos. A continuación se presentan alguno de ellos:

2.4.1. Catálogo de elementos MAGERIT

MAGERIT es una metodología de análisis y gestión de riesgos desarrollada por el Consejo Superior de la Administración Electrónica de España (Administración Electrónica (PAe), 2012), relacionada con el uso de las tecnologías de la información y los riesgos que pueden derivarse de ello. Está orientada hacia los riesgos que pueden presentarse en el uso y manejo de la información digital y sistemas de información con el fin de facilitar la implantación y aplicación del Esquema Nacional de Seguridad en España y tiene como base el marco de referencia para la gestión del riesgo, establecido en la norma ISO 31000 de gestión del riesgo.

Dentro de esta metodología se propone un catálogo que brinda pautas en cuanto a:

- Tipos de activos
- Dimensiones de valoración de los activos
- Criterios de valoración de los activos
- Amenazas típicas sobre los sistemas de información
- Salvaguardas a considerar para proteger los sistemas de información

En cada una de las secciones, además de las pautas establecidas, se incluye una notación en el formato estándar XML que se emplea para la publicación regular de estos elementos de tal manera que la información pueda ser procesada automáticamente por herramientas de análisis y gestión.

Uno de los elementos de esta metodología es el catálogo de amenazas posibles sobre los activos de un sistema de información, que contiene elementos estándar que facilitan la identificación del riesgo. En el Anexo 1, se reproduce el listado con las amenazas que se presentan en esta metodología, así como una breve descripción que sirve de referencia para la identificación de riesgos asociados a procesos y sistemas de gestión documental.

2.4.2. Riesgos y amenazas en *cloud computing*

El informe presentado por el Instituto Nacional de Tecnologías de la Comunicación – INTECO (Instituto Nacional de Tecnologías de la Comunicación, 2011), resume algunos documentos generados por la consultora Gartner[6], *Cloud Securiity Alliance (CAS)* [7] y National Institute of Standards and Technology (NIST)[8], que dan una visión general de amenazas, riesgos y recomendaciones, relacionados con la seguridad en *cloud.* Con el fin de tener un acercamiento a las amenazas y riesgos asociados a procesos y sistemas de gestión documental, relacionados con infraestructura y servicio *cloud*, se reproduce parcialmente la información contenida en este informe en los Anexos 2,3 y 4 de este documento.

2.4.3. Riesgos de preservación digital

El trabajo que presenta (Rosenthal, Robertson, Lipkis, Reich, & Morebito, 2005), sobre *los requisitos de preservación digital,* se basa en el modelo OAIS. Aquí se propone un espectro de amenazas que podrían afectar un sistema de preservación digital, a partir de una selección de aquellas que se consideran más importantes para establecer las estrategias. Lo que se plantea es la creación de una lista de requisitos que sirva para la para la certificación de sistemas en el mediano plazo. Este trabajo se estructura en estos tres elementos:

- Conjunto de amenazas que se consideren importantes.
- Estrategias seleccionadas para su implementación
- Forma en que se ponen en práctica dichas estrategias

En principio los diseñadores de un sistema de preservación digital requieren de una visión clara de las amenazas y riesgos contra los sistemas de preservación digital, que no son exclusivas de este tipo de sistemas. Rosenthal propone una taxonomía de amenazas que se reproduce en el Anexo 5 de este estudio.

---

[6] *Gartner S.A*. es una compañía de investigación y consultoría de tecnologías de la información; *Gartner* utiliza los cuadrantes Mágicos y los ciclos de sobre-expectación para presentar sus análisis.

[7] *Cloud Security Alliance (CSA)* es una organización sin fines de lucro que tiene como fin promover el uso de las mejores prácticas para ofrecer garantías de seguridad en *Cloud Computing.*

[8] *National Institute of Standards and Technology (NIST),* es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos. La misión de este instituto es promover la innovación y la competencia industrial en Estados Unidos mediante avances en metrología, normas y tecnología, paramejorar la estabilidad económica y la calidad de vida.

Desde la perspectiva de los aspectos teóricos, técnicos y referentes que se presentan en este capítulo, es necesario abordar la identificación del riesgo en procesos y sistemas de gestión documental, mediante la aplicación de una metodología integral y rigurosa que combine diferentes enfoques, de tal manera que puedan obtenerse resultados objetivos sobre los riesgos y amenazas que en un momento determinado pueden afectar la autenticidad, integridad, fiabilidad, disponibilidad y confidencialidad de los documentos y con ello su capacidad de satisfacer las necesidades de una organización.

3. LA GESTIÓN DEL RIESGO EN EL CONTEXTO COLOMBIANO

Frente a las reformas administrativas y cambios políticos y económicos, en Colombia se ha desarrollado normativa, modelos y metodologías que permiten la alineación de las políticas de desarrollo así como el monitoreo y evaluación de los avances en la gestión institucional. Dentro de este contexto, las políticas de gestión del riesgo constituyen un marco de acción necesario para dar cumplimiento a los objetivos institucionales y para garantizar la transparencia en la administración pública. A continuación se presentan algunos referentes para la gestión del riesgo en Colombia:

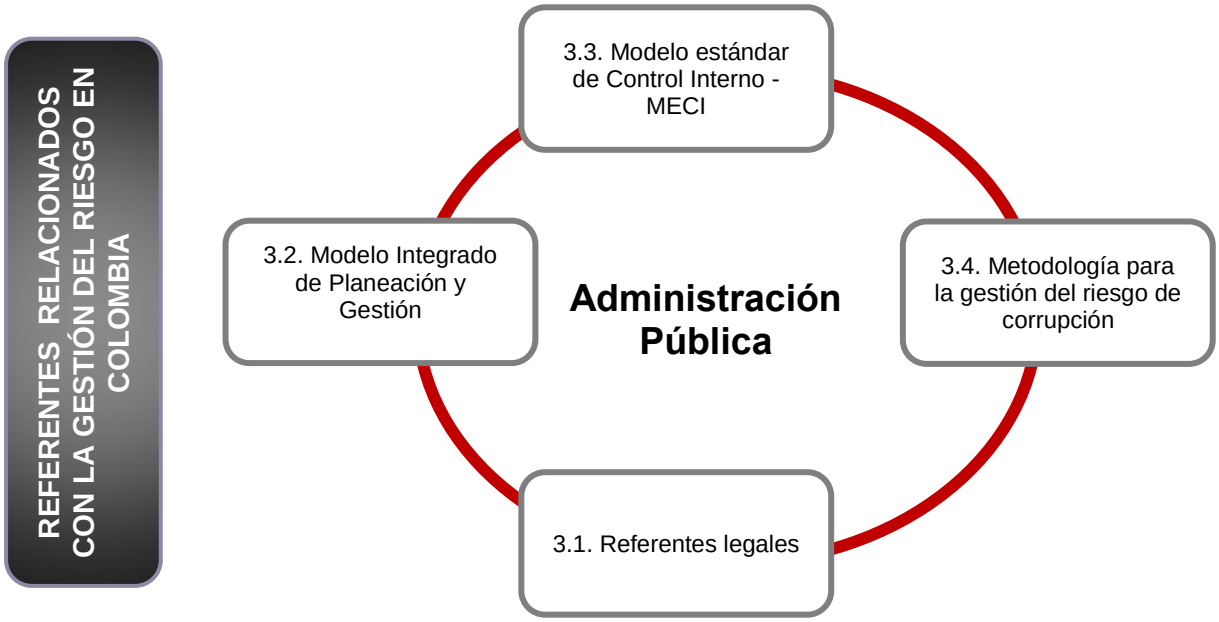

Figura 8. Referentes relacionados con la gestión del riesgo en Colombia
(Fuente: Elaboración propia, 2016)

3.1. Referentes legales

NORMA	CONTENIDO
Ley 87 de 1993	Establece normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones. Esta Ley define en su artículo 2 literal a). *Proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afecta*; y en el mismo artículo literal f). *Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de los objetivos*.
Ley 489 de 1988	Por la cual se dictan normas sobre la organización y funcionamiento de las entidades del orden nacional, se expiden las disposiciones, principios y reglas generales para el ejercicio de las atribuciones previstas en los numerales 15 y 16 del artículo 189 de la Constitución Política y se dictan otras disposiciones.
Ley 594 de 2000	Por medio de la cual se dicta la Ley general de archivos y se dictan otras disposiciones. Esta Ley tiene por objeto establecer las reglas y principios generales que regulan la función archivística del Estado.
Ley 1474 de 2011	Estatuto Anticorrupción, artículo 73. " Plan anticorrupción y de atención al Ciudadano" que deben elaborar anualmente todas las entidades del Estado, incluyendo el mapa de riesgos de corrupción, las medidas concretas para mitigar esos riesgos, las estrategias anti-trámites y los mecanismos para mejorar la atención al ciudadano.
Ley 1712 de 2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. Esta Ley regula el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de la información.
Decreto 2145 de 1999	Por el cual se dictan normas sobre el Sistema Nacional de Control Interno de las entidades y organismos de la Administración Pública del orden nacional y territorial y se dictan otras disposiciones. (Modificado parcialmente por el Decreto 2593 del 2000 y por el artículo 8 de la Ley 1474 de 2011.
Decreto 2593 de 2000	Por el cual se modifica parcialmente el Decreto 2145 de 1999.
Decreto 1537 de 2001	Reglamenta parcialmente la Ley 87 de 1993 y establece la *"administración de los riesgos*" como lo parte integral del fortalecimiento de los sistemas de control interno en las entidades públicas, las autoridades correspondientes establecerán y aplicarán *políticas de gestión del riesgo.*

Decreto 4485 de 2009	Por el cual se adopta en la Gestión Pública la actualización de la Norma Técnica de Calidad NTCGP 1000 en su versión 2009, numeral 4.1. Requisitos generales, literal g)"establecer controles sobre los riesgos identificados y valorados que puedan afectar la satisfacción del cliente y el logro de los objetivos de la entidad.
Decreto 1599 de 2005	Mediante el cual se adopta el Modelo Estándar de Control Interno (MECI) para todas las entidades del Estado, y se presenta el anexo técnico del MECI 1000:2005, 1.3. Componentes de la administración del riesgo.
Decreto 2482 de 2012	Modelo Integrado de Planeación y Gestión, por el cual se establecen los lineamientos generales para la integración de la planeación y la gestión.
Decreto 1080 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector Cultura. Este decreto compila las normas de carácter reglamentario que rigen el sector. En su Título II *Patrimonio Archivístico* compila los decretos que aplican al Sistema Nacional de Archivos y la gestión documental, en desarrollo de la Ley 594 de 2000.
Documento CONPES 3854	A través de este documento, el Consejo Nacional de Política Económica y Social de Colombia, establece la Política Nacional de Seguridad Digital, cuyo enfoque incluye la gestión del riesgo como uno de los elementos más importantes para abordar la seguridad digital.
Directiva presidencial 09 de 1999	Establece los lineamientos para la implementación de la Política de Lucha Anticorrupción.
Acuerdo 07 de 1994	Establece el reglamento general de archivos. En su artículo 64 estipula la obligatoriedad de adelantar controles sistemáticos y periódicos de las condiciones ambientales, instalaciones, manejo, mantenimiento y estado físico de los fondos. Y el parágrafo, establece los planes de prevención de desastres que contemplen sistemas de seguridad para la salvaguarda de los bienes documentales.
Acuerdo 050 de 2000	Por el cual se desarrolla el artículo 64 del título VII "Conservación de documentos", del Reglamento General de Archivos sobre "Prevención de deterioro de los documentos de archivo y situaciones de riesgo.
Acuerdo 006 de 2014	Por medio del cual se desarrollan los artículos 46, 47 y 48 del Título XI "Conservación de Documentos" de la Ley 594 de 2000. Este Acuerdo reglamenta el Sistema Integrado de Conservación –SIC, así como los planes de conservación documental y los planes de preservación digital a largo plazo. En su artículo 21 establece los riesgos mínimos que deben evaluarse para la formulación del plan de preservación digital a largo plazo.

Circular 001 de 2015	Da alcance a la expresión “Cualquier medio técnico que garantice su reproducción exacta”. Establece la necesidad de gestionar los riesgos asociados a la información, dentro del proceso de valoración documental.

Tabla 3. Referentes legales relacionados con la gestión del riesgo en Colombia
(Fuente: elaboración propia, 2016)

3.2. Modelos y referentes metodológicos

El desarrollo en la aplicación de las normas legales expuestas anteriormente, ha dado lugar a la generación de instrumentos que contribuyen a la administración pública en relación con la gestión del riesgo organizacional; estos instrumentos están alineados con la norma técnica de calidad NTC GP 1000 y la NTC-ISO 31000 de gestión del riesgo, teniendo como referencia los requisitos establecidos en el Modelo estándar de Control Interno - MECI.

3.2.1. Modelo Integrado de Planeación y Gestión

Mediante el Decreto 2482 de 2012 se adopta el Modelo Integrado de Planeación y Gestión como instrumento de articulación y reporte de la planeación. Este instrumento tiene como fin integrar los registros de avance de la gestión administrativa que permita el análisis, evaluación y control de los resultados para las entidades del Orden Nacional, y comprende los siguientes elementos:

- **Referentes**: Punto de partida para la construcción de la planeación; incluyen las metas de Gobierno establecidas en el Plan Nacional de Desarrollo, las competencias normativas asignadas a cada entidad y el marco fiscal.
- **Políticas de Desarrollo Administrativo**: Conjunto de lineamientos que orientan a las entidades en el mejoramiento de su gestión para el cumplimiento de las metas institucionales y de Gobierno, a través de la simplificación de procesos y procedimientos internos, el aprovechamiento del talento humano y el uso eficiente de los recursos administrativos, financieros y tecnológicos.
- **Metodología:** Esquema de planeación articulado que facilita la implementación de las políticas e iniciativas gubernamentales que estén orientadas a fortalecer el desempeño institucional, en procura del cumplimiento de las metas institucionales y de Gobierno para la prestación de un mejor servicio al ciudadano.

- **Instancias**: Responsables de liderar, coordinar y facilitar la implementación del modelo a nivel sectorial e institucional.
- **Formulario Único Reporte de Avances de la Gestión**: Herramienta en línea de reporte de avances de la gestión, como insumo para el monitoreo, evaluación y control de los resultados institucionales y sectoriales.

La metodología del Modelo aplica a las entidades y organismos de la Rama Ejecutiva del Poder Público del Orden Nacional en los términos señalados en el artículo 42 de la Ley 489 de 1998, y la herramienta empleada para el monitoreo y evaluación de los resultados de la gestión de la entidades, contempla aspectos de gestión documental relacionados con la planeación de la función archivística, planeación documental y procesos de gestión documental; y en lo referente al tema de riesgos, destina un apartado denominado *Transparencia, Participación y Atención al ciudadano,* sobre el Plan Anticorrupción y de Atención al Ciudadano, que a su vez incluye todos los aspectos referentes al mapa de riesgos de corrupción y las medidas para mitigarlos.

3.2.2. Modelo estándar de Control Interno - MECI[9]

El MECI es un modelo que especifica los requisitos para un Sistema de Control Interno aplicable a entidades obligadas por la Ley 87 de 1993 y se constituye en una herramienta de gestión que permite establecer las acciones, las políticas, los métodos, procedimientos y mecanismos de prevención, control, evaluación y de mejoramiento continuo de la entidad y para ello establece objetivos específicos agrupados en las siguientes categorías: objetivos de control de cumplimiento; objetivos de control de planeación y gestión; objetivos de control de ejecución; objetivos de control de información y comunicación.

[9] Mediante el Decreto 1599 de 2005 se adopta el Modelo Estándar de Control Interno (MECI) para todas las entidades del Estado, y se presenta el anexo técnico del MECI 1000:2005, 1.3. Componentes de la administración del riesgo.

El Modelo estándar de Control Interno - MECI está integrado por dos módulos, seis componentes y trece elementos, con un eje trasversal enfocado a la información y comunicación (Departamento Administrativo de la Función Pública, 2014). A continuación se presenta la estructura del MECI:

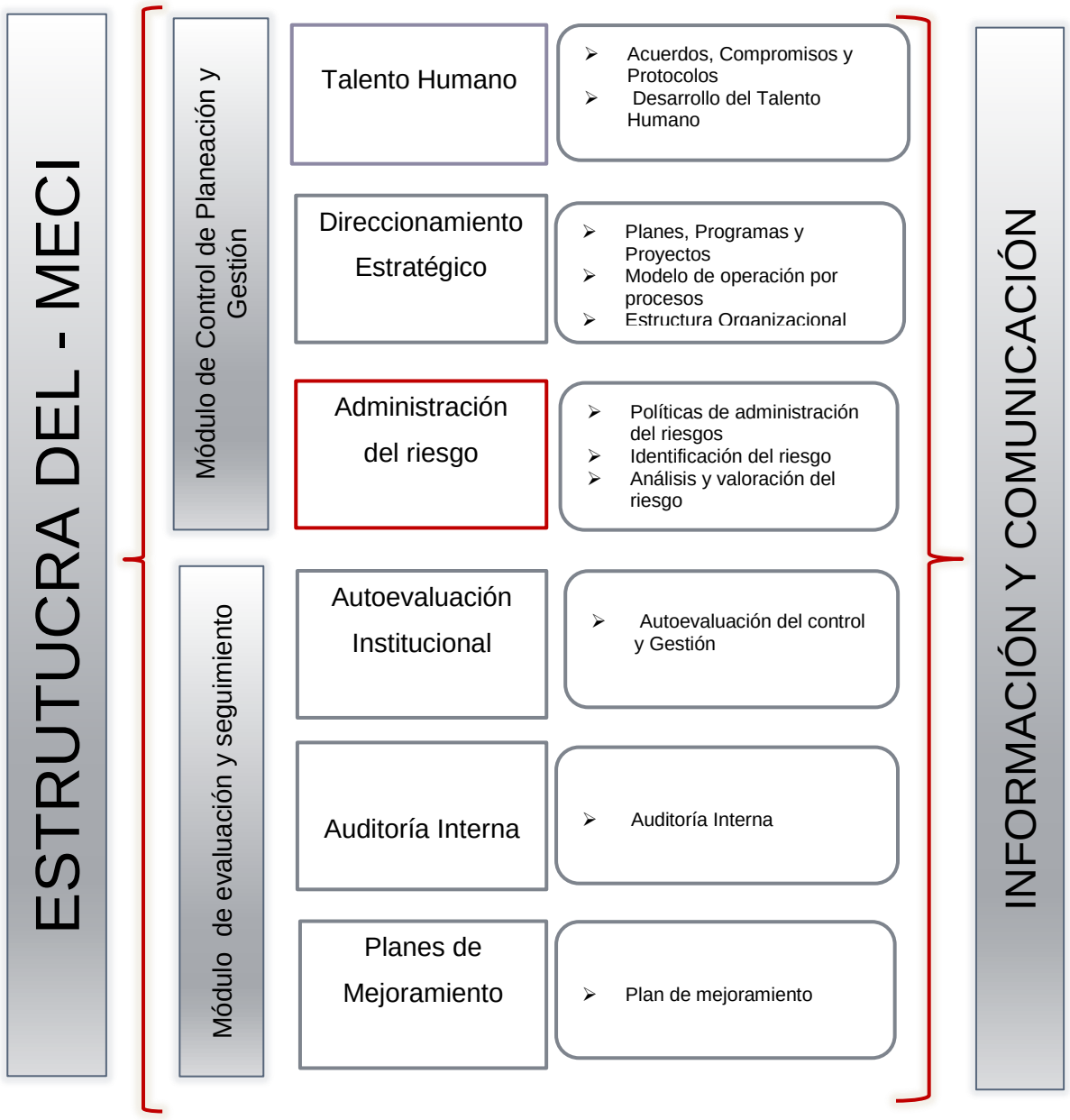

Figura 9. Estructura del MECI
(Fuente: Departamento Administrativo de la Función Pública, 2014)

Dentro de la estructura del MECI, la administración del riesgo es uno de los componentes del Módulo de Control de Planeación y Gestión y constituye el conjunto de elementos que le permiten a una entidad evaluar y gestionar aquellos eventos negativos, tanto internos como externos, que pueden afectar o impedir el logro de los objetivos institucionales o los eventos positivos, que permitan identificar oportunidades, para un mejor cumplimiento de su función. A continuación se presenta la estructura general de este componente, a través de sus tres elementos de control y sus productos mínimos:

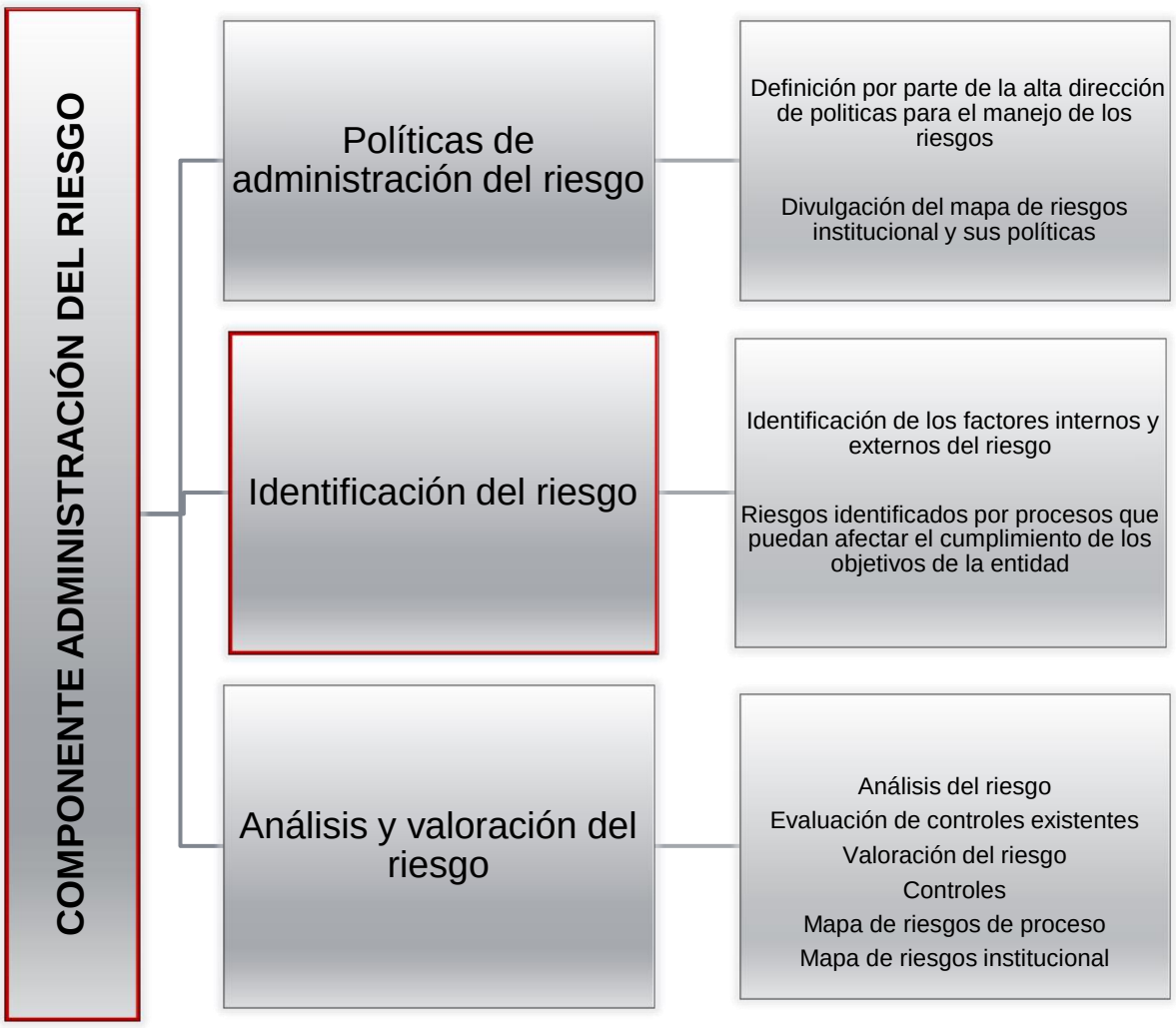

Figura 10. Estructura del componente *Administración del Riesgo* del MECI
(Fuente: Departamento Administrativo de la Función Pública, 2014)

Esta estructura corresponde a una metodología[10] general que facilita el cumplimiento de la normativa relacionada con la gestión del riesgo en las entidades públicas en Colombia la cual se integra con los procesos y objetivos de la entidad, como un elemento básico de la planeación estratégica.

De esta manera la intención de la normativa es hacer que la administración del riesgo se incorpore en el seno de las entidades como una política de gestión emanada de la alta dirección con la participación y apoyo de todos los servidores públicos.

La administración de riesgo siendo un componente del Módulo de Control de Planeación y Gestión, contribuye a la gestión institucional y el logro de los objetivos de una entidad y además fortalece el ejercicio del Control Interno en las entidades de la administración pública (Departamento Administrativo de la Función Pública, 2014).

A través de la Guía para la Administración del Riesgo, el Departamento Administrativo de la Función Pública desarrolla el componente de la administración del riesgo del MECI (Departamento Administrativo de la Función Pública, 2011). Ésta herramienta metodológica armoniza el Modelo Estándar de control interno MECI y la norma técnica de calidad NTCGP 1000:2009, con el fin de facilitar las entidades el ejercicio de la administración del riesgo con base en los procesos establecidos en la NTC-ISO 31000: 2011.

3.2.3. Metodología para la gestión del riesgo de corrupción

La Guía para la Gestión del Riesgo de Corrupción (Departamento Administrativo de la Función Pública, 2015) es una herramienta metodológica que se adapta a la metodología general para la gestión del riesgo (UNE-ISO 31000, 2010) y se encuentra alineada con otros instrumentos de gestión como el Modelo Integrado de Planeación y Gestión y el Modelo Estándar de Control Interno – MECI. El marco legal se fundamenta en el Estatuto Anticorrupción (Ley 1474 de 2011) y la Ley de Transparencia y Acceso a la Información Pública Nacional (Ley 1712 de 2014).

[10] De conformidad con el Decreto 1599 de 2005, el Departamento Administrativo de la Función Pública - DAFP, es el encargado de administrar y distribuir para todas las entidades del Estado obligadas, los instrumentos necesarios para el diseño, desarrollo e implementación de cada uno de los elementos, componentes y subsistemas del Modelo Estándar de Control Interno.

En esta guía se incluye el Impacto en la valoración del riesgo de corrupción y para su medición se propone el diligenciamiento de un cuestionario de dieciocho preguntas para determinar la zona en que se encuentra un determinado riesgo y con ello poder evaluar los controles para minimizar los riesgos de corrupción.

La gestión del riesgo en el contexto colombiano, está relacionada con un marco legal en el que este proceso se considera como un elemento transversal dentro de lineamentos y directrices dirigidos a la administración pública.

De este modo, a través de leyes, decretos, acuerdos y documentos de política, relacionados con aspectos de la gestión pública, control interno de las entidades, gestión documental, seguridad de la información, planes anticorrupción, transparencia, control de riesgos, prevención de deterioro y situaciones de riesgo de archivos, planes de conservación documental y de preservación digital, así como uso de medios tecnológicos, entre otros, es que se aborda la gestión del riesgo en Colombia.

4. PROPUESTA METODOLÓGICA PARA LA IDENTIFICACIÓN DE RIESGOS ASOCIADOS A LA GESTIÓN DOCUMENTAL

4.1. Introducción

Los riesgos dependen de las particularidades de la organización y por lo tanto su variedad puede ser alta, así que resulta difícil establecer una sola metodología para la identificación y clasificación de riesgos asociados a procesos y sistemas de gestión documental. En primera instancia es importante tener en cuenta que para ello es necesario tener claridad que el proceso de identificación del riesgo debe integrarse a la gestión del riesgo organizacional y evitar que el mismo se realice de forma parcial o fragmentaria.

La identificación de riesgos se realiza con el fin de estar preparados ante eventos inesperados e imprevistos que puedan afectar de forma negativa el logro de los objetivos de la organización o evitar sanciones por el incumplimiento de normas legales. En positivo, la identificación del riesgo, permite detectar aquellos aspectos relacionados con el riesgo, que pueden convertirse en una oportunidad para el cumplimiento de los objetivos de la organización.

A nivel organizacional el personal responsable de la identificación de riesgos estratégicos puede estar en la alta dirección. Para los riesgos relacionados con el proceso de gestión documental, los responsables deben ser los líderes de los procesos, proyectos, servicios o productos relacionados con la gestión documental, específicamente los líderes de procesos y sistemas de gestión documental, quienes con el apoyo del administrador del riesgo de la organización, adelantarán las actividades relativas a la identificación del riesgo.

Es muy importante tener en cuenta que los responsables de los riesgos, deben tener conocimiento y experticia en el ámbito de la gestión documental, procesos y sistemas de gestión documental y estar capacitados en materia de gestión del riesgo, para poder desarrollar el proceso de identificación de acuerdo con las metodologías y las técnicas más adecuadas para el desarrollo del proceso.

Además del conocimiento técnico, este proceso implica que el personal encargado de la identificación de riesgos esté abierto a nuevas ideas o posibilidades y tenga la capacidad de proyectar la influencia de eventos negativos o positivos sobre los procesos relacionados con la

gestión documental, manteniendo siempre la objetividad en las apreciaciones referidas al riesgo. (Mejía Quijano, Identificación de Riesgos, 2013).

El alcance de esta propuesta metodológica es el subproceso de identificación del riesgo en procesos y sistemas de gestión documental establecido en la norma UNE-ISO/TR 18128:2014, tal como se ilustra a continuación:

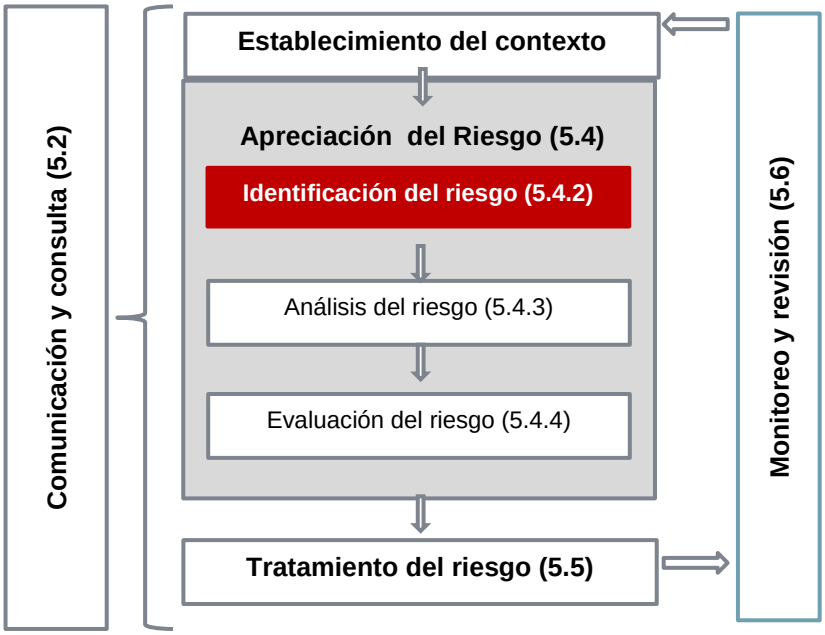

Figura 11. Esquema del proceso para la gestión del riesgo
(Fuente: UNE-ISO/TR 18128, 2014)

Las referencias para el desarrollo de esta metodología se encuentran en la norma UNE-ISO/TR 18128:2014, así como en normas y metodologías aplicables dentro del marco legal colombiano relacionado con la gestión del riesgo. También se tienen en cuenta los referentes teóricos y conceptuales aplicables a la identificación del riesgo, citados en este documento.

4.2. Objetivo de la identificación de riesgos en procesos y sistemas de gestión documental

La identificación del riesgo tiene por objeto encontrar, reconocer y describir el riesgo; este proceso implica la detección del origen o las fuentes de riesgo, los eventos así como sus causas y consecuencias (UNE-ISO 31000, 2010). Puntualmente y en relación con los procesos y sistemas de gestión documental, este proceso tiene como objetivo detectar lo que puede suceder o qué situaciones pueden darse que puedan afectar la capacidad de los documentos para satisfacer las necesidades de la organización (UNE-ISO/TR 18128, 2014).

4.3. Términos y definiciones básicas para la identificación del riesgo en procesos y sistemas de gestión documental

Para el desarrollo y aplicación de esta metodología, aplican las los términos y definiciones establecidos en la norma UNE- ISO 31000:2010 *gestión del riesgo* y la UNE-ISO/TR 18128: 2014 *Apreciación del riesgo en procesos y sistemas de gestión documental*; las definiciones específicas de esta propuesta metodológica son:

- **Riesgo:** efecto de incertidumbre.
- **Gestión del riesgo:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
- **Identificación del riesgo:** proceso para encontrar, reconocer y describir el riesgo.
- **Procesos de gestión documental:** conjunto de actividades de la organización que crean, controlan, conservan y eliminan documentos (UNE-ISO/TR 18128: 2014)
- **Sistema de gestión documental:** sistema de información que captura, gestiona y facilita el acceso a los documentos a lo largo del tiempo (UNE-ISO/TR 18128: 2014)

4.4. Metodología para la identificación del riesgo en procesos y sistemas de gestión documental

Esta metodología de identificación del riesgo, tiene un enfoque de hechos y requisitos, basado en el análisis de referentes preexistentes para la identificación de riesgos y en el análisis de los requerimientos del marco jurídico que regula la administración pública y la función archivística en el Estado colombiano, así como de los requisitos establecidos en las normas técnicas y estándares nacionales y/o internacionales sobre gestión documental, como las que se relacionan en este documento.

Las herramientas y técnicas para identificación del riesgo en procesos y sistemas de gestión documental seleccionadas son listas de verificación y cuestionarios. Tanto las listas de verificación como los cuestionarios pueden utilizarse en combinación con otras técnicas como por ejemplo, la entrevista, de tal manera que pueda darse mayor claridad al desarrollo de proceso y con ello lograr una identificación de los riesgos más eficiente.

Esta metodología se desarrolla a partir de los siguientes componentes con sus actividades específicas:

1. Establecimiento del contexto externo e interno de la organización
2. Aplicación de listas de verificación de riesgos
3. Aplicación de cuestionarios para la identificación de riesgos
4. Identificación de riesgos
5. Registro de riesgos

Como herramientas metodológicas, se presentan tablas cuyos campos permiten estructurar y analizar la información; estas tablas tienen carácter orientativo y sirven para dar una idea de cómo realizar la identificación de los riesgos en procesos y sistemas de gestión documental y aportan a la elaboración del inventario, la clasificación y catalogación de riesgos institucional.

4.4.1. Establecimiento del contexto externo e interno de la organización

El contexto externo e interno de la organización, se establece a partir de la identificación de factores externos (fuera del control de la organización) e internos (no controlados por los responsables de los procesos y sistemas de gestión documental), que pueden generar oportunidades o afectar negativamente el cumplimiento de la misión y objetivos de una institución.

Teniendo como referencia la norma UNE-ISO/TR 18128: 2014, a continuación se presenta una clasificación de los factores externos e internos de una organización, según las áreas de incertidumbre que allí se establecen y algunos de los elementos que deben tenerse en cuenta para la identificación de los riesgos asociados a la gestión documental.

Estos elementos se determinan a partir del análisis político, social, económico, tecnológico, cultural y normativo tanto externo como interno de la organización, cuya información puede estructurarse siguiendo el modelo que se presenta en la tabla a continuación:

FACTORES EXTERNOS			FACTORES INTERNOS	
Políticos	Modificaciones legales y normativas. Pueden ser de carácter nacional o internacional		**Cambios organizacionales**	Supresión Fusión, Privatización Liquidación, Reestructuración, Reducción, Externalización
Sociales	Nuevas políticas públicas, de carácter nacional o internacional		**Cambio tecnológico**	Introducción de nuevas tecnologías de la información
Macroeconómicos	Propagación de tecnologías de la información para uso comercial y actividades de negocio		**Personas y competencias**	Personal competente para realizar actividades relacionadas con

FACTORES EXTERNOS			FACTORES INTERNOS	
Tecnológicos	Introducción y adopción de nuevas tecnologías de la información de manera transversal en la sociedad			procesos, sistemas de gestión documental y tecnologías de la información
Entorno físico e infraestructura	Desastres naturales, acciones de guerra y terrorismo, daños en instalaciones físicas		**Recursos económicos y materiales**	Disponibilidad de recursos para la adecuada gestión de los procesos y sistemas de gestión documental. Este elemento está relacionado con el contexto externo de la organización.
Seguridad externa	Amenazas a la seguridad, accesos no autorizados a los sistemas, virus informáticos, espionaje, vandalismo físico, pérdida de servicios de terceros, entre otros.			

Tabla 4. Contexto de la organización. Factores externos e internos
(Fuente: elaboración propia, adaptado de UNE-ISO/TR 18128, 2014)

4.4.2. Aplicación de listas de verificación

Las listas de verificación son herramientas estándar o formatos preestablecidos que pueden aplicarse a la organización e incluso de manera global a un amplio número de organizaciones; son útiles para la creación del inventario y catálogo de riesgos.

Existen listas de amenazas preestablecidas, realizadas por diferentes organizaciones para la identificación de riesgos. Estas listas son los principales referentes para la construcción de las listas de verificación de riesgos aplicables a una organización.

Algunas sobre amenazas, riesgos y recomendaciones, relacionados con sistemas de información, uso del *cloud* y preservación digital, que pueden tomarse como referencia para la elaboración de las listas de verificación para la identificación de riesgos asociados a procesos y sistemas de gestión documental, son las que se presentan en la figura a continuación:

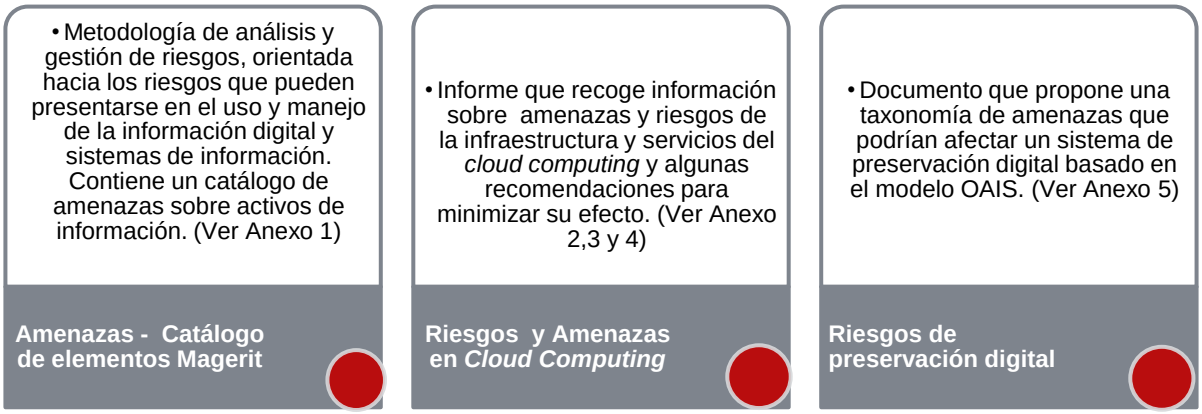

Figura 12. Referentes de listas de amenazas, riesgos y recomendaciones
(Fuente: elaboración propia, 2016)

a) Actividades para la elaboración y aplicación de listas de verificación

- Identificación de listas de verificación o catálogo de riesgos asociados a la gestión documental, elaborado por diferentes organizaciones. (ver Anexos 1 a 5).
- Recopilación de los riesgos aplicables al proceso de gestión documental, junto con su descripción, según el alcance definido y las actividades de la organización. El resultado es la construcción de una lista de riesgos.
- Identificación de riesgos asociados a procesos y sistemas de gestión documental de la organización mediante la aplicación de la lista de verificación de riesgos.
- Elaboración del informe de los riesgos identificados con las observaciones que precisan por qué podrían ocurrir en la organización.

b) Aplicación de la herramienta para listas de verificación de riesgos

Para la recopilación de información generada en el desarrollo de las actividades expuestas, se puede elaborar una tabla con los siguientes campos para el registro de información:

RIESGO	DESCRIPCIÓN	SI	NO	OBSERVACIONES

Tabla 5. Aplicación de lista de verificación para la identificación de riesgos
(Fuente: elaboración propia, 2016)

La descripción de cada uno de los campos de la tabla es la siguiente:

- ✓ **Riesgo**: Efecto de incertidumbre. El nombre debe ser corto, genérico y expresar un evento (negativo o positivo).
- ✓ **Descripción**: Caracterización general del riesgo que da claridad sobre el escenario de ocurrencia del riesgo, la probabilidad y las consecuencias.
- ✓ **SI/NO:** una vez revisados cada uno de los elementos de la lista de verificación de riesgos, se selecciona SI o NO el riesgo ha sido identificado.
- ✓ **Observaciones:** anotaciones que sirven para mejorar el entendimiento de los riesgos identificados y establecer sus causas.

4.4.3. Aplicación de cuestionarios

Los cuestionarios son herramientas que constan de dos elementos: las preguntas y las respuestas. El número de preguntas varía dependiendo de los ajustes que se hagan al cuestionario de referencia o estándar de acuerdo con las particularidades de la organización (Mejía Quijano, Administración de riesgos. Un enfoque empresarial, 2006). El cuestionario de referencia o estándar para el desarrollo de esta propuesta, es el que se presenta en el Anexo B de la norma (UNE-ISO/TR 18128: 2014) y las preguntas se elaboran de acuerdo con los

controles establecidos para el cumplimento de los requisitos establecidos en normas y estándares relacionados con la gestión documental.

a) Actividades para la aplicación del cuestionario para la identificación de riesgos

- Identificación de normativa legal, normas y estándares técnicos aplicables a la gestión documental y modelo de gestión documental.
- Identificación de los controles de las normas técnicas y estándares técnicos relacionados con procesos y sistemas de gestión documental. El resultado de esta sub-actividad es una lista de los controles establecidos en la normativa.
- Elaboración del cuestionario de riesgos, basado en la descripción de los controles para el cumplimiento de requisitos establecidos las normas técnicas identificadas, siguiendo las categorías en las que se clasifican las áreas de incertidumbre de la norma de referencia UNE-ISO/TR 18128:2014.
- Identificación de riesgos asociados a procesos y sistemas de gestión documental de la organización. En este caso los riesgos se identifican por la ausencia de los controles establecidos en las normas técnicas.
- Elaboración del informe de los riesgos identificados con las observaciones que precisan por qué podrían ocurrir en la organización. Para la elaboración del cuestionario de riesgos, también se puede tomar como referencia el Anexo B de la norma UNE-ISO/TR 18128: 2014, que de manera informativa presenta varios ejemplos que sirven para la construcción de los cuestionarios.

  Las preguntas están relacionadas con las diferentes áreas de incertidumbre que se estructuran e tres categorías: Contexto (factores externos y factores internos), sistemas y procesos de gestión documental; a través de estas preguntas se indaga sobre las situaciones que pueden representar riesgo.

b) Aplicación de la herramienta para cuestionarios de identificación de riesgos

Para la recopilación de esta información, se puede elaborar una tabla con los siguientes campos para el registro de información:

REQUISITOS / CONTROLES	CUESTIONARIO	SI	NO	RIESGO	DESCRIPCIÓN
AREA DE INCERTIDUMBRE: CONTEXTO - FACTORES EXTERNOS					
ÁREA DE INCERTIDUMBRE: CONTEXTO - FACTORES INTERNOS					
AREA DE INCERTIDUMBRE: SISTEMAS DE GESTIÓN DOCUMENTAL					
AREA DE INCERTIDUMBRE: PROCESOS DOCUMENTALES					

Tabla 6. Aplicación de cuestionarios para la identificación de riesgos
(Fuente: elaboración propia, 2016)

La descripción de cada uno de los campos de la tabla es la siguiente:

- ✓ **Requisitos/Controles:** referencia de los requisitos (legales, técnicos, normativos) a los que están asociados los controles que darán origen a las preguntas, en los ítems que corresponda. Por ejemplo normas técnicas como la UNE-ISO/IEC 27001:2014 *Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la*

Información (SGSI). Requisitos y la UNE-ISO 30301:2011 *Información y documentación. Sistemas de gestión de documentos. Requisitos* y normativa sobre archivos y gestión documental, entre otros.

- ✓ **Cuestionario**: Preguntas para la identificación de riesgos, basadas en los controles para el cumplimiento de los requisitos.
- ✓ **Si – No:** son las respuestas al cuestionario que permitirán la identificación del riesgo. **Si**, quiere decir que se cumple con el requisito por la existencia del control; **No**, que no se cumple con el mismo por la ausencia del control.
- ✓ **Riesgo:** efecto de incertidumbre. El nombre debe ser corto, genérico y expresar un evento (negativo o positivo). Se identifica a partir de las respuestas obtenidas en la aplicación del cuestionario.
- ✓ **Descripción:** Caracterización general del riesgo que da claridad sobre el escenario de ocurrencia del riesgo, la probabilidad y las consecuencias.

En particular, esta técnica se puede complementar con una entrevista para facilitar la comprensión de las preguntas por parte de la persona o el grupo que diligencia el cuestionario.

4.4.4. Identificación de riesgos

Con la información obtenida mediante el empleo de la lista de verificación y cuestionario de riesgos, se identifican los riesgos asociados a procesos y sistemas de gestión documental, de conformidad con las áreas de incertidumbre establecidas en la norma UNE-ISO/TR 18128: 2014 y las cuatro categorías de riesgos definidas por la Organización ARMA. A continuación se presenta una tabla con los campos para el registro de información que sirve para la consolidación de los datos obtenidos en los pasos anteriores:

RIESGO	TIPO DE RIESGO	DESCRIPCIÓN	CAUSAS	CONSECUENCIAS
CONTEXTO - FACTORES EXTERNOS				
CONTEXTO - FACTORES INTERNOS				

RIESGO	TIPO DE RIESGO	DESCRIPCIÓN	CAUSAS	CONSECUENCIAS
SISTEMAS DE GESTIÓN DOCUMENTAL				
				.
PROCESOS DOCUMENTALES				

Tabla 7. Identificación de riesgos asociados a procesos y sistemas de gestión documental (Fuente: elaboración propia, 2016)

La descripción de cada uno de los campos de la tabla es la siguiente:

- ✓ **Riesgo:** Efecto de incertidumbre. Nombre del riesgo, el cual debe ser corto y genérico y expresar un evento (negativo o positivo). En esta tabla, se recogen los riesgos que han sido identificados en la aplicación de las listas de verificación o a través del cuestionario.
- ✓ **Tipo de riesgo:** información sobre las categorías de riesgos teniendo en cuenta el cuadrante de riesgos de ARMA: Riesgos (administrativos, control de documentos, legales o normativos y tecnológicos). Un riesgo puede clasificarse en una o más categorías.
- ✓ **Descripción:** Caracterización general del riesgo que da claridad sobre el escenario de ocurrencia del riesgo, la probabilidad y las consecuencias. Puede relacionarse con la actividad del proceso de gestión documental.
- ✓ **Causas:** Son los motivos o razones por las cuales se puede presentar un riesgo. Pueden ser múltiples.
- ✓ **Consecuencias:** Corresponden a los efectos, negativos o positivos de la ocurrencia de los riesgos. Pueden ser varias por cada riesgo.
- ✓ **Contexto - factores externos**: Los factores externos son áreas de incertidumbre que están por fuera del control de la organización, pero que afectan a los documentos y los sistemas donde se crean y gestionan.
- ✓ **Contexto - factores internos:** Los factores internos son áreas de incertidumbre que tienen un efecto inmediato en la gestión de los documentos. Están relacionados con los cambios

del entorno económico, tecnológico y estructural de las organizaciones, para adaptarse a nuevas circunstancias.

- ✓ **Sistemas de gestión documental:** son áreas de incertidumbre relacionadas con los sistemas para crear y controlar documentos, cambian a lo largo del tiempo de acuerdo con el contexto externo e interno de la organización y por esto es necesario que la alta dirección esté informada y asuma la responsabilidad de respuesta de la organización ante posibles amenazas.
- ✓ **Procesos documentales:** Son áreas de incertidumbre en las que la identificación de riesgos se centra en la creación de los documentos, en los procesos de control para gestionarlos y en los sistemas de gestión documental.

4.4.5. Registro de riesgos

El registro de riesgos debe permitir su adecuada gestión dentro del sistema, a fin de garantizar su trazabilidad e interrelación. Dentro del subproceso de identificación del riesgo, los campos de registro que deben tenerse en cuenta son los siguientes:

CAMPO DE REGISTRO	DESCRIPCIÓN
ID	Identificador del riesgo que permite el procesamiento de la información mediante herramientas de análisis y gestión.
Nombre del riesgo	El nombre debe ser corto y genérico. Representa la probabilidad de ocurrencia de un evento negativo o positivo cuyas consecuencias pueden afectar el logro de los objetivos de la organización.
Tipo de riesgo	Categoría y subcategoría de riesgo que facilitan su identificación de forma estructurada. En esta propuesta se tienen en cuenta las categorías establecidas por la organización ARMA.
Descripción	Características generales o formas en las que se manifiesta el riesgo identificado. Debe tener en cuenta las categorías y subcategorías de referencia.
Causas	Motivos o razones por las cuales se puede presentar un riesgo. Pueden ser múltiples.

CAMPO DE REGISTRO	DESCRIPCIÓN
Consecuencias	Efectos negativos o positivos de la ocurrencia de los riesgos. Pueden ser varias por cada riesgo.
Propietario del riesgo	Responsable del proceso, proyecto o servicio según las funciones de la organización.
Fecha de identificación	Fecha del levantamiento de la información.
Fecha de última actualización	Fecha de la actualización, en caso que el riesgo se haya identificado anteriormente.

Tabla 8. Registro de identificación del riesgo
(Fuente: elaboración propia, adaptado de UNE-ISO/TR 18128 IN: 2014)

La aplicación de listas de verificación y cuestionario de riesgos, son herramientas técnicas útiles para desarrollar el subproceso de identificación del riesgo con un enfoque tanto de hechos como de requisitos, ya que permiten combinar elementos de riesgos y amenazas seleccionados de listas elaboradas por diferentes organizaciones, con elementos del riesgo identificados a partir del análisis de las respuestas de cuestionarios elaborados con base en los controles establecidos para el cumplimiento de los requisitos legales y técnicos para la gestión de documentos.

Estas herramientas técnicas pueden complementarse con otras como las entrevistas para lograr mayor objetividad en la identificación del riesgo y facilitar la identificación de las causas y posibles consecuencias de los riesgos, que serán de gran utilidad en las siguientes etapas de análisis y evaluación del riesgo en procesos y sistemas de gestión documental.

5. CONCLUSIONES

Esta propuesta constituye una metodología integral para la identificación del riesgo que combina diferentes enfoques con énfasis en el de requisitos.

Se encuentra alineada con la norma UNE-ISO 31000:2010 de gestión del riesgo y con la norma UNE-ISO/TR 18128:2014 de apreciación de riesgos en procesos y sistemas de gestión documental.

Es un referente metodológico para la identificación de riesgos asociados a la gestión documental dentro del contexto colombiano.

Plantea la aplicación de herramientas técnicas complementarias para la identificación del riesgo, como son listas de verificación y cuestionarios, que ayudan a mejorar el control de los documentos y de su uso para los fines de una organización.

Facilita la difusión del tema específico de riesgos en gestión documental, procesos y sistemas de gestión documental, en el contexto colombiano.

Es viable su articulación con los instrumentos de control y reporte establecidos por la administración pública en Colombia para su aplicación.

Responde a las necesidades que demanda el contexto de la gestión documental en Colombia.

Es un punto de partida para el desarrollo de futuras investigaciones relacionadas con el tema y sirve de referencia para su aplicación en diferentes el ámbitos de la gestión documental.

Amplía la visión general de la gestión de riesgos organizacional, ya que pone de manifiesto la importancia de los riesgos asociados a la gestión documental.

Ésta es una propuesta innovadora que se convierte en un aporte significativo para el desarrollo de la política de archivos en Colombia.

El marco de acción de la identificación de riesgos asociados a procesos y sistemas de gestión documental, representa uno de los compromisos de la administración pública para alcanzar los fines de la transparencia.

6. BIBLIOGRAFIA Y FUENTES

Administración Electrónica (PAe). (2012). MAGERIT - versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catalogo de elementos. (M. d. Públicas, Ed.) Madrid, : Ministerio de Hacienda y Administraciones públicas. Recuperado el 31 de Agosto de 2016, de http://administracionelectronica.gob.es/

ARMA International. (2009). Evaluating and Mitigating Records and Information Risks. An ARMA International Guideline. USA: ARMA International.

Bustelo, R. C. (s.f.). Identificación de riesgos en la producción, gestión y mantenimiento de documentos electrónicos. (F. F. Catalunya, Ed.) Recuperado el 15 de Mayo de 2016, de https://www.exabyteinformatica.com/uoc/Informatica/Analisis_del_contexto_organizativo/Analisis_del_contexto_organizativo_(Modulo_7).pdf

Casadesús, A. (2015). Gestión de riesgos aplicada a la gestión de documentos: una metodología para garantizar una rendición de cuentas confiable. I Xornadas Fundación Olga Gallego, (págs. 119–135.).

Consejo Superior de Administración Electrónica. (Octubre de 2012). Portal de Administración Electrónica. Recuperado el 13 de Agosto de 2016, de http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.V69iKrjhCM8

Departamento Administrativo de la Función Pública. (2011). Guía para la Administración del Riesgo. Recuperado el 27 de Julio de 2016, de https://www.funcionpublica.gov.co/documents/418537/506911/1592.pdf/73e5a159-2d8f-41aa-8182-eb99e8c4f3ba

Departamento Administrativo de la Función Pública. (2014). Manual Técnico del Modelo Estandar de Control Interno para el Estado Colombiano MECI 2014. Recuperado el 1 de Junio de 2016, de Portal Función Pública: http://portal.dafp.gov.co/form/formularios.retrive_publicaciones?no=2162

Departamento Administrativo de la Función Pública. (2015). Guía para la Gestión del Riesgo de Corrupción. Recuperado el 1 de Septiembre de 2016, de https://www.funcionpublica.gov.co/documents/418537/616038/GUIA+PARA+LA+GESTI

ON+DE+RIESGO+DE+CORRUPCION+%282%29.pdf/e301def2-8218-4205-a320-99c3ef9989f6

Egbuji, A. (1999). Risk management of organisational records. Records Management Journal, 9 (Iss2), 93-116.

Instituto Nacional de Tecnologías de la Comunicación. (2011). Riesgos y Amenazas en Cloud Computing. Obtenido de www.inteco.es

Lemieux, V. (2004). Two Approaches to Managing Information Risk. The Information Management Journal, 56-62.

Lemieux, V. (Julio de 2010). The records-risk nexus: Exploring the relationship between records and risk. RecordsManagement Journal, 20(Iss 2), 199-216.

Lobato Domínguez, J. (1 de Mayo de 2009). El nuevo marco normativo en Gestión de documentos de archivo, las normas ISO / UNE: Guía para profesionales. Recuperado el 05 de Agosto de 2016, de http://www.juntadeandalucia.es/cultura/archivos_html/sites/default/contenidos/general/revista/numeros/Numero_1/galeria/01-05_Javier_Lobato_Domxnguez.pdf

Mejía Quijano, R. C. (2006). Administración de riesgos. Un enfoque empresarial. Medellín: Fondo Editorial Universidad EAFIT.

Mejía Quijano, R. C. (2013). Identificación de Riesgos. Medellín: Fondo Editorial Universidad EAFIT.

NTC:5921. (2012). Información y documentación. Requisitos para el almacenamiento documental. Instituto Colombiano de Normas Técnicas y Certificación.

Pullen, T., & Maguire, H. (2007). The information management risk construct: identifying the potential impact of information, quality on corporate risk. International Journal of Information Quality, 412-443.

Rosenthal, D. S., Robertson, T., Lipkis, T., Reich, V., & Morebito, S. (Noviembre de 2005). Requirements for Digital Preservation Systems. A Bottom-up Approach. D-Lib Magazine, 11(11).

UNE-ISO 31000. (2010). Gestión del Riesgo. Principios y directrices. Instituto Colombiano de Normas Técnicas y Certificación.

UNE-ISO/TR 18128. (2014). Información y documentación. Apreciación del riesgo en procesos y sistemas de gestión documental. Asociación Española de Normalización y Certificación.

UNE-ISO 30301:2011 Información y documentación. Sistemas de gestión de documentos. Requisitos. Asociación Española de Normalización y Certificación.

UNE/ISO15489-1:2006, Información y documentación. Gestión de documentos Parte 1: Generalidades. Asociación Española de Normalización y Certificación.

UNE/ISO 23081:2011 Información y documentación. Procesos de gestión de documentos. Metadatos para la gestión de documentos. Parte 2: Elementos de implementación y conceptuales. Asociación Española de Normalización y Certificación.

UNE-ISO/IEC 27001:2014 Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información (SGSI). Requisitos. Asociación Española de Normalización y Certificación.

UNE-ISO/IEC 27002:2009 Tecnología de la Información Técnicas de seguridad. Código de buenas prácticas para la gestión de la seguridad de la información. Asociación Española de Normalización y Certificación.

UNE-ISO 31000:2010 Gestión del riesgo. Principios y directrices, es una norma que brinda los principios y directrices. Asociación Española de Normalización y Certificación.

7. ANEXOS

7.1. Anexo 1. Catálogo de elementos de riesgo MAGERIT

AMENAZAS	*DESCRIPCIÓN*
Desastres naturales: Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta. (origen natural, accidental)	
Fuego	Incendios: posibilidad de que el fuego acabe con recursos del sistema.
Daños por agua	Inundaciones: posibilidad de que el agua acabe con recursos del sistema.
De origen industrial: Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.	
Fuego	Incendio: posibilidad de que el fuego acabe con los recursos del sistema.
Daños por agua	Escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.
Desastres industriales	Otros desastres debidos a la actividad humana: explosiones, derrumbes, contaminación química, sobrecarga eléctrica, fluctuaciones eléctricas, accidentes de tráfico,
Contaminación mecánica	Vibraciones, polvo, suciedad
Contaminación electromagnética	Interferencias de radio, campos magnéticos, luz ultravioleta
Avería física o lógica	Fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema. En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.
Corte del suministro eléctrico	Cese de la alimentación de potencia.
Condiciones inadecuadas de temperatura y humedad	Deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad.
Fallo de servicios de comunicaciones	Cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente.
Interrupción de otros servicios y suministros esenciales	Otros servicios o recursos de los que depende la operación de los equipos; por ejemplo, papel para las impresoras, tóner, refrigerante, ...

AMENAZAS	***DESCRIPCIÓN***
Degradación de los soportes de almacenamiento de la información	Como consecuencia del paso del tiempo
Emanaciones electromagnéticas	Hecho de poner vía radio datos internos a disposición de terceros. Es una amenaza donde el emisor es víctima pasiva del ataque. Prácticamente todos los dispositivos electrónicos emiten radiaciones al exterior que pudieran ser interceptadas por otros equipos (receptores de radio) derivándose una fuga de información.
Errores y fallos no intencionados: Fallos no intencionales causados por las personas. El orden está alineado con los ataques deliberados, muchas veces de naturaleza similar a los errores no intencionados, difiriendo únicamente en el propósito del sujeto.	
Errores de los usuarios	Equivocaciones de las personas cuando usan los servicios, datos, etc.
Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación.
Errores de monitorización	Inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos...
Errores de configuración	Introducción de datos de configuración erróneos. Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.
Deficiencias en la organización	Cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión. Acciones descoordinadas, errores por omisión, entre otros.
Difusión de software dañino	Propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.
Errores de re-encaminamiento	Envío de información a través de un sistema o una red usando accidentalmente una ruta incorrecta que lleve la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Es particularmente destacable el caso de que el error de encaminamiento suponga un error de entrega, acabando la información en manos de quien no se espera.
Errores de secuencia	Alteración accidental del orden de los mensajes transmitidos.
Escapes de información	La información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en sí misma se vea alterada.
Alteración accidental de la información	Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.
Destrucción de información	Pérdida accidental de información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún

AMENAZAS	*DESCRIPCIÓN*
	soporte informático, hay amenazas específicas.
Fugas de información	Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel, etc.
Vulnerabilidades de los programas (software)	Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar.
Errores de mantenimiento/ actualización de programas (software)	Defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.
Errores de mantenimiento/ actualización de programas (software)	Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.
Caída del sistema por agotamiento de recursos	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
Pérdida de equipos	La pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. Se puede perder todo tipo de equipamiento, siendo la pérdida de equipos y soportes de información los más habituales. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.
Indisponibilidad del personal	Ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriológica,...
Ataques Intencionados: Fallos deliberados causados por las personas. El orden está determinado para coordinarlo con los errores no intencionados, muchas veces de naturaleza similar a los ataques deliberados, difiriendo únicamente en el propósito del sujeto.	
Manipulación de los registros de actividad	Manipulación de los registros de actividad.
Manipulación de la configuración	Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.
Suplantación de la identidad del usuario	Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la organización o por personal contratado temporalmente.
Abuso de privilegios de acceso	Cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.
Uso no previsto	Utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.

AMENAZAS	***DESCRIPCIÓN***
Difusión de software dañino	Propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.
Re-encaminamiento de mensajes	Envío de información a un destino incorrecto a través de un sistema o una red, que llevan la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Un atacante puede forzar un mensaje para circular a través de un nodo determinado de la red donde puede ser interceptado. Es particularmente destacable el caso de que el ataque de encaminamiento lleve a una entrega fraudulenta, acabando la información en manos de quien no debe.
Alteración de secuencia	Alteración del orden de los mensajes transmitidos. Con ánimo de que el nuevo orden altere el significado del conjunto de mensajes, perjudicando a la integridad de los datos afectados.
Acceso no autorizado	El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.
Análisis de trafico	El atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios. A veces se denomina “monitorización de tráfico”.
Repudio	Negación a posteriori de actuaciones o compromisos adquiridos en el pasado. Repudio de origen: negación de ser el remitente u origen de un mensaje o comunicación. Repudio de recepción: negación de haber recibido un mensaje o comunicación. Repudio de entrega: negación de haber recibido un mensaje para su entrega a otro.
Interceptación de información (escucha)	El atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada.
Modificación deliberada de la información	Alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.
Destrucción de información	Eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.
Divulgación de información	Revelación de información.
Manipulación de programas	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.
Manipulación de los equipos	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.
Denegación del servicio	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
Robo	La sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. El

AMENAZAS	***DESCRIPCIÓN***
	robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información los más habituales. El robo puede realizarlo personal interno, personas ajenas a la organización o personas contratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.
Ataque destructivo	Vandalismo, terrorismo, acción militar,... Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la organización o por personas contratadas de forma temporal.
Ocupación enemiga	Cuando los locales han sido invadidos y se carece de control sobre los propios medios de trabajo.
Indisponibilidad del personal	Ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos,...
Extorsión	Presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido.
Ingeniería social (picaresca)	Abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.

Tabla 9. Lista de referencia - Catálogo de elementos de riesgo MAGERIT
(Fuente: Administración Electrónica PAe, 2012)

7.2. Anexo 2. Riesgos y amenazas en *cloud computing* según CSA

AMENAZA	***DESCRIPCIÓN***
Abuso y mal uso del Cloud Computing	Esta amenaza afecta principalmente a los modelos de servicio *IaaS* y *PaaS* y se relaciona con un registro de acceso a estas infraestructuras/plataformas poco restrictivo. Es decir, cualquiera con una tarjeta de crédito válida puede acceder al servicio, con la consecuente proliferación de *spammers*, creadores de código malicioso y otros criminales que utilizan la nube como centro de operaciones.
Interfaces API poco seguros	Generalmente los proveedores de servicios en la nube ofrecen una serie de interfaces y API (del inglés, *Application Programming Interface*) para controlar e interactuar con los recursos. De este modo, toda la organización, el control, la provisión y la monitorización de los servicios *cloud* se realiza a través de estos API o interfaces. Dado que todo (autenticación, acceso, cifrado de datos, etc.) se realiza a través de estas herramientas, se hace necesario que las interfaces estén diseñadas de forma segura, evitando así los problemas de seguridad, tanto los que son intencionados como los que se producen de forma accidental.
Amenaza interna	Como en todos los sistemas de información, la amenaza que suponen los propios usuarios es una de las más importantes, dado que tienen acceso de forma natural a los datos y aplicaciones de la empresa. En un entorno *cloud* esto no es en absoluto diferente ya que se pueden desencadenar igualmente incidentes de seguridad provocados por empleados descontentos y accidentes por error o desconocimiento. Además, en muchos casos, es el propio proveedor del servicio es el que gestiona las altas y bajas de los usuarios, produciéndose brechas de seguridad cuando el consumidor del servicio no informa al proveedor de las bajas de personal en la empresa. Como es lógico, estos incidentes repercuten de forma importante en la imagen de la empresa y en los activos que son gestionados. Los proveedores de servicio deberán proveer a los consumidores del servicio de medios y métodos para el control de las amenazas internas.
Problemas derivados de las tecnologías compartidas	Esta amenaza afecta a los modelos *IaaS*, ya que en un modelo de Infraestructura como Servicio los componentes físicos (CPU, GPU, etc.) no fueron diseñados específicamente para una arquitectura de aplicaciones compartidas. Se han dado casos en los que los hipervisores de virtualización podían acceder a los recursos físicos del anfitrión provocando, de esta forma, incidentes de seguridad. Para evitar este tipo de incidentes se recomienda implementar una defensa en profundidad con especial atención a los recursos de computación, almacenamiento y red. Además, se ha de generar una buena estrategia de seguridad que gestione correctamente los recursos para que las actividades de un usuario no puedan interferir en las del resto.
Pérdida o fuga de información	Existen muchas formas en las que los datos se pueden ver comprometidos. Por ejemplo, el borrado o modificación de datos sin tener una copia de seguridad de los originales, supone una pérdida de datos. En la nube, aumenta el riesgo de que los datos se vean comprometidos ya que el número de interacciones entre ellos se multiplica debido a la propia arquitectura de la misma. Esto deriva en pérdida de imagen de la compañía, daños

AMENAZA	***DESCRIPCIÓN***
	económicos y, si se trata de fugas, problemas legales, infracciones de normas, etc.
Secuestro de sesión o servicio	En un entorno en la nube, si un atacante obtiene las credenciales de un usuario del entorno puede acceder a actividades y transacciones, manipular datos, devolver información falsificada o redirigir a los clientes a sitios maliciosos.
Riesgos por desconocimiento	Uno de los pilares de las infraestructuras *cloud* es reducir la cantidad de software y hardware que tienen que adquirir y mantener las compañías, para así poder centrarse en el negocio. Esto, si bien repercute en ahorros de costes tanto económicos como operacionales, no puede ser motivo para el deterioro de la seguridad por falta de conocimiento de esta infraestructura. Para asistir en la toma de decisiones sobre las medidas de seguridad que se han de implantar en un entorno *cloud* es conveniente conocer, al menos en parte, la información técnica de la plataforma. Datos como con quién se comparte la infraestructura o los intentos de acceso no autorizados pueden resultar muy importantes a la hora de decidir la estrategia de seguridad. La carencia de información de este tipo puede derivar en brechas de seguridad desconocidas por el afectado.

Tabla 10. Lista de referencia - Riesgos y Amenazas en *cloud computing* según CSA
(Fuente: Instituto Nacional de Tecnologías de la Comunicación, 2011)

7.3. Anexo 3. Riesgos y amenazas en *cloud computing según Gardner*

AMENAZA	***DESCRIPCIÓN***
Accesos de usuarios con privilegios	El procesamiento o tratamiento de datos sensibles fuera de las instalaciones de la empresa conlleva un riesgo inherente, ya que es posible que estos servicios externos sorteen los controles físicos, lógicos y humanos siendo, por este motivo, necesario conocer quién maneja dichos datos.
Cumplimiento normativo	Los clientes son en última instancia responsables de la seguridad e integridad de sus datos, aunque estos se encuentren fuera de las instalaciones y gestionados por un proveedor de servicios *cloud*.
Localización de datos	Al utilizar entornos en la nube no se conoce de forma exacta en qué país están alojados.
Aislamiento de datos	Los datos en los entornos *cloud* comparten infraestructura con datos de otros clientes. El proveedor debe garantizar el aislamiento de los datos de los respectivos clientes. El cifrado de los datos es una buena práctica, pero el problema es cómo aislar los datos cuando se encuentran en reposo ya que el cifrado, cuando no se hace uso de los datos, puede resultar una operación costosa.
Recuperación	Los proveedores de servicio deben tener una política de recuperación de datos en caso de desastre. Asimismo, es muy recomendable que los datos sean replicados en múltiples infraestructuras para evitar que sean vulnerables a un fallo general.
Soporte investigativo	La investigación de actividades ilegales en entornos *cloud* puede ser una actividad casi imposible, porque los datos y *logs* (registros de actividad) de múltiples clientes pueden estar juntos e incluso desperdigados por una gran cantidad de equipos y centros de datos.
Viabilidad a largo plazo	En un entorno ideal un proveedor de servicios *cloud* siempre permanecerá en el mercado dando un servicio de calidad y con una disponibilidad completa, pero el mercado es cambiante y cabe la posibilidad de que el proveedor sea comprado o absorbido por alguno con mayores recursos.

Tabla 11. Lista de referencia - Riesgos y amenazas en *cloud computing* según Gardner
(Fuente: Instituto Nacional de Tecnologías de la Comunicación, 2011)

7.4. Anexo 4. Recomendaciones de seguridad según NIST

ÁREA	***RECOMENDACIONES***
Gobernanza	Implantar políticas y estándares en la provisión de servicios. Establecer mecanismos de auditoría y herramientas para que se sigan las políticas de la organización durante el ciclo de vida.
Cumplimiento	Entender los distintos tipos de leyes y regulaciones y su impacto potencial en los entornos *cloud.* Revisar y valorar las medidas del proveedor con respecto a las necesidades de la organización.
Confianza	Incorporar mecanismos en el contrato que permitan controlar los procesos y controles de privacidad empleados por el proveedor.
Arquitectura	Comprender las tecnologías que sustentan la infraestructura del proveedor para comprender las implicaciones de privacidad y Riesgos y amenazas en *Cloud Computing,* seguridad de los controles técnicos.
Identidad y acceso	Asegurar las salvaguardas necesarias para hacer seguras la autenticación, la autorización y las funciones de control de acceso.
Aislamiento de software	Entender la virtualización y otras técnicas de aislamiento que el proveedor emplee y valorar los riesgos implicados.
Disponibilidad	Asegurarse que durante una interrupción prolongada del servicio, las operaciones críticas se pueden reanudar inmediatamente y todo el resto de operaciones, en un tiempo prudente.
Respuesta a incidentes	Entender y negociar los contratos de los proveedores así como los procedimientos para la respuesta a incidentes requeridos por la organización.

Tabla 12. Lista de referencia - Recomendaciones de seguridad según NIST
(Fuente: Instituto Nacional de Tecnologías de la Comunicación, 2011)

7.5. Anexo 5. Riesgos de preservación digital

RIESGOS	***DESCRIPCIÓN***
Fallo de medios	Debe tenerse en cuenta que los medios de almacenamiento pueden degradarse con el paso del tiempo, causando errores de *bit* irrecuperables y con ello pérdida repentina y masiva de datos, como fallos en el disco o pérdida de medios fuera de línea u *off line*.
Fallo de hardware	Hay que tener en cuenta que los componentes del hardware pueden sufrir fallos transitorios que pueden ser recuperables, como la pérdida de potencia, así como fallas catastróficas irrecuperables tales como fuentes de alimentación quemadas.
Fallo de software	Los componentes de software pueden presentar errores como "*bugs*" que representan riesgos para los datos almacenados.
Errores de comunicación	Fallos en las trasferencias de redes, para la ingesta o difusión de contenidos. Estas transferencias pueden tener éxito o pueden fracasar en un periodo de tiempo determinado, afectando la entrega del contenido inalterado.
Errores de los servicios de red	Los sistemas deben anticiparse a los errores que pueden presentarse en los servicios de red externos; estos errores pueden ser tanto transitorios como no recuperables. Por ejemplo, los nombres de dominio pueden desaparecer o ser reasignados.
Obsolescencia de medios y del hardware	Todos los medios de almacenamiento y los componentes de hardware, finalmente, producirán un error ya que pueden llegar a ser obsoletos y no tener la capacidad de comunicarse con otros componentes del sistema. El problema es particularmente grave para los medios extraíbles.
La obsolescencia de software	De mismo modo los componentes del software pueden quedar obsoletos. En este caso, aunque algunos datos pueden seguir siendo accesibles, la información no puede ser descodificada desde el formato de almacenamiento de una forma legible.
Error del operador	Se debe contar con las acciones del operador para incluir errores recuperables y no recuperables. Aplica no solo para la preservación digital si no para el sistema operativo en el que se está ejecutando, otras aplicaciones que comparten el mismo entorno, el hardware y subyacente y la red a través de la cual se comunican.
Desastres naturales	Tales como inundaciones, incendios, y terremotos deben ser anticipados. Cuando se presentan, se manifiestan otro tipo de riesgos como fallas de comunicación, de hardware y de infraestructura.
Ataque externo	Así como los archivos en papel pueden estar sujetos a ataques maliciosos, sus equivalentes digitales no están exentos de ello. Es peor porque todos los sistemas conectados a las redes públicas son vulnerables a virus y gusanos. Los sistemas de preservación deben defenderse contra los ataques inevitables o estar completamente aislados de redes externas.

RIESGOS	***DESCRIPCIÓN***
Ataque interno	Se debe anticipar el mal uso de la información privilegiada; esto implica la aplicación de instrumentos para la autorización de acceso al sistema. Incluso si un sistema de preservación digital está completamente aislado de las redes externas, debe anticiparse el mal uso de información privilegiada
El fracaso económico	La información gestionada en formatos digitales es más vulnerable a interrupciones en el suministro presupuestal. Los presupuestos pueden ser variables y se debe anticipar que se contará con ellos a través de la generación de modelos de financiamiento de los sistemas de preservación a largo plazo.
Fallas organizacionales	La visión del sistema de preservación debe incluir no solo los aspectos tecnológicos, sino que debe incluir la organización a la que pertenece. Una organización puede dejar de existir, quizás por efecto de la quiebra, o sus objetivos misionales pueden cambiar. Esto puede privar al sistema de preservación digital de la ayuda necesaria para sobrevivir. Entonces, la planificación del sistema debe prever la posibilidad de que los activos de información preservados, sean transferidos a una organización sucesora o que sean realizadas las acciones más apropiadas.

Tabla 13. Lista de referencia - Riesgos de preservación digital
(Fuente: Rosenthal, Robertson, Lipkis, Reich, & Morebito, 2005)