Las auditorías, una metodología para planificar la preservación digital. Experiencias en España

Miquel Térmens
Doctor en Documentación, Universidad de Barcelona. Profesor del Departamento de Biblioteconomía y Documentación. Universidad de Barcelona. España
E-mail: termens@ub.edu

Resumen

Se presentan los resultados obtenidos en la aplicación de diversas metodologías de auditoría para comprobar el estado de la preservación digital en distintas instituciones de España. Se concluye que las auditorías también se pueden usar como herramienta de ayuda a la planificación de sistemas de preservación digital.

Palabras clave

Preservación digital. Auditoría. Repositorios confiables. Seguridad informática. ISO 27000. ISO 16363

Audits, a digital preservation planning methodology. Experiences in Spain

Abstract

The article presents the results of the application of different audit methodologies to check the status of digital preservation in several institutions of Spain. We conclude that audits can also be used as a tool to help in planning digital preservation systems.

Keywords

Digital preservation. Audit. Trustworthy Repositories. Information Security. ISO 27000. ISO 16363.

INTRODUCCIÓN

La aplicación a nivel básico de las medidas que conforman la conservación tradicional (control de la humedad y la temperatura, control de agentes patógenos, sistemas antirrobo y antiincendios, etc.) es fácilmente comprensible incluso para personas no expertas. En cambio, las medidas que se aplican a la preservación digital (control de integridad, migración de formatos, registro de metadatos PREMIS, control de acceso, etc.) solamente pueden ser entendidas y verificadas por personal experto. Por otro lado, los sistemas de preservación digital son complejos y están formados por procedimientos, controles, tecnologías que pueden ser o no adecuadas para la función prevista, e incluso no estar funcionando correctamente en un momento concreto.

Los sistemas de auditoría informática llevan años aplicándose como procedimientos objetivos que permiten la comprobar el correcto funcionamiento de un sistema informático. Los actuales sistemas de auditoría parten de las recomendaciones de la norma británica BS 7799, después reconvertida en la familia de normas internacionales ISO 27000, auditables por un equipo externo. La limitación de estas metodologías se encuentra en que no contemplan los problemas específicos de los sistemas de preservación, como es la problemática tecnológica a largo plazo, la dificultad para asegurar el compromiso institucional o las dificultades de financiación. Por ello han aparecido nuevas metodologías de auditoría especializadas en el ámbito de la preservación digital, entre las que destacan: Drambora en el Reino Unido, Nestor 2 en Alemania y TRAC en los Estados Unidos, esta última reconocida como norma ISO/IEC 16363:2012.

EXPERIENCIAS DESARROLLADAS

Las grandes organizaciones ya han empezado a utilizar estos sistemas de auditoría con el fin de justificar sus actuaciones ante sus *skateholders* y poder demostrar que gestionan repositorios seguros y de confianza. En el caso de organizaciones medianas esta rendición de cuentas muchas veces no es lo más importante pues su sistema de preservación aún se encuentras en un estadio incipiente, si es que disponen del mismo. En este caso, las auditorías también tienen un importante papel: el de mecanismo para comprobar el nivel de preparación de la organización para afrontar esta tarea.

Con esta orientación hemos conducido diversas auditorías en España:

• 9 Instituciones hospitalarias de la región de Cataluña (España), para evaluar su capacidad para preservar sus archivos de historias clínicas electrónicas (BOTÉ; TÉRMENS, 2011).

• Instituto Cartográfico de Cataluña (Barcelona, España), para evaluar su capacidad para preservar los datos geográficos digitales (geodata) que produce (TÉRMENS; LOCHER, 2012).

• Repositorio institucional DDD de la Universidad Autónoma de Barcelona (UAB), para evaluar la seguridad de su gestión informática. El Dipòsit Digital de Documents (DDD) de la UAB es el primero de España y el 16º del mundo en el ranking de repositorios (fuente: Ranking web de repositorios, 2013. (http://repositories.webometrics.info/es) (TÉRMENS; CASALDÁLIGA; AZORÍN, 2013).

En estas auditorías se han usado diversos instrumentos: un sistema de auditoría de seguridad informática propio de la administración pública española –el Esquema Nacional de Seguridad (ENS) – y los sistemas de auditoría de preservación digital –Drambora y TDR ISO/IEC 16363:2012–. Se ha de advertir que estas auditorías, dado que su objetivo no era obtener ningún tipo de certificación, no fueron conducidas por auditores oficiales si no por personal experto en preservación. Aunque la experiencia aún no está cerrada y se está a la espera de realizar nuevas auditorías, ya se pueden extraer algunos resultados globales que presentamos a continuación.

A nivel metodológico. Se comprobó que es más fácil realizar auditorías sin valor de certificación pues así se rebaja la trascendencia de los resultados obtenidos y, como consecuencia, es posible conseguir la participación de todos los agentes implicados (gestores de la documentación, informáticos…), que en otro caso recibirían con un mayor recelo la realización de una auditoría oficial. En cualquier caso, el éxito de la auditoría depende de la colaboración de la dirección de la institución, del personal responsable de los datos y del personal informático, siendo imprescindible contar desde un inicio con la participación del responsable de seguridad de los sistemas de información. Por último se comprobó que para el personal informático es más fácil participar en aquellos procesos de auditoría que siguen metodologías que ya han aplicado con anterioridad, como son las auditorías de seguridad informática ISO 27001 o las relacionadas con el aseguramiento de los sistemas de administración electrónica.

A nivel de resultados. Se pudo comprobar que a menudo las organizaciones aplican soluciones que externamente se pueden considerar heterodoxas o parciales según las prácticas más comunes, pero que sin embargo dan los resultados deseados. Por ello el equipo auditor no debe limitarse a comprobar mecánicamente si se cumplen unos determinados requerimientos sino que debe escuchar atentamente las explicaciones dadas por los gestores del sistema y entender sus razonamientos. En el apartado organizativo es donde se detectan los mayores incumplimientos, concretados en la falta de planificación a medio plazo, en la aplicación de procedimientos no documentados y en una delimitación no suficientemente clara de las funciones entre los departamentos implicados.

A nivel de planificación. Las auditorías sirvieron a las organizaciones para tomar conciencia de su situación actual y para marcarse una hoja de ruta de las mejoras que deberían implementar para desarrollar un sistema de preservación eficaz. De forma más concreta les proporcionaron un listado ordenado de los puntos que aún no estaban cumpliendo y cuál es el papel que éstos desempeñan dentro del conjunto de acciones en favor de la preservación. En este sentido, se descubrieron las debilidades existentes en cuanto a disponer del necesario respaldo institucional, al aseguramiento de la financiación, a la organización de responsabilidades y la planificación a medio y largo plazo. En definitiva, las auditorías evidenciaron de forma más clara que el estricto cumplimiento de buenas prácticas de mantenimiento y seguridad de los medios informáticos no son suficientes para asegurar la preservación de los contenidos digitales.

CONCLUSIONES

Las auditorías realizadas han demostrado ser un instrumento eficaz y contrastable para comparar la situación de una institución determinada con los requerimientos de preservación que emanan del modelo OAIS y de las buenas prácticas en gestión informática. Así ha resultado fácil comprobar hasta qué punto unos procedimientos técnicos particulares pueden cumplir perfectamente con los requisitos de preservación digital.

AGRADECIMIENTOS

Investigación realizada dentro del proyecto *El acceso abierto (open access) a la ciencia en España*. 2012-2014. Plan Nacional I+D+i, código CSO2011-29503-C02-01.

REFERENCIAS

BOTÉ Vericad, Juan-José. *Propuesta de un modelo de preservación digital para pequeñas y medianas instituciones sanitarias*. Barcelona, Universitat de Barcelona, 2012. 353 p. Tesis doctoral. Disponible en: <http://hdl.handle.net/10803/96254> Consulta: 27 nov. 2013.

BOTÉ, J.; TÉRMENS, M. Trac y ENS en la Auditoría de Preservación Digital de los Archivos Sanitarios. In: CONGRESO NACIONAL DE INFORMÁTICA DE SALUD. Inforsalud, 14., 2011. Madrid: Sociedad Española de Informática de la Salut, 2011. p. 155-159. Disponible en: <http://bd.ub.edu/pub/termens/docs/inforsalud2011.pdf> Consulta: 27 nov. 2013.

TÉRMENS, M.; CASALDÀLIGA, N.; AZORÍN, C. Evaluación con el Esquema Nacional de Seguridad (ENS): la aplicación en el repositorio institucional de la UAB. In: JORNADAS ESPAÑOLAS DE DOCUMENTACIÓN, Fesabid 13., *2013*. Toledo, 2013. p. 176-179. Disponible en: <http://www.fesabid.org/toledo2013/actas-de-las-jornadas> Consulta: 27 nov. 2013.

TÉRMENS, M.; LOCHER, A. E. Digital preservation audit on spatial data: a practical experience. *SOMAP 2012:* service-oriented mapping. Wien, Jobstmedia, 2012. Disponible en: <http://bd.ub.edu/pub/termens/docs/SOMAP2012.pdf> Consulta: 27 nov. 2013.