Evaluación con el Esquema Nacional de Seguridad (ENS): la aplicación en el repositorio institucional de la UAB

Miquel Térmens
termens@ub.edu. Universitat de Barcelona. Departament de Biblioteconomia i Documentació
Núria Casaldàliga
Nuria.Casaldaliga@uab.cat. Universitat Autònoma de Barcelona. Servei de Biblioteques
Cristina Azorín
Cristina.Azorin@uab.cat. Universitat Autònoma de Barcelona. Servei de Biblioteques

Resumen: Esta comunicación se propone evaluar la adecuación de las auditorías del Esquema Nacional de Seguridad (ENS) en los repositorios institucionales. Este esquema de seguridad está previsto en el artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, y delimita los requisitos mínimos para una protección adecuada de la información con la finalidad de garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios digitales.

Para comprobar esta adecuación se ha partido de un caso práctico, la evaluación de la seguridad de un repositorio universitario de acceso abierto. En concreto el Depósito Digital de Documentos de la Universidad Autónoma de Barcelona (DDD), http://ddd.uab.cat

Palabras clave: evaluación; seguridad; auditoría; administración electrónica; Esquema Nacional de Seguridad; repositorios institucionales; Dipòsit Digital de Documents de la UAB

1. Antecedentes

El Esquema Nacional de Seguridad (ENS) es un sistema de gestión de la seguridad previsto en el artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. La misión del ENS es asegurar los requisitos mínimos de protección que permitan la correcta disponibilidad y funcionamiento de los sistemas informáticos que sostienen los servicios de administración electrónica de cualquier administración pública española. Estos requisitos de seguridad se basan en la segregación de las funciones en tres ámbitos: legal (normativa interna, cumplimiento de disposiciones legales…), organizativo (segregación de responsabilidades, formación del personal, establecimiento de controles…) e informático (medidas tecnológicas), de manera que la seguridad integral solo se puede alcanzar mediante la aplicación de medidas en cada uno de los tres ámbitos. El ENS marca cuáles han de ser estas medidas y reglamenta como comprobar su correcta aplicación mediante un sistema de auditoría.

El ENS es de aplicación a cualquier administración pública española, incluidas las universidades. En cambio su aplicabilidad a los servicios bibliotecarios universitarios no es una cuestión cerrada y aún es tema de debate técnico, pues en general se considera que el ENS no es de aplicación dado que no prestan servicios de administración electrónica y apoyo del procedimiento administrativo general. Con independencia de esta discusión, está claro que el sistema de aseguramiento de la calidad que propone el ENS puede ser de gran utilidad a las bibliotecas para mejorar la seguridad de los servicios que prestan. El presente trabajo pretende contribuir al debate estudiando la aplicabilidad de las auditorías ENS como metodología de autoevaluación de la seguridad de los repositorios institucionales de las universidades españolas. Este objetivo se ha desarrollado a partir de un estudio de caso: el uso del ENS como metodología para analizar la seguridad del repositorio DDD de la UAB.

El Depósito Digital de Documentos de la Universidad Autónoma de Barcelona (DDD), http://ddd.uab.cat, nació en noviembre de 2006 con el objetivo de recoger y difundir la producción científica de la universidad, así como facilitar el acceso y mejorar la visibilidad del fondo patrimonial y colecciones especiales de las bibliotecas.

Después de seis años en funcionamiento y con un personal, una normativa y unas políticas estables sus responsables del Servicio de Bibliotecas han considerado que es un buen momento para centrarse en los procesos de calidad y en emprender acciones de mejora a largo plazo. En esta comunicación se presenta una primera fase del proceso de evaluación centrada en el ámbito de la seguridad informática del repositorio, con la voluntad de trabajar en el futuro la evaluación de la calidad y la preservación de los contenidos. A continuación se presentan los principales resultados de interés general de esta evaluación, sin entrar en los resultados pormenorizados, que tienen un carácter reservado.

2. Metodología

Para realizar el análisis de la seguridad del repositorio de la UAB se ha utilizado la metodología de auditoría reglamentada en el Esquema Nacional de Seguridad (ENS), prevista en el artículo 42 de la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, y específicamente dentro de los requisitos del Artículo 34 (Auditoría de la Seguridad) y del Anexo III (Auditoría de la Seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

La evaluación ENS, realizada en octubre de 2012, fue administrada bajo la forma de entrevistas al personal implicado en la gestión del repositorio realizadas por un equipo evaluador independiente externo; el objetivo no ha sido obtener una certificación acreditada. Dado el carácter no acreditativo de la evaluación, no se requirió la comprobación documental exhaustiva de las afirmaciones realizadas por los responsables del repositorio, dándose por buenas las explicaciones orales.

El análisis de riesgos se realizó con la herramienta PILAR, versión 5.2.3, que implementa la metodología de análisis de riesgos MAGERIT, versión 3, de la Dirección General de

Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, del Ministerio de Hacienda y Administraciones Públicas.

También se tuvieron en cuenta las Guías de Seguridad CCN-STIC, en especial:

- 802. Esquema Nacional de Seguridad. Guía de auditoría. Junio 2010
- 803. Esquema Nacional de Seguridad. Valoración de los sistemas. Enero 2011
- 804. Esquema Nacional de Seguridad. Guía de implantación (borrador). Octubre 2011
- 808. Verificación del cumplimiento de las medidas en el ENS. Septiembre 2011

A efectos de la evaluación, el DDD fue clasificado a priori como sistema de información de categoría BASICA (Apartados 3, 4 y 5 del Anexo I del Real Decreto 3/2010), con unos requerimientos de seguridad bajos, dado que un fallo de seguridad del sistema no puede comprometer derechos o servicios fundamentales de los ciudadanos. La valoración del DDD se hizo según las cinco dimensiones de la seguridad: disponibilidad, integridad de los datos, confidencialidad de los datos, autenticidad de los usuarios y de la información, y trazabilidad del servicio y de los datos.

En el informe de evaluación no se contemplaron los apartados que, todo y ser de la categoría BASICA, no eran aplicables a este repositorio, por ejemplo, la protección de equipos portátiles o la gestión de la información clasificada. En cambio, se añadió un conjunto de medidas de seguridad de grado superior, MEDIA, las relacionadas con las copias de seguridad (*backup*), ya que se consideró que son una herramienta clave en la garantía de seguridad, tanto de los contenidos como de los metadatos.

3. Resultados

Los resultados obtenidos se analizaron respecto a los dos objetivos iniciales:

a) Evaluar la utilización de las auditorías ENS como metodología de autoevaluación de la seguridad de los repositorios institucionales.

ENS es una metodología muy ligada al modelo PDCA (Plan-Do-Check-Act) también aplicado, entre otros ámbitos, a la gestión de la calidad (ISO 9001:2008) y a los sistemas de gestión de la seguridad de la información (ISO 27001:2005). Como ya es bien conocido, una de las principales críticas que recibe este modelo es su carácter excesivamente procedimental, reglamentista, pues espera que todo el conocimiento y actuaciones sigan las indicaciones y estén sustentados en documentación escrita. En las bibliotecas universitarias, los procedimientos de seguridad no siempre están documentados de manera específica, o bien se ejecutan de forma intuitiva y/o se aplican las medidas de seguridad generales que la universidad tenga establecidas. Por esta razón, una evaluación ENS tiende a destacar esta falta de documentación de los procedimientos como un apartado mejorable, aunque su ausencia no signifique necesariamente que exista una falta de seguridad.

Se comprobó que resulta difícil delimitar cuál es la infraestructura (incluido el personal) que está directamente implicada en un repositorio institucional. Estos problemas de delimitación

se localizan tanto respecto a la infraestructura informática general de la institución (la universidad en nuestro caso de estudio), como respecto a los otros servicios que componen la biblioteca digital y que en buena parte son administrados por la biblioteca. Estos problemas de delimitación dificultan la identificación de las amenazas de seguridad y de las medidas de seguridad que ya han sido aplicadas. Por ello la revisión del nivel de seguridad de un repositorio institucional no se puede realizar de forma independiente de la seguridad aplicada al conjunto de la institución; en este punto es esencial contar con la estrecha colaboración del responsable de seguridad de la institución.

Tal como señalan los distintos sistemas de gestión de la información, es necesario que se asignen de forma clara los roles de responsable del servicio, de responsable de los datos y de responsable de la seguridad. De esta forma se consigue, entre otras mejoras, clarificar las responsabilidades entre distintas unidades de una misma organización y que la seguridad ya no se vea como una función específica del personal informático si no como un objetivo común de todas las partes implicadas en la gestión.

Se comprobó que la metodología ENS es adecuada como sistema de auditoría de las administraciones públicas, pero que en cada caso debe ser adaptada para que cumpla de forma correcta con sus objetivos. En este sentido es importante que se detallen qué elementos de análisis pueden ser declarados como "no aplicables" y, por el contrario, que otros elementos de nivel superior deben incorporarse a la auditoría de un sistema concreto.

b) Analizar la seguridad del repositorio DDD de la UAB.

La evaluación concluyó que el repositorio DDD disponía de medidas adecuadas de seguridad acordes con su categoría, aunque presentaba deficiencias en la implementación del marco organizativo de la política de seguridad. Así mismo, identificó que los esfuerzos de mejora se deberían centrar en primer lugar en el establecimiento formal de los responsables del repositorio (el de la seguridad, el de los datos y el del servicio), en la redacción de los procedimientos específicos, si son necesarios, y en fomentar una mayor difusión de las medidas de seguridad entre el personal implicado en la gestión del repositorio.

4. Conclusiones

Las evaluaciones ENS, como todos los sistemas de evaluación formal, son procesos engorrosos pero que ofrecen una imagen muy precisa de la realidad de un sistema. Para conseguirlo es esencial que las personas implicadas los asuman como un instrumento positivo de mejora y no como una medida de fiscalización que es vista con aprehensión. Estos beneficios se pueden dar incluso cuando las evaluaciones se aplican a servicios que legalmente no están obligados a realizarlas, como es el caso de los servicios que sustentan los repositorios de las universidades. Son un instrumento de planificación de los objetivos y las tareas a corto y medio plazo.

Los sistemas de acceso abierto en el ámbito español se han creado y consolidado en la última década y en estos momentos de crisis son uno de los pocos sectores en crecimiento. Si los repositorios institucionales en abierto quieren garantizar la evaluación de calidad una de las

líneas a seguir es la revisión periódica de los procedimientos que hacen referencia a los aspectos críticos de seguridad.

5. Agradecimientos

Agradecemos la participación del personal responsable del Servicio de Bibliotecas y del Servicio de Informática de la UAB, así como el apoyo recibido de las respectivas direcciones para realizar la evaluación.

Esta evaluación ha contado con la ayuda del proyecto *El acceso abierto (open access) a la ciencia en España: análisis del grado de implantación y de la sostenibilidad de un nuevo modelo de comunicación científica*. 2012-2014. Plan Nacional I+D+i, código CSO2011-29503-C02-01.

6. Bibliografía

Azorín, Cristina; [et al]: *Els repositoris institucionals: entre la gestió i l'avaluació*. *12 Jornades Catalanes d'Informació i Documentació* (Barcelona, 19-20 de mayo 2010). Acceso: http://ddd.uab.cat/record/56939 [Consultado el 7 de diciembre de 2012].

Ariño, Lluís: "Esquema Nacional de Seguridad". *Jornada sobre els esquemes nacionals d'interoperabilitat i de seguretat* (Girona, 26 mayo 2010). Universitat de Girona, ACUP, CESCA. Acceso: http://dugi-doc.udg.edu/handle/10256/2821 [Consultado el 7 de diciembre de 2012].

International Standards Office: *ISO 16363:2012. Space data and information transfer systems - Audit and certification of trustworthy digital repositories*. Geneva: ISO, 2012.

Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (BOE 23-6-2007).

Porter, B.; Simon, J.; Hatherly, D.: *Principles of External Auditing*. New York: John Wiley & Sons, 2003.

Quisbert, H.: "Evaluation of a Digital Repository". *Archiving 2008 Conference: Final Program and Proceedings* (Berna, Suiza, 24-27 Junio 2008). Springfield: Society for Imaging Science and Technology, 2008. P. 120-124.

Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica (BOE del 29 de enero).

Térmens, Miquel; [et al.]: "Proyecto de una metodología para la auditoría de los repositorios digitales institucionales". *IX Workshop Rebiun*. (Salamanca, 1-2 octubre 2009).