La auditoría en los archivos

Audit of the archives

Vicent Giménez-Chornet
vigicho@har.upv.es
Universitat Politècnica de València

Resumen

La inspección de los archivos ha existido desde época antigua, especialmente porque las administraciones querían tener conocimiento de su correcto funcionamiento. En el siglo XXI, con la producción de los documentos electrónicos, se exige que la gestión de los documentos y del funcionamiento de los archivos sea confiable a la comunidad. Para garantizar la confiabilidad de los archivos es necesario que haya auditorías externas. En este artículo se proponen los principales aspectos que debe reunir una auditoría externa de los archivos para generar confianza a su comunidad.

Palabras clave

Auditoría; Inspección; Responsabilidad; Confianza; Gestión de documentos electrónicos

Abstract

The inspection of the archives has existed since ancient times, especially because the administrations wanted to be aware of their proper functioning. In the 21st century, with the production of electronic documents, the management of documents and the operation of the archives is required to be reliable to the community. External audits are necessary to ensure the reliability of the archives. This article proposes the main aspects that an external audit of the archives should gather in order to generate confidence in the community.

Keywords

Audit; Inspection; Accountability; Trust; Electronic document management

Recibido: 14/04/2020
Aceptado: 18/04/2020
DOI: https://dx.doi.org/10.5557/IIMEI11-N20-001030
Descripción propuesta: Giménez-Chornet, Vicent, 2020. La auditoría en los archivos. *Métodos de Información*, **11**(20), 1-30

1. Introducción

Con la irrupción de las Tecnologías de la Información y la Comunicación (TIC) de forma patente en los años ochenta, y de forma revolucionaría en el presente siglo, la archivística tradicional de gestionar los documentos ha dado un salto exponencial, y en la que técnicas antiguas persisten de alguna forma (identificación y descripción de los documentos para registrarlos, por regla general, en inventarios) y otras técnicas se han actualizado o generado de nuevo para afrontar los retos de los documentos electrónicos y la comunicación el línea.

Con el uso de los documentos electrónicos auténticos por empresas, o por administraciones públicas, en el actual contexto de gobierno electrónico, los archiveros deben asegurar que su servicio incorpora estos documentos a su sistema de gestión, de forma que los capture y administre para que sean accesibles, tanto en el presente como a largo plazo, de lo contrario no se cumplirá su objetivo, que es gestionar, mantener y preservar los documentos para cumplir su finalidad, la evidencia. Resolver los nuevos desafíos requiere de nuevos conocimientos especializados para tener éxito (Kallberg 2012). En el ciclo de vida de los documentos, la archivística actual da valor a la información contextual. Además, la recuperación de información basada en la procedencia, centrada en la función de los documentos, en el contexto de la creación, podría considerarse superior a los métodos de gestión basados en el sujeto y el contenido (Runardotter *et al.* 2006).

El buen mantenimiento de los documentos es también fundamental para la rendición de cuentas del gobierno en una sociedad democrática igual que, a nivel de las empresas, su gestión también es básica y esencial para las actividades de negocio. Con ello se proporciona la evidencia de lo que ha hecho una organización, cómo hace sus negocios y por qué llevó a cabo

ciertas acciones y tomó ciertas decisiones, y en algunos casos la buena gestión de los documentos llega a ser crítica, como en las áreas de salud, justicia, cobertura social a los más desprotegidos, etc. Para todo ello un estándar en gestión de los documentos puede ayudar a las organizaciones, en general, a implementar estrategias para conseguir el mantenimiento de unos registros completos y precisos, como se consiguió en Australia en su norma AS 4390, que ha sido reemplazada por la ISO 15489. Swan, K., Cunningham, A. y Robertson, A. (2002) han destacado algunos de los beneficios de la buena gestión: mayor eficiencia y efectividad en la actividad comercial porque hay más información relevante y oportuna disponible; mejor cumplimiento de los requisitos legales y reglamentarios, así como mayor satisfacción en las expectativas de la comunidad; mejor intercambio de conocimientos y retención y acceso a la memoria corporativa; mejor gestión de los riesgos relacionados con la evidencia; capacidad mejorada para explicar y proporcionar los testimonios de las acciones y decisiones de una organización; gestión adecuada de documentos conformes con sus requisitos de retención, y una disminución de los costes de almacenamiento, materiales y mano de obra.

2. Inicio de las inspecciones de archivos

No es lo mismo una auditoría que una autoevaluación. Una auditoría, que debe ser certificable, es un proceso realizado por un proveedor de servicio externo, que requiere de bastante tiempo y en el que se han de cumplir unos requisitos elevados, para servir como medio de demostrar a la comunidad externa que se está cumpliendo con unos estándares específicos o unos objetivos concretos. Mientras que un proceso de autoevaluación es un sistema de auditoría realizado por personal de dentro de la propia organización, que se ejecuta para que la alta dirección de esa organización conozca y evalúe sus resultados, y éstos no se suelen comunicar a la comunidad externa. Las autoevaluaciones permiten identificar carencias, prácticas escasamente desarrolladas, infraestructuras deficientes, etc., susceptibles de mejoras, y que se pueden resolver para, en una fecha posterior, realizar una auditoría y certificación más completa por un proveedor de servicios externo. En el entorno de la propia organización, y en las administraciones públicas, la autoevaluación se llevaba a cabo mediante visitas de inspección. En el entorno

bibliotecario, el Reglamento de la Biblioteca Nacional de 1857 fue el precursor en ordenar que bianualmente «tres personas de superior instrucción y categoría, delegadas por el Gobierno, practicarán una visita de inspección en la Biblioteca Nacional, para informar acerca de su estado» (Título XVII.3) (España 1857). De forma general, para los archivos, bibliotecas y museos, el Reglamento de 1871 especificaba qué aspectos del servicio había interés en inspeccionar:

«Art. 21 El Inspector observará especialmente al visitar cada establecimiento:

1. El modo de cumplirse las instrucciones respectivas para el arreglo y clasificación de libros, documentos y antigüedades.
2. La observancia de las disposiciones reglamentarias.
3. El celo y aptitud de los empleados facultativos.
4. El desempeño y moralidad de los dependientes.
5. Las necesidades relativas al personal y material del establecimiento.
6. La situación en el distrito en que se gire la visita de establecimientos cuyas condiciones hagan posible su incorporación al Ministerio de Fomento.
7. La existencia en el propio distrito de libros, documentos u objetos arqueológicos que puedan tener legal y apropiado destino en alguno de los establecimientos del ramo.» (España 1871)

El Decreto 2675/1973, de 11 de octubre, por el que se regulan las funciones de la Inspección General de Archivos y de la Inspección General de Bibliotecas, indica cuales eran las principales prioridades de las visitas de inspección: informar sobre la situación de los Archivos en todos sus aspectos y proponer las medidas oportunas para corregir las deficiencias e irregularidades de orden técnico que haya podido advertir en el ejercicio de su función inspectora; asesorar en los planes de mejora y ampliación de los servicios de Archivos, así como en la concesión de subvenciones que se otorguen, con cargo a sus créditos para este fin, y vigilar e informar sobre la aplicación de estas últimas; recoger los datos estadísticos de todos los archivos y servicios sobre los que ejerce su función inspectora; proponer al órgano competente, en cada caso, la apertura de expedientes por infracción de la legislación, y estimular la actuación de los funcionarios proponiendo la concesión de recompensas que premien su dedicación y competencia profesional (España, 1973).

Más recientemente, cuando se crea la estructura orgánica del primer Ministerio de Cultura español, en 1978, también se configura el órgano de Inspección General, dependiente de la Subdirección General del Ministerio, con una Sección de Inspección de Servicios, entre los que se encuentra «Documentación y Archivo» (España, 1978); así mismo, en distintas normas jurídicas vigentes en la actualidad se contempla la función de inspección en archivos, como por ejemplo en la Ley Foral 12/2007, de 4 de abril, de Archivos y Documentos de Navarra (en el art. 8.1.i) (Comunidad Foral de Navarra, 2007), y en prácticamente todas las leyes autonómicas sobre archivos; en el Real Decreto 1816/2009, de 27 de noviembre, por el que se aprueba el Reglamento de los Archivos Judiciales Militares, es el Auditor Presidente del Tribunal o el Juez Togado Militar quien está a cargo de la inspección y de que se lleven «al corriente los libros del archivo, efectuar las anotaciones correspondientes, formar los legajos debidamente numerados para su identificación y proceder a la custodia y conservación de los documentos» (art. 8.1) (España, 2009); y en los archivos históricos de la Unión Europea, regulados por el Reglamento (UE) 2015/496 del Consejo, de 17 de marzo de 2015, por el que se modifica el Reglamento (CEE, Euratom) n.º 354/83, en lo que respecta al depósito de los archivos históricos de las instituciones en el Instituto Universitario Europeo de Florencia, permite a cada institución depositante «llevar a cabo una inspección de los archivos» de aquellos fondos que ha entregado (Unión Europea, 2015).

3. La auditoría de los archivos en la era digital

Con la aparición, y generalización, del nuevo soporte digital se plantearon una serie de riesgos, especialmente en la década de los noventa, a consecuencia de estos había detractores del uso de las TIC, porque priorizaban en las características adversas del soporte electrónico, y había defensores por las particularidades ventajosas que traería la sociedad digital. Este debate favoreció un desarrollo en la investigación centrada en cómo detectar los riesgos y cómo afrontarlos, y de la que se produjo abundante bibliografía y estándares en las tres últimas décadas. En la actualidad ya disponemos de los conocimientos teóricos y de las soluciones técnicas para resolver o minimizar estos riesgos. Hemos resuelto riesgos técnicos, como la captura, indexación, autocategorización, formatos y conversión de documentos, gestión de contenidos, acceso, protección con gestión de usuarios y trazabilidad,

preservación para garantizar la disponibilidad a lo largo del tiempo, implementación de redes de archivos, interoperabilidad, la valoración documental (retención y disposición); también hemos dado respuesta a los riesgos de seguridad, con las normas de gestión de riesgos (de carácter informático) y con las normas de política de seguridad de riesgos, donde se establecen los requisitos, servicios y órganos responsables; además se han abordado otros tipos de riesgos que están íntimamente ligados con la gestión de la información, los riesgos legales que deben resolver la validez de los trámites con documentos electrónicos, los derechos inherentes a estos documentos digitales (propiedad intelectual, patentes y secretos industriales y comerciales), el ejercicio y regulación de la transparencia, la regulación de la sede electrónica, la regulación legal de los organismos y funciones en la valoración documental, la regulación de la interoperabilidad, de la reutilización, de las políticas de conservación a largo plazo, de la custodia o transferencias en la administración electrónica, de la rendición de cuentas o buena gobernanza, de la prestación de servicios (en los que se reglamenta sobre el catálogo de los servicios públicos, con los derechos y obligaciones de sus usuarios, estructura funcional, competencias, financiación y gestión), o de la publicación de una política de gestión de documentos electrónicos; igualmente se han abordado los riesgos económicos, ya que algunos proyectos de implementación de sistemas de gestión de documentos electrónicos se han suspendido o han fracasado por falta de financiación, y por último, se han tenido en cuenta los riesgos institucionales, ya que las organizaciones deben asegurar la sostenibilidad del proyecto a lo largo del tiempo, llevando a cabo una gestión del cambio para preparar adecuadamente a las personas, realizando programas de formación que potencie un desarrollo de capacidades del personal, programas de gestión de calidad, acciones de cultura corporativa (en la gestión y en la memoria corporativa), en la gestión de proyectos (donde es importante saber controlar los recursos, el tiempo y las tareas en unas etapas diferenciadas) o en las responsabilidades del equipo de dirección.

Un riesgo que aún no hemos resuelto satisfactoriamente es la falta de confianza en un sistema de gestión de documentos electrónicos implementado en los archivos, tanto por la alta dirección que los debe impulsar, como por los gestores o usuarios de este sistema en nuestra sociedad digital. Esta falta de confianza provoca que no se avance en la implementación técnica y organizacional de un sistema de gestión de documentos de archivo a la altura

de la demanda de la comunidad, cuyos usuarios son cada vez más nativos digitales y que no entienden la ralentización en la implementación de la gestión digital. Una de las respuestas contra esta desconfianza es ejercer auditorías que certifiquen el correcto funcionamiento de los archivos, de los repositorios digitales o los sistemas de gestión. El NARA (*National Archives and Records Administration*) potenció un estándar sobre Auditoría y Certificación de Repositorios Confiables (*Trustworthy Repositories Audit & Certification*, TRAC) que tenía como objetivo promover un método de auditoría independiente para certificar el estándar OAIS (un sistema de información de archivo abierto). El OAIS fue elaborado en 1996 por el *Consultative Committee for Space Data Systems*, que posteriormente pasó a ser la norma ISO 14721, como modelo que garantiza la eficiente gestión y preservación de los documentos digitales. Esto propició la elaboración de un catálogo de criterios para la evaluación de la confiabilidad de los archivos digitales, el *Trustworthy Repositories Audit & Certification: Criteria and Checklist* (TRAC) (Dale et al., 2007). Para Wilson (2017) el modelo OAIS ha funcionado como una guía para conceptualizar y desarrollar sistemas, para abordar las necesidades de preservación en un nivel abstracto y, en concreto, los modelos de referencia de gestión documental pueden ser útiles para representar los componentes funcionales requeridos en una clase de sistemas complejos diseñados para abordar necesidades compartidas a gran escala.

Por otra parte, la Unión Europea promueve una política similar con el *European Framework for Audit and Certification of Digital Repositories* (Marco Europeo para la Auditoría y Certificación de Repositorios Digitales), que concede unos sellos de calidad, a aquellos repositorios que han sido auditados por algunos instrumentos de auditoría, para certificar que son confiables. Un impulso europeo lo da el Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, conocido como Reglamento eIDAS. El primer considerando de este reglamento declara que «la creación de un clima de confianza en el entorno en línea es esencial para el desarrollo económico y social. La desconfianza, en particular debida a la inseguridad jurídica percibida, hace que los consumidores, las empresas y las administraciones públicas duden a la hora de realizar transacciones por vía electrónica y adoptar nuevos servicios». En relación con la interoperabilidad de datos entre las

administraciones, el considerando 20 indica que «la cooperación de los Estados miembros debe contribuir a la interoperabilidad técnica de los sistemas de identificación electrónica notificados con vistas a fomentar un nivel de confianza y seguridad elevados, adaptados al grado de riesgo. El intercambio de información y de las mejores prácticas entre los Estados miembros con miras a su reconocimiento mutuo debe facilitar dicha cooperación». En este reglamento se hace diferencia entre un servicio de confianza y un servicio de confianza cualificado. Para que reúna los requisitos de un servicio de confianza cualificado ha de existir una auditoría externa: «los prestadores cualificados de servicios de confianza serán auditados, al menos cada 24 meses, corriendo con los gastos que ello genere, por un organismo de evaluación de la conformidad. La finalidad de la auditoría será confirmar que tanto los prestadores cualificados de servicios de confianza como los servicios de confianza cualificados que prestan cumplen los requisitos establecidos en el presente Reglamento» (art. 20.1).

Actualmente existen diversos modelos de auditorías y certificación de repositorios digitales promovidos desde distintos ámbitos, entre los que destacamos:

- La ISO 16363: 2012 *Space data and information transfer systems — Audit and certification of trustworthy digital repositories*. Este estándar fue revisado y confirmado en 2017, existiendo una versión en español (AENOR 2017).
- El Sello de certificación de datos para repositorios (DSA). En 2018, junto con el Sistema de datos de Word (WDS) ICSU, se fusionó en CoreTrustSeal (Core Trust Seal 2020).
- El Sello Nestor, basado en la verificación según DIN 31644, *Criteria for trusted digital repositories*, de origen alemán, fue traducido al inglés como NESTOR (2009).

Figura 1. Número de repositorios certificados en el mundo (2017-2019).
Fuente: https://www.coretrustseal.org/why-certification/certified-repositories/ [Consulta: 25/03/2020]

Paralelamente, la norma ISO/IEC 17065 (ISO 2012), sobre la certificación de productos, procesos o servicios, con la finalidad de proporcionar confianza a las partes interesadas (como podrían ser los usuarios de los servicios o la propia administración pública o alta dirección de las organizaciones), es útil para analizar criterios de buenas prácticas en un plan de auditoría de archivos. En el contexto de la Unión Europea se elabora el estándar EN 9223-103: 2018, Gestión de programas. Gestión de configuración. Verificaciones de configuración, revisiones y auditorías (AENOR 2018a), cuya finalidad es asegurar la gestión de la configuración durante todo el ciclo de vida del producto, que radica en la consistencia y la homogeneidad de la información técnica entre todos los actores, y en la trazabilidad de esa información técnica. Esto se puede llevar a cabo mediante algunas acciones como la captura, conservación y puesta a disposición de esa información, o la verificación y validación de la coherencia de esa información en etapas definidas del ciclo de vida del producto (verificaciones, revisiones y auditorías de la configuración). En esta norma europea no se contempla que las auditorías de configuración sean realizadas, en ningún caso, por auditores de tercera parte (organismos acreditados para entregar certificados de auditoría sobre sistemas de calidad), sino por un auditor perteneciente a la empresa o, como mucho, por un auditor de segunda parte (el cliente). La norma ISO 19011:2018, Directrices para la auditoría de los sistemas de gestión (una actualización de la norma de 2012), sí que contempla la auditoría de tercera parte, como auditoría de certificación y/o acreditación (AENOR 2018b), pero más específicamente es la Norma ISO/IEC 17021-1 la que proporciona los requisitos para la

auditoría de sistemas de gestión para la certificación de tercera parte (AENOR 2015). Para la ISO 17021-1 «la certificación tiene por objetivo general proporcionar confianza a todas las partes de que un sistema de gestión cumple los requisitos especificados. El valor de la certificación reside en el grado de confianza y fe pública que se establece con una evaluación imparcial y competente por una tercera parte».

En base al marco jurídico y las normas de buenas prácticas realizamos una propuesta de los aspectos que consideramos esenciales para que en los archivos se lleven a cabo auditorías de tercera parte, o independientes de la organización, para garantizar la confiabilidad de la misma como entidad responsable de un sistema de gestión y custodia de los documentos producidos. En definitiva, la auditoría nos asegurará que hacen lo que dicen hacer, que lo que hacen es correcto, y esta podrá ayudar a la entidad a implementar buenas prácticas, así como a detectar carencias de alto riesgo.

3.1 Competencias y habilidades del auditor

Cabe señalar que «la calidad de la auditoría depende de la habilidad y competencia del auditor» (Mertzanis *et al.* 2019). Al fin y al cabo, el auditor tendrá una percepción de la realidad en el proceso de la auditoría, de la cual se hará una representación, y las distorsiones de esa realidad se producen durante las etapas adyacentes, como resultado de la subjetividad, la incompetencia técnica, la falta de confianza y las malas habilidades de presentación del cliente o del auditor (Comunale *et al.* 2003). Dos aspectos esenciales en la formación de una persona profesional competente son la adquisición de conocimientos y sus habilidades prácticas, por ello en la formación de un auditor es conveniente «lograr una mezcla de habilidades prácticas y conocimiento académico» (Hassall et al. 1996). Para Boiral *et al.* (2019) el desarrollo de la profesionalidad y la profesionalización implica la integración de un conjunto de conocimientos y habilidades personales para garantizar la correcta ejecución de actividades específicas.

El auditor de archivos debería tener las siguientes habilidades:

- **Pensamiento crítico:** como un proceso de toma de decisiones o juicio reflexivo para dar solución a problemas, en los que se requiere desarrollar el razonamiento (Peña Suárez *et al.* 2018).

- **Comprensión e integración.** En un entorno donde las organizaciones, con el uso de las TIC, trabajan en circunstancias de rápidos cambios, es importante comprender los sistemas complejos, que están altamente interrelacionados, en los que debe haber una rápida integración de la información (Zamora Enciso 2010:56).
- **Análisis y resolución de problemas**: capacidad de identificar los problemas y sus elementos más significativos para poderlos resolver de forma efectiva.
- **Planificación y gestión del tiempo**: capacidad de organizar y distribuir correctamente el tiempo disponible, mediante una planificación, que permita alcanzar los objetivos marcados. El éxito de esta habilidad influye en el liderazgo de quien la desarrolla (Fitsimmons 2008).
- **Comunicación efectiva**: capacidad de expresar ideas y transmitir conocimientos de forma convincente, adaptándose a las características de la audiencia. En este tipo de comunicación también tiene relevancia la empatía cognitiva, que consiste en comprender la posición de la otra persona desde un nivel objetivo, así como la empatía afectiva, que consiste en dar una respuesta emocional con la misma emoción de la otra persona (Delpechitre *et al.* 2019).
- **Habilidades tecnológicas**: amplio dominio en el uso de las herramientas y tecnologías necesarias para el ejercicio profesional. En nuestra sociedad actual el ritmo y la difusión del progreso tecnológico afecta a la aptitud de las habilidades laborales que se les exige a los profesionales, donde la tecnología repercute en la demanda de mano de obra altamente cualificada (Mertzanis *et al.* 2019).
- **Trabajo colaborativo**: capacidad para desarrollar un equipo en un clima de confianza para trabajar de forma responsable y colaborativa. La colaboración es importante en una sociedad cada vez más interdependiente. El trabajo en equipo se convierte en una parte central del trabajo en las organizaciones, deseando que los miembros de los grupos cooperen de manera efectiva, lo que puede redundar también en la proactividad con mejores resultados afectivos (Ghitulescu 2018).

3.2. Conocimientos específicos del auditor

Los conocimientos específicos en cuanto a técnicas y retos de la archivística en el entorno digital son esenciales para poder comprender el objeto auditable, y, sobre todo, también, para poder comunicarse con el personal archivero, desde la alta dirección hasta los técnicos. La carencia de ciertos conocimientos por los auditores redunda negativamente en la comunicación fluida, en el entendimiento de las partes, en la comprensión de los problemas, y en la identificación de los principales retos.

El auditor de archivos debería saber en:

- **Organización de archivos:** proceso intelectual consistente en analizar y disponer los documentos de acuerdo con los procedimientos archivísticos, en los que se identifica la estructura de un fondo, y se realizan tareas de clasificación y ordenación.
- **Normas técnicas de descripción e indización:** entre los estándares de descripción archivística cabe destacar la ISAD (G) (Norma Internacional General de Descripción Archivística), la ISAAR-CPF (Norma Internacional sobre los Registros de Autoridad de Archivos relativos a Instituciones, Personas y Familias), publicadas por el Consejo Internacional de Archivos, y la norma UNE ISO 25964-1 Información y documentación - Tesauros y su interoperabilidad con otros vocabularios - Parte 1: Tesauros para la recuperación de la información.
- **Administración de archivos**: conjunto de estrategias de la alta dirección para la aplicación de la política archivística a través de los programas establecidos, y para el control de los recursos (financieros, tecnológicos y humanos).
- **Marco jurídico**: normas jurídicas de obligado cumplimiento que regulan los sistemas archivísticos nacionales, los accesos a los documentos o los organismos responsables de la valoración documental, entre otros aspectos.
- **Riesgos y seguridad de la información**: conocer las normas de análisis de riesgos de la información y las normas de implementar sistemas de seguridad de la información, especialmente en los organismos que producen documentos electrónicos.

- **Mercado de la tecnología archivística**: cada vez más las empresas están desarrollando paquetes de software para la gestión de los documentos de archivos, con diferentes prestaciones y funcionalidades. El auditor debería conocer las principales funcionalidades de los softwares, así como los requisitos funcionales que debe cumplir la tecnología para implementar un sistema de gestión de documentos electrónicos.
- **Retos de los archivos en la era digital**: redes, administración electrónica, preservación, interoperabilidad, datos, etc. Irrumpe el concepto de curadoría digital relacionado con el profesional que analiza toda la información digital en bloque, ya sean datos, documentos, etc. (Yakel 2007)

3.3. Principios de quien audita

La norma ISO 17021 especifica los requisitos que deben reunir los organismos que auditan y certifican sistemas de gestión, como forma de asegurar que las organizaciones implementan un sistema que cumple con la política de dicha organización en los aspectos relacionados con sus actividades, productos y servicios. Para ello precisa algunos de los principios y requisitos que debe poseer el organismo auditor, entre los que destacamos:

- **Imparcialidad:** la objetividad de la auditoría requiere la ausencia de conflicto de intereses, independencia, carencia de prejuicios o actitud abierta, entre otros elementos. Es tan importante ser imparcial, como ser percibido como imparcial, para evitar las amenazas que surgen del conflicto de intereses personales o de la familiaridad con la persona u organismo auditado, que podría conllevar la ausencia de búsqueda de evidencias en la auditoría.
- **Responsabilidad legal:** el órgano auditor debe ser una entidad legal con funciones de auditoría. Más allá de la responsabilidad legal, el auditor se ve obligado a participar en juicios morales y seguir principios éticos, algunos relacionados con la protección de datos (La Torre *et al.* 2019). Es necesario evitar auditores alegales, sin responsabilidades de auditoría que, entre otras cuestiones, podrían conllevar que no se tramitasen las quejas de la auditoría.

- **Competencia:** el personal del organismo auditor debe certificar que posee los conocimientos pertinentes, de lo contrario esto puede acarrear una falta de entendimiento entre la empresa auditora y el organismo auditado; unas graves carencias en las tareas de la auditoría o unos informes de auditoría ininteligibles.
- **Transparencia:** el organismo auditor proporcionará acceso público al proceso y a los resultados de la auditoría (excepto en la información confidencial). La opacidad en una auditoría es totalmente adversa a la confianza, cuando lo que se persigue con la auditoría es, precisamente, certificar sistemas de gestión de documentos y organismo responsables confiables.
- **Confidencialidad:** el organismo auditor debe probar la confidencialidad (por su trayectoria y con la firma de un documento de confidencialidad) para tener acceso privilegiado a la información. La carencia de un compromiso documentado de confidencialidad puede inducir a dos tipos de riesgos: a la divulgación de información restringida o a la apropiación de información privilegiada para intereses particulares.
- **Receptividad (respuesta oportuna a las quejas):** el organismo auditor ha de tratar adecuadamente las opiniones y quejas para demostrar su integridad y credibilidad a la comunidad. Una ausencia en el tratamiento de las quejas podría acarrear acciones discriminatorias, además de que el mismo proceso de auditoría podría adolecer de errores.

3.4. Áreas auditables en los archivos

Diferentes aspectos inciden en que una organización genere confianza en su sistema de gestión de documentos, que puede abarcar tanto los fondos de soportes tradicionales como los soportes digitales. Más recientemente uno de los desafíos reside en generar confianza en los archivos depositados en un tercero, en la nube, donde es imprescindible garantizar unos servicios que protejan la autenticidad de los documentos y de los datos (Guo *et al.* 2016). Se debe tener en cuenta que los datos almacenados pueden ser inexactos, y se deben garantizar algunas medidas para su rectificación, además de garantizar

su seguridad y confiabilidad, contra un acceso o uso no autorizado (Ramón 2019).

A. Cuestiones técnicas. El auditor debe analizar especialmente evidencias que demuestren el adecuado desarrollo del trabajo técnico en los temas siguientes:

- **Clasificación multinivel:** configuración en el sistema de gestión documental de una clasificación multinivel que garantice la identificación de los fondos, subfondos, series, subseries y documentos (simples o compuestos), y que en dicha clasificación multinivel esté claramente comprensible el significado de cada nivel, especialmente si se incrementan niveles por necesidades del sistema.
- **Descripción normalizada:** contenido y productores. Es necesaria la adopción de un estándar internacional, tanto para la descripción del contenido como para la descripción de los productores. En el sistema de gestión documental ha de existir un enlace entre el productor y la unidad documental descrita.
- **Indización con lenguajes documentales**. Especialmente con el uso de tesauros. La construcción previa del tesauro, tanto para las materias como para los sitios geográficos o las entidades o instituciones, es imprescindible para que el trabajo técnico del análisis documental se desarrolle en su totalidad. El uso de lenguaje libre no se debe aplicar en un sistema de gestión de documentos, dado que obstaculiza la eficacia en la recuperación de la información.
- **Valoración documental:** retención, disposición, calendarios. Es un requisito esencial que se tiene que aplicar a los archivos administrativos, que producen tanto documentos en papel como electrónicos.
- **Software de gestión**. Este software ha de cumplir estándares en cuanto a requisitos de gestión de documentos electrónicos, como por ejemplo el estándar europeo MoReq (*Model Requirements for the Management of Electronic Documents and Records*)
- **Criterios de digitalización:** copia máster y de difusión. Para asegurarse de implementar buenas prácticas en un proyecto de digitalización es aconsejable seguir un estándar internacional, como la UNE-ISO/TR 13028:2011 IN, Información y documentación.

Directrices para la implementación de la digitalización de documentos (AENOR 2011).

- **Recuperación de la información.** De poco sirve realizar una gran labor técnica de descripción o indización, si después no hay implementado un buen sistema de recuperación de la información que garantice de forma óptima que las opciones de búsqueda por los usuarios dan una respuesta lo más exhaustiva posible de la información registrada en el sistema.
- **Transferencias.** En un sistema archivístico nacional el sistema tiene que garantizar tanto las transferencias de documentos en papel como de documentos electrónicos.
- **Redes de archivos**. No solamente es necesaria la creación de una red de archivos para el traspaso de la custodia de documentos, sino también para crear redes en línea de archivos que permitan la búsqueda en su catálogo y que den unos resultados relevantes con relación a la información solicitada. Gresham (*et al.* 2012) indica como muchos catálogos en línea pueden describirse como «grandes colecciones digitales», pero es probable que muchos usuarios se vean afectados por una mala funcionalidad de navegación. Los usuarios necesitan acceso a tecnologías Web 2.0 para navegar con éxito en los catálogos en línea y que éstas respalden su comportamiento de navegación.

B. Cuestiones de la entidad productora. El organismo productor y responsable de la custodia de los documentos debe demostrar evidencias en la auditoría que verifiquen el adecuado ejercicio en los siguientes asuntos:

- **Responsabilidades**: alta dirección, técnicos archiveros, etc. Una de las novedades de la ISO 15489 es la de recalcar la responsabilidad de la alta dirección en la gestión de los documentos. La alta gerencia y los técnicos archiveros deberían conocer los desarrollos tecnológicos, además la alta gerencia habrá de impulsar que la organización cumpla con los estándares y requisitos legales, y poder demostrar la transparencia en las operaciones y en la toma de decisiones (Joseph *et al.* 2012)

- **Políticas y directrices de la entidad archivística**. La existencia de políticas archivísticas sirve como una guía para facilitar las acciones y decisiones a tomar. Una entidad ha de marcar políticas de acción general y directrices concretas para la gestión de los documentos, que deben ser lo más completas, claras y fáciles de implementar (Tough *et al*. 2009).
- **Código ético.** Tanto los profesionales archiveros como las organizaciones deben señalar qué código ético usan (Giménez Chornet 2017a).
- **Responsabilidad social.** En el proceso de evaluación de la autoridad archivística se pueden investigar los valores secundarios que tengan en cuenta las necesidades sociales (Klett 2019), para que la toma de decisiones permita cohesionar la comunidad a la que pertenecen.
- **Plan de innovación.** La innovación y la mejora continua se basan en la capacidad de la entidad para ser creativa y aprender. Una estrategia de la innovación requiere estar estrechamente vinculada a la visión de la entidad (Martensen 1999). Se debe implantar un sistema de gestión de la innovación en los archivos que permita efectuar un seguimiento, una medición y un análisis del proceso innovador en las distintas actividades archivísticas y responsabilidades de la alta gerencia (Giménez Chornet 2010).

C. Cuestiones de seguridad:

- **Sistema de seguridad de la información**. Hay que garantizar con evidencias la implementación de un sistema de seguridad de la información, especialmente cuando los incidentes de seguridad en Internet incrementan la vulnerabilidad de las organizaciones. Para ello, los profesionales de la seguridad de la información deben implementar estándares que aborden la gestión de riesgos y contemplen un plan de contingencias (Areito 2008, 200-201).
- **Directrices de preservación/conservación de la información.** La preservación digital persigue la longevidad de los documentos digitales y su accesibilidad en todo momento, pero, además, nos encontramos con la información de los datos abiertos que se centran en la utilidad de éstos a través de servicios en línea, y su reutilización y distribución con

fines de transparencia y participación ciudadana (Adu 2016). Como buenas prácticas en un proyecto de preservación digital es recomendable el uso de la norma ISO 14641:2018(en) *Electronic document management - Design and operation of an information system for the preservation of electronic documents – Specifications*.

- **Plan de prevención de desastres**. La planificación de una gestión de desastres ayudará a preservar tanto los materiales históricos, que son esenciales para la comprensión y los valores de la comunidad, como la información digital, tan esencial para la supervivencia de los organismos y de los derechos de la comunidad. Uno de los peligros más comunes en los archivos son los incendios, intencionados o fortuitos, a los que hay que enfrentarse con planes previos (Vergara 2009: 13-23).
- **Infraestructura adecuada.** Tanto los recursos de hardware como de software son esenciales para la seguridad de la información, su actualización debe estar contemplada en un plan de seguridad de la información.
- **Accesos.** Una organización es necesario que se proteja contra todos aquellos intrusos que quieran acceder a sus recursos. Para Boyfriend (2011) es vital mantener a los intrusos y a los códigos maliciosos fuera de la red de una organización, porque una vez que están dentro, los intrusos pueden deambular libremente y tener los mismos, o incluso más, privilegios que los usuarios legítimos.
- **Trazabilidad.** Se ha demostrado que, en algunas certificaciones de gestión de calidad en sistemas de información, la trazabilidad es uno de los factores más importantes (Gunnlaugsdottir 2012).

D. Cuestiones legales:

- **Cumplimiento del marco jurídico en archivística.** En cada país existe una norma jurídica que regula aspectos esenciales de la archivística, como el sistema archivístico, el ciclo vital de los documentos, la accesibilidad, la transparencia, la interoperabilidad, la valoración documental, entre otros (Giménez Chornet 2017b), que los archivos están obligados a cumplir.
- **Protección de los derechos de autor y las patentes.** Un archivo puede custodiar documentación que requiera una especial protección

por derechos vinculados a la propiedad industrial o a la propiedad intelectual. Es necesario establecer unos requisitos de protección especiales para este tipo de documentación.

- **Transparencia.** Aunque la regulación de la transparencia afecta más a las administraciones públicas, en general, la información que custodian las organizaciones por sus actividades, como entidades científicas, empresas, organizaciones sin ánimo de lucro, etc., pueden ejercer también la transparencia a su comunidad para dar confiabilidad.
- **Reutilización de la información**. La reutilización de la información es uno de los objetivos de las administraciones públicas, promovidos en parte por directivas de la Unión Europea, que ha propiciado la creación de portales de acceso abierto (Simón *et al.* 2012).

E. Cuestiones económicas:

- **Financiación garantizada.** La ISO 17021 menciona que «el organismo de certificación debe evaluar sus finanzas y sus fuentes de ingresos, y debe demostrar que las presiones comerciales, financieras u otras no comprometen su imparcialidad» (AENOR 2015). Tanto en las administraciones públicas, mediante los presupuestos anuales, como en las empresas privadas se tienen que especificar las cantidades destinadas a la gestión de la información.
- **Auditoría** económica: minimizar riesgo financiero. Debe haber evidencias de que los organismos llevan a cabo auditorías económicas internas para constatar las posibles carencias que puedan poner en peligro la gestión de la información.
- **Sostenibilidad:** planificación a corto y largo plazo. Especialmente las entidades privadas deberían demostrar que el sistema de gestión de información es sostenible a lo largo del tiempo, y que dicha información será conservada incluso si desaparece la entidad, si la información en cuestión es de interés para la comunidad.

F. Recursos humanos:

- **Personal adecuado en formación y habilidades.** Las entidades y administraciones públicas deben mostrar evidencias de que el personal es el adecuado para la gestión de la información.
- **Carrera profesional.** Las entidades y las administraciones públicas documentarán los estímulos de promoción en la carrera profesional de los gestores de la información.
- **Formación continua.** Los avances tecnológicos y los conocimientos técnicos están en renovación continua, a un ritmo acelerado. Las entidades y administraciones públicas tendrán que facilitar el acceso a la formación continua de sus empleados.
- **Dedicación y remuneración**. Tanto la duración de la jornada laboral como la remuneración deben estar acordes con las tareas desarrolladas por los trabajadores. Una excesiva jornada laboral, o una remuneración no conforme a los requerimientos de conocimientos exigidos al trabajador, puede incumplir las normas jurídicas del país y producir perjuicio en el rendimiento del profesional.

G. Tercerización (outsourcing). La norma UNE-ISO 17068:2020 Información y documentación. Repositorio de tercero de confianza para documentos electrónicos (AENOR 2020), hace hincapié en las buenas prácticas para asegurar que los documentos electrónicos confiados a un organismo externo están garantizados mediante su sistema de gestión documental, avalando la integridad y validez de los documentos electrónicos, y que éstos puedan servir de evidencia efectiva a lo largo del tiempo. Para ello el auditor deberá inspeccionar las siguientes cuestiones:

- **Contratación:** derechos transferidos, responsabilidades y expectativas de las partes. Mediante documentos que evidencien los acuerdos contractuales entre las partes, en los que se constaten sus responsabilidades en la gestión de la información.
- **Garantías y solvencia.** Garantías en que su servicio de repositorio o custodia de documentos (también para los terceros que custodian documentos en soporte papel) reúne todos los requisitos técnicos y funcionales para alcanzar los objetivos definidos en su servicio, incluido el de solvencia económica.

- **Subcontratación:** costes y derechos (privacidad, etc.). Si el tercero subcontratase funciones propias, se mostrarán evidencias de la protección de la privacidad de la información y de la solvencia económica para ejercer dicha subcontratación.
- **Transparencia**. Ejercer acciones transparentes da confiabilidad a los organismos terceros contratados.
- **Valor económico de los servicios:** garantizar la competencia del mercado, cualitativa y cuantitativamente.
- **Evaluación de resultados.** Las empresas terceras prestadoras de servicios deben realizar evaluaciones internas que muestren la eficiencia de su gestión.

4. Conclusión

Los archivos han sido siempre inspeccionados con el fin de supervisar la gestión de los documentos y las adecuadas prácticas técnicas en relación con las exigencias de sus organismos superiores o de la sociedad a la cual deben su responsabilidad. La inspección de los archivos sirve para identificar las carencias que pueda haber y planificar su resolución.

Con la irrupción de los documentos electrónicos, así como de la información y los datos electrónicos, el gran reto que se plantea a los organismos productores es garantizar que hacen lo que ellos han decidido que deben hacer, según los requisitos y estándares internacionales y, sobre todo, dar confianza a la sociedad o a su comunidad de que hacen lo que deben hacer. Precisamente, la gran preocupación de una sociedad cada vez más exigente, y comunicada por las redes sociales, es resolver la duda razonable de si los gestores de la información hacen lo que deben hacer. Esta duda persistente puede provocar una desconfianza generalizada en la comunidad.

La auditoría externa en los archivos, realizada por profesionales con acreditados conocimientos, y abarcando diversos aspectos que incidan en el éxito de la buena gestión de la información, puede proporcionar la confianza en su comunidad y también puede ayudar, en gran medida, a identificar las carencias de los organismos auditados para emprender acciones de mejoras

que influirán en la autoconfianza de los propios productores de la información.

El auditor debe reunir unas competencias y unos conocimientos específicos para desarrollar su labor, sin ello no habrá garantías de una eficiente auditoría. El pensamiento crítico, el análisis y resolución de problemas, la comunicación efectiva o las habilidades tecnológicas son algunas de las competencias importantes que debe reunir el auditor, y por lo que respecta a los conocimientos específicos, debe conocer las principales tareas de la archivística para poderlas valorar en la auditoría, como por ejemplo la organización de archivos, la descripción multinivel, la administración de archivos, el mercado de la tecnología archivística y en general los retos de los archivos en la era digital. El dominio de la archivística permitirá que las distintas áreas auditables en los archivos se realicen con profesionalidad y que el resultado de la auditoría sea tan beneficioso para la propia organización, como confiable para la comunidad.

5. Bibliografía

ADU, K.; DUBE, L.; ADJEI, E., 2016. Digital preservation: The conduit through which open data, electronic government and the right to information are implemented. *Library Hi Tech*, **34**(4), 733-747. https://doi.org/10.1108/LHT-07-2016-0078

AENOR, 2011. *UNE-ISO/TR 13028:2011 IN. Información y documentación. Directrices para la implementación de la digitalización de documentos*. Disponible en: https://www.aenor.com/normas-y-libros/buscador-de-normas/une/?c=N0048666

AENOR, 2015. *UNE-EN ISO/IEC 17021-1:2015. Evaluación de la conformidad. Requisitos para los organismos que realizan la auditoría y la certificación de sistemas de gestión. Parte 1: Requisitos*. Disponible en: https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0055409

AENOR, 2017. *UNE-ISO 16363:2017, Sistemas de transferencia de información y datos espaciales. Auditoría y certificación de repositorios digitales de confianza*. Disponible en: https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0058850

AENOR, 2018a. *UNE-EN 9223-103:2018 (Ratificada). Gestión del programa. Gestión de la configuración. Parte 103: Verificación, revisión y auditoría de la configuración*. Disponible en: https://www.aenor.com/normas-y-libros/buscador-de-normas/une/?c=N0059847

AENOR, 2018b. *UNE-EN ISO 19011:2018. Directrices para la auditoría de los sistemas de gestión*. Disponible en: https://www.aenor.com/normas-y-libros/buscador-de-normas/une/?c=N0060855

AENOR, 2020. *UNE-ISO 17068:2020. Información y documentación. Repositorio de tercero de confianza para documentos electrónicos*. Disponible en: https://www.aenor.com/normas-y-libros/buscador-de-normas/UNE?c=N0063117

AREITO BERTOLÍN, J. 2008. *Seguridad de la información. Redes, informática y sistemas de información*. Madrid: Paraninfo.

BOIRAL, O.; HERAS-SAIZARBITORIA, I.; BROTHERTON, M., 2019. Professionalizing the assurance of sustainability reports: the auditors' perspective. *Accounting, Auditing & Accountability Journal*, **33**(2), 309-334. https://doi.org/10.1108/AAAJ-03-2019-3918

BOYFRIEND WILTON MLITWA, N.; BIRCH, D., 2011. The role of intrusion detection systems in electronic information security: From the activity theory perspective. *Journal of Engineering, Design and Technology*, **9**(3), pp. 296-312. https://doi.org/10.1108/17260531111179915

COMUNALE, C.; SEXTON, T.; GARA, S., 2003. The auditors' client inquiry process. *Managerial Auditing Journal*, **18**(2), 128-133. https://doi.org/10.1108/02686900310455119

COMUNIDAD FORAL DE NAVARRA, 2007. Ley Foral 12/2007, de 4 de abril, de Archivos y Documentos. *BOE*, núm. 113, de 11 de mayo de 2007, pp. 20394-20402. Disponible en: https://www.boe.es/eli/es-nc/lf/2007/04/04/12

CORE TRUST SEAL, 2020. *Data Seal of Approval Synopsis (2008–2018)*. Disponible en: https://www.coretrustseal.org/about/history/data-seal-of-approval-synopsis-2008-2018/

DALE, R. L.; AMBACHER, B., 2007. *Trustworthy Repositories Audit & Certification: Criteria and Checklist (TRAC)*. Chicago: CRL Center for Research Libraries. Disponible en: http://www.crl.edu/sites/default/files/attachments/pages/trac_0.pdf

DELPECHITRE, D.; RUTHERFORD, B.; COMER, L., 2019. The importance of customer's perception of salesperson's empathy in selling. *Journal of Business & Industrial Marketing*, **34**(2), 374-388. https://doi.org/10.1108/JBIM-03-2017-0073

ESPAÑA, 1857. Reglamento de la Biblioteca Nacional, decretado por S. M. en 7 de Enero de 1857. *Gaceta de Madrid*, núm. 1467, de 09/01/1857. Disponible en: https://www.boe.es/datos/pdfs/BOE//1857/1467/A00001-00002.pdf

ESPAÑA, 1871. Reglamento orgánico del cuerpo de Archiveros, Bibliotecarios y Anticuarios y establecimientos de él dependientes. *Gaceta de Madrid*, núm. 191, de 10/07/1871, pp. 109-111. Disponible en: https://www.boe.es/datos/pdfs/BOE//1871/191/A00109-00111.pdf

ESPAÑA, 1973. Decreto 2675/1973, de 11 de octubre, por el que se regulan las funciones de la Inspección General de Archivos y de la Inspección General de Bibliotecas. *BOE*, núm. 261, de 31 de octubre de 1973, pp. 21005-21006. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-1973-1493

ESPAÑA, 1978. Orden de 31 de enero de 1978 por la que se desarrollan los Reales Decretos 2258/1977, de 27 de agosto, y 132/1978, de 13 de enero, sobre estructura orgánica del Ministerio de Cultura. *BOE*, núm. 36, de 11 de febrero de 1978, pp. 3430-3437. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-1978-4182

ESPAÑA, 2009. Real Decreto 1816/2009, de 27 de noviembre, por el que se aprueba el Reglamento de los Archivos Judiciales Militares. *BOE*, núm. 13, de 15 de enero de 2010, pp. 3240-3249. Disponible en: https://www.boe.es/eli/es/rd/2009/11/27/1816

FITSIMMONS, G., 2008. Time management part I: goal setting as a planning tool. *The Bottom Line*, 21(2), 61-63. https://doi.org/10.1108/08880450810898328

GHITULESCU, B., 2018. Psychosocial effects of proactivity: The interplay between proactive and collaborative behavior. *Personnel Review*, **47**(2), 294-318. https://doi.org/10.1108/PR-08-2016-0209

GIMÉNEZ CHORNET, V., 2010. La innovación en los archivos. VIII Congreso de Archivología de Mercosur. Montevideo (Uruguay), 17-20 de noviembre de 2009. Publicado en *Revista de ANABAD*, LX, CD anexo, pp. 132-144.

GIMÉNEZ CHORNET, V., 2017a. Ethics and social responsibility in archival institutions: Elements to consider. *El profesional de la información*, **26**(4), 765-770. https://doi.org/10.3145/epi.2017.jul.20

GIMÉNEZ CHORNET, V., 2017b. *Legislación de archivos*. Barcelona: UOC.

GRESHAM, E.; HIGGINS, S., 2012. Improving browsability of archive catalogues using Web 2.0. *Library Review*, **61**(5), 309-326. https://doi.org/10.1108/00242531211280450

GUNNLAUGSDOTTIR, J., 2012. Information and records management: A precondition for a well functioning quality management system. *Records Management Journal*, 22(3), 170-185. https://doi.org/10.1108/09565691211283138

GUO, W.; FANG, Y.; PAN, W.; LI, D., 2016. Archives as a trusted third party in maintaining and preserving digital records in the cloud environment. *Records Management Journal*, **26**(2), 170-184. https://doi.org/10.1108/RMJ-07-2015-0028

HASSALL, T.; DUNLOP, A.; LEWIS, S., 1996. Internal audit education: exploring professional competence. *Managerial Auditing Journal*, **11**(5), 28-36. https://doi.org/10.1108/02686909610120514

ISO, 2012. *ISO/IEC 17065:2012(es). Conformity assessment — Requirements for bodies certifying products, processes and services*. Disponible en: https://www.iso.org/obp/ui#iso:std:iso-iec:17065:ed-1:v1:es

JOSEPH, P.; DEBOWSKI, S.; GOLDSCHMIDT, P., 2012. Paradigm shifts in recordkeeping responsibilities: implications for ISO 15489's implementation. *Records Management Journal*, 22(1), 57-75. https://doi.org/10.1108/09565691211222108

KALLBERG, M., 2012. Archivists 2.0: redefining the archivist's profession in the digital age. *Records Management Journal*, **22**(2), 98-115. https://doi.org/10.1108/09565691211268162

KLETT, E., 2019. Theory, regulation and practice in Swedish digital records appraisal. *Records Management Journal*, 29(1/2), 86-102. https://doi.org/10.1108/RMJ-09-2018-0027

LA TORRE, M.; BOTES, V.; DUMAY, J.; ODENDAAL, E., 2019. Protecting a new Achilles heel: the role of auditors within the practice of data protection. *Managerial Auditing Journal*, vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/MAJ-03-2018-1836

MARTENSEN, A.; DAHLGAARD, J., 1999. Strategy and planning for innovation management: a business excellence approach. *International Journal of Quality & Reliability Management*, 16(8), 734-755. https://doi.org/10.1108/02656719910283344

MERTZANIS, C.; BALNTAS, V.; PANTAZOPOULOS, T., 2019. Internal auditor perceptions of corporate governance in Greece after the crisis. *Qualitative Research in Accounting & Management*, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/QRAM-07-2018-0045

MERTZANIS, C.; SAID, M., 2019. Access to skilled labor, institutions and firm performance in developing countries. *International Journal of Manpower*, **40**(2), 328-355. https://doi.org/10.1108/IJM-11-2017-0301

NESTOR, 2009. *Catalogue of Criteria for Trusted Digital Repositories -Version 2-*. Frankfurt: Nestor Working Group Trusted Repositories. Disponible en: https://files.dnb.de/nestor/materialien/nestor_mat_08_eng.pdf

PEÑA SUÁREZ, D.; RAMOS SERPA, G.; LÓPEZ FALCON, A.; ARIAS RICARDO, Y., 2018. Desarrollo del aprendizaje en la educación superior a través del pensamiento eficaz: el caso de la carrera de Contabilidad y Auditoría en Uniandes, Puyo, Ecuador. *Ciencias Sociales y Educación*, **7**(14), 21-37. https://doi.org/10.22395/csye.v7n14a2

RAMÓN FERNÁNEZ, F., 2019. La normativa de protección de datos y derechos digitales en el ámbito de los recursos humanos: un reto para la sociedad y la legislación. *¿Se puede crear capital social?. Innovación y tecnología: retos para los recursos humanos de las organizaciones.*Valencia: Tirant Humanidades, pp. 203-227.

RUNARDOTTER, M.; QUISBERT; H.; NILSSON, J.; HÄGERFORS, A.; MIRIJAMDOTTER; A., 2006. The Information Life Cycle. Issues in Long-term Digital Preservation. *Arkiv, Samhälle Och Forskning*, 1: 17-29

SIMÓN, L. R. *et al.*, 2012. De la reutilización de la información del sector público a los portales de datos abiertos en Europa. *BiD: textos universitaris de biblioteconomia i documentació*, **29**(3). Disponible en: http://bid.ub.edu/29/pdf/ramos2.pdf

SWAN, K.; CUNNINGHAM, A.; ROBERTSON, A., 2002. Establishing a high standard for electronic records management within the Australian public sector. *Records Management Journal*, **12**(3), 79-86. https://doi.org/10.1108/09565690210454761

TOUGH, A.; ASMA' MOKHTAR, U.; MOHAMMAD YUSOF, Z., 2009. Electronic records management in the Malaysian public sector: the existence of policy. *Records Management Journal*, **19**(3), 231-244. https://doi.org/10.1108/09565690910999201

UNIÓN EUROPEA, 2014. Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior. *Diario Oficial de la Unión Europea*, L 257 de 28.8.2014, 73-114. Disponible en: http://data.europa.eu/eli/reg/2014/910/oj

UNIÓN EUROPEA, 2015. Reglamento (UE) 2015/496 del Consejo, de 17 de marzo de 2015, por el que se modifica el Reglamento (CEE, Euratom) n.º 354/83 en lo que respecta al depósito de los archivos históricos de las instituciones en el Instituto Universitario Europeo de Florencia. *Diario Oficial de la Unión Europea*, núm. 79, de 25 de marzo de 2015, pp. 1-5. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2015-80540

VERGARA PERIS, J., 2009. *La memoria quemada.* Valencia: Generalitat Valenciana.

WILSON, T., 2017. Rethinking digital preservation: definitions, models, and requirements. *Digital Library Perspectives*, **33**(2), 128-136. https://doi.org/10.1108/DLP-08-2016-0029

YAKEL, E., 2007. Digital curation. *OCLC Systems & Services: International digital library perspectives*, 23(4), 335-340. https://doi.org/10.1108/10650750710831466

ZAMORA ENCISO, R., 2010. *Competencias socio-emocionales: su desarrollo a través del juego y la simulación*. Madrid: Lulu. ISBN 978-1-4457-6098-8