

La importancia de la Cadena de custodia documental digital en la preservación documental

The importance of the digital chain of custody in document preservation

A importância da cadeia de custódia documental digital na preservação documental

Martha Hernández Olvera

Universidad Nacional Autónoma de México, México

mholi@unam.mx

<https://orcid.org/0009-0001-6300-7539>

Resumen

La cadena de custodia documental digital es un proceso que asegura la integridad, autenticidad y disponibilidad a largo plazo, porque proporciona un registro detallado en la vida del documento relacionado en la manipulación y modificación del documento digital. Esto lo apoya la seguridad en los documentos con firmas digitales, criptografía, auditorías físicas y con herramientas tecnológicas; para asegurar el estado actualizado a los formatos digitales en los que se almacenan los documentos dentro de repositorios adecuados y seleccionados por los actores que resguardan estos.

Palabras Clave: Cadena de custodia documental digital, Preservación digital, documento digital, Estándares ISO, Formato estándar.

Abstract

The digital document chain of custody is a process that ensures integrity, authenticity and long-term availability, because it provides a detailed record over the life of the document related to the manipulation and modification of the digital document. This is supported by document security with digital signatures, cryptography, physical audits and technological tools. To ensure the updated status of the digital formats in which the documents are stored within appropriate repositories selected by the actors who safeguard them.

Keywords: Digital document custody chain, Digital preservation, digital document, ISO Standards, standard format.

Resumo

A cadeia de custódia de documentos digitais é um processo que garante integridade, autenticidade e disponibilidade a longo prazo, pois fornece um registro detalhado ao longo da vida do documento relacionado à manipulação e modificação do documento digital. Isto é apoiado pela segurança documental com assinaturas digitais, criptografia, auditorias físicas e ferramentas tecnológicas; garantir o estado atualizado dos formatos digitais em que os documentos são armazenados em repositórios apropriados selecionados pelos atores que os salvaguardam.

Palavras-chave: Cadeia de custódia de documentos digitais, Preservação digital, documento digital, Normas ISO, Formato padrão.

Fecha Recepción: Abril 2024

Fecha Aceptación: Agosto 2024

Introducción

La preservación digital de documentos, tanto digitales como físicos, ha adquirido una importancia creciente en las organizaciones, ya que permite conservar la información y el testimonio de los hallazgos obtenidos a lo largo del tiempo. Para garantizar la integridad y autenticidad de estos documentos y evitar que sean alterados o manipulados de manera indebida, es fundamental implementar un proceso de cadena de custodia documental.

Este proceso es crucial para asegurar que, desde su creación, un documento sea manejado de manera adecuada, registrando quién tuvo acceso a él, cuándo fue modificado y con qué propósito. Si estos pasos no se siguen correctamente, la integridad del documento puede verse comprometida, y su fiabilidad no puede ser garantizada.

Por ejemplo, si un archivo, digital o físico, con información relevante para la organización no se gestiona adecuadamente, la falta de documentación sobre su manejo puede llevar a que se cuestione su autenticidad. Esto no solo expone a la organización a riesgos de seguridad tecnológica, humana y organizacional, sino que también puede resultar en la pérdida de confianza por parte de los responsables de la custodia del documento, así como en posibles repercusiones legales. La ausencia de una cadena de custodia sólida impide además determinar si una alteración fue causada por un error humano o por un acto malicioso, complicando la identificación de los responsables y la toma de acciones correctivas.

La preservación digital a largo plazo y la cadena de custodia documental digital son procesos interdependientes que aseguran la integridad, veracidad y disponibilidad de los documentos digitales. Para lograr un documento fiable, íntegro y auténtico, es necesario considerar

diversos factores, como los recursos humanos, la tecnología, los estándares, las políticas y los procedimientos implementados.

En una sociedad de la información y el conocimiento, estos recursos son fundamentales para impulsar el desarrollo en múltiples ámbitos. Las tecnologías de la información y la comunicación (TIC) adquieren una relevancia creciente, lo que exige una gestión adecuada. Esta sociedad tiene un impacto significativo en áreas como la educación, la investigación, los negocios y la cultura (Sánchez, 2016).

La sociedad de la información y el conocimiento ha transformado de manera esencial la forma en que se accede y comparte la información. En el contexto de los documentos digitales y los archivos, esta sociedad enfrenta nuevos retos para cubrir las necesidades contemporáneas en educación e investigación, desempeñando un papel crucial por varias razones, tales como:

Acceso global de la información: parte de la información está disponible en formato digital. Por lo que esto brinda a la sociedad que tiene conexión de Internet, un acceso instantáneo parcial y global de una gran cantidad de datos y documentos. Como indica la Unión Internacional de Telecomunicaciones (UIT, 2023), el 67% de la población mundial está ya en línea; es decir, unos 5 400 millones de personas tienen el privilegio de acceso por medio de algún dispositivo electrónico a recursos digitales.

Documentos en diferentes formatos: con el crecimiento de la información digital, la diversidad y tipos de documentos digitales almacenados han aumentado significativamente. El archivo digital abarca una amplia variedad de formatos, como JPEG, PNG, GIF, TIFF, WAV, MP3, TXT, PDF y HTML (Oliva y Pérez, 2022). Para garantizar que estos archivos permanezcan accesibles a lo largo del tiempo, es fundamental adoptar un formato estándar. Esto evita la necesidad de realizar conversiones futuras, que podrían comprometer la integridad y accesibilidad de los documentos.

El riesgo de obsolescencia tecnológica es una preocupación constante en la sociedad de la información y el conocimiento, debido a los rápidos y dinámicos avances tecnológicos. Estos cambios pueden llevar a la obsolescencia de formatos de archivos, así como de aplicaciones, herramientas de software y hardware. Dado que el hardware debe estar alineado con el software, también tiende a volverse obsoleto en un corto período de tiempo, lo que representa un desafío significativo para la preservación digital y la continuidad operativa. Ortiz (2022) expone que “Si una pieza de tecnología o software ha llegado a su fin de venta, significa que el fabricante ya no vende ese hardware o software. Los productos llegan al final de la venta mucho antes de que lleguen al final del soporte”. Esto implica la necesidad de migrar

periódicamente los documentos a nuevos formatos estándar para garantizar su accesibilidad a largo plazo, preservando al mismo tiempo la integridad de la información contenida en ellos.

El nacimiento de nuevas formas de documentación: El surgimiento de nuevas formas de documentación ha dado lugar a expresiones innovadoras, como blogs y plataformas digitales que facilitan la conexión entre personas, sistemas, repositorios y el intercambio de información en redes sociales. Si la preservación documental digital no existiera, la sociedad enfrentaría la pérdida de información valiosa en investigaciones en diversos campos en los que ha sido protagonista o creadora de conocimiento.

Sin una adecuada preservación, se perderían documentos con información única e irremplazable, resultado de logros humanos y descubrimientos que desaparecerían con el tiempo, dejando a la humanidad sin una memoria histórica. Esto implicaría la pérdida de hallazgos y avances de investigaciones cruciales, afectando nuestra capacidad para enfrentar los desafíos contemporáneos y futuros. Una generación sin historia caería en el caos al no contar con las experiencias de sucesos pasados que ofrecen valiosas enseñanzas.

La falta de accesibilidad a la información genera desinformación y desconocimiento en áreas de estudio, impidiendo el progreso científico, cultural y social. La comunidad científica y académica basa su trabajo en información y literatura previas; por lo tanto, la ausencia de documentos digitales disponibles para consulta amplía la brecha digital existente. Esta limitación restringe el acceso al conocimiento a aquellos con menos recursos económicos, tecnológicos e infraestructurales, negando oportunidades de desarrollo y exacerbando la desigualdad social. Esta situación subraya la necesidad de un esfuerzo sostenido en la digitalización de documentos, lo cual representa un gran desafío en el contexto actual. Al respecto, Iberdrola (2024) plantea “Pero la digitalización no se está dando por igual en todo el mundo y es que, también en esto, existe un desequilibrio y recibe el nombre de brecha digital. Este retraso en la digitalización de la información genera una gran afectación, contribuyendo negativamente a la humanidad. Si los documentos no están disponibles ni en formato físico ni digital, se agrava el impacto en el acceso al conocimiento y la preservación de la información. En ese sentido: Esos archivos que adquieren relevancia por su interés como prueba o testimonio de hechos, como garantía de transparencia y al cabo del tiempo se vuelven históricos, y que por lo tanto se convierten en depósito de la memoria e identidad de sus generadores y, recuperando la cita de San Agustín se han convertido en presente del pasado (Carreño-Alvarado, G., S/F, p. 104).

Riesgo de manipulación y falsificación: La preservación digital ayuda a garantizar la autenticidad e integridad de los documentos. Sin ellos los documentos digitales son vulnerables de ser alterados, manipulados o dañados de forma intencional o involuntaria y el resultado será no poder confiar en la veracidad de la información y el almacenamiento de esta. Existen varios factores para que el contenido de la información resulte dudoso.

La integridad de los datos puede verse comprometida de diversas formas, que incluyen errores humanos accidentales, ataques internos maliciosos, cualquier ciberataque externo, incluido el fraude por correo electrónico, fraude de identidad y los ataques de ransomware como ejemplos, errores de transferencia de datos, hardware comprometido, como una falla de disco, corrupción en el software. (Acronis, 2021).

Como se menciona en el párrafo anterior, la integridad de los datos puede verse comprometida por errores humanos accidentales en el manejo, procesamiento o almacenamiento de la información. La falta de normas de seguridad para el tratamiento de la información y para el lugar donde se resguarda puede poner en riesgo la autenticidad de los datos. Tanto el software como el hardware utilizados para la transferencia de datos y las plataformas que facilitan su disponibilidad deben contar con normas y políticas adecuadas para el manejo de la información, tal como lo indican las directrices establecidas. Como lo indican Barnard *et al.* (2017) “En el contexto de la preservación digital, la integridad de la información es fundamental para asegurar que los datos se mantengan íntegros y fiables a lo largo del tiempo.

La preservación documental digital es esencial para proteger el conocimiento y la memoria histórica de una sociedad. Contar con información auténtica y fiable permite tomar decisiones fundamentadas que favorezcan el progreso en diversos ámbitos del conocimiento y evitar la repetición de errores cometidos por desconocimiento. La importancia de la preservación digital radica en garantizar la disponibilidad, accesibilidad e integridad de los documentos digitales a lo largo del tiempo.

Concepto y principios de la cadena de custodia documental digital

Como señala Flores (2020), la custodia de documentos digitales debe considerar que la cadena de custodia digital no debe romperse ni interrumpirse y debe ser auditada por la cadena de preservación u otro procedimiento capaz de verificar esta garantía en el entorno digital. Este proceso se define como el aseguramiento de la integridad, autenticidad y trazabilidad de los documentos digitales durante todo su ciclo de vida. Este concepto es fundamental para el almacenamiento y gestión de información digital, especialmente en entornos donde la autenticidad y confiabilidad de los documentos son cruciales, como en el derecho, la ciencia, los archivos y la gestión de documentos en organizaciones de cualquier índole.

La cadena de custodia de documentos digitales implica una observación y registros detallados de cada paso desde la creación del documento digital hasta su disposición final o archivo. Esto incluye identificar a la persona responsable de cada edición, la fecha y hora de cada acción, y cualquier cambio o corrección realizada. Un seguimiento detallado de la evolución del documento y de las personas que intervinieron en su proceso es esencial para comprender la vida y el resultado del documento digital. El objetivo principal es garantizar que la información contenida en los documentos digitales sea auténtica, fiable, inalterada y pueda ser verificada en cualquier momento presente o futuro.

Principios de la cadena de custodia documental digital

Integridad: garantiza que los documentos digitales no estén sujetos a cambios no autorizados durante su ciclo de vida y que la información que contienen sea siempre completa y precisa.

Autenticidad: verifica la autenticidad de los documentos digitales, asegurando que provengan de fuentes confiables y que nunca hayan sido manipulados para alterar su contenido.

Confidencialidad: protege la información sensible contenida en los documentos digitales, limitando el acceso a personas autorizadas y garantizando que no se divulgue de ninguna manera. Respetando datos e información que integra el documento.

Trazabilidad: registrar detalladamente cada acción realizado sobre los documentos digitales, incluyendo quién accedió a ellos, cuándo y qué cambios se realizaron, permitiendo guardar la señal de cualquier alteración o acceso autorizado y no autorizado.

Voutssas (2010) resume esto como: El conjunto de principios, políticas, reglas y estrategias que rigen la estabilización física y tecnológica, así como la protección del contenido intelectual de documentos de archivo adquiridos, con objeto de lograr en ellos una secuencia de

existencia a largo plazo continua, perdurable, estable, duradera, ininterrumpida, inquebrantada, sin un final previsto.

Técnicas y herramientas para la implementación de la cadena de custodia

La implementación efectiva de la cadena de custodia documental digital requiere el uso de diversas técnicas y herramientas especializadas. Algunas de las técnicas ayudan a garantizar la integridad, autenticidad y confidencialidad de los documentos digitales, e incluyen:

Firmas digitales: utilizadas para verificar la autenticidad e integridad de un documento digital, permitiendo a los usuarios firmar electrónicamente los documentos y verificar que no han sido modificados.

Criptografía: se utiliza para proteger la confidencialidad de los documentos digitales mediante el cifrado de su contenido, asegurando que solo las personas autorizadas puedan acceder a ellos. Con los mecanismos autorizados electrónicamente por quienes realizaron la encriptación.

Control de acceso: implementación de políticas de acceso que regulen quién puede acceder y realizar cambios en los documentos digitales, así como la asignación de permisos de usuario específicos. Este control puede darse por niveles de acceso, conforme a la autorización de conocer los datos.

Registro de auditoría o control de acciones: se registra cada acción realizada sobre los documentos digitales, incluyendo quién accedió a ellos, cuándo y qué cambios se realizaron, y ¿porqué?, proporcionando una trazabilidad completa de las actividades realizadas.

Almacenamiento seguro: utilización de sistemas, plataformas de almacenamiento seguro que protejan los documentos digitales contra pérdidas, robos o daños físicos, climáticos, así como contra amenazas cibernéticas como malware o ataques de hacking.

También se considera como herramienta, software especializado en gestión documental y preservación digital que facilitan la aplicación de la cadena de custodia documental. Como sistemas de gestión documental (DMS), sistemas de gestión de registros electrónicos (ERMS), software de firma electrónica, herramientas de cifrado, sistemas de control de versiones y soluciones de almacenamiento seguro.

La combinación adecuada de técnicas y herramientas permite establecer una cadena de custodia documental digital sólida y confiable, garantizando la seguridad y autenticidad de los documentos digitales a lo largo del tiempo.

No debe confundirse con seguridad informática, sino como:

El proceso de establecer y observar un conjunto de estrategias, políticas, técnicas, reglas, guías, prácticas y procedimientos tendientes a prevenir, proteger y resguardar de daño, alteración o sustracción a los recursos informáticos de una organización y que administren el riesgo al garantizar en la mayor medida posible el correcto funcionamiento ininterrumpido de esos recursos (Voutssas, 2010).

Por lo tanto, los recursos deben estar soportados por sistemas informáticos para garantizar la continuidad y disponibilidad de los procesos que se llevan a cabo para dar continuidad para estar disponible en línea a largo plazo.

Normativas y estándares aplicables

Para la implementación de la cadena de custodia documental digital, es fundamental seguir normativas y estándares específicos que garanticen la integridad, autenticidad y trazabilidad de los documentos digitales. Algunos de los más relevantes son:

ISO 14721:2012 (OAIS)

Este estándar establece un modelo de referencia para la preservación a largo plazo de recursos digitales, incluyendo la gestión de la cadena de custodia documental. También conocido como "Space data and information transfer systems - Audit and certification of trustworthy digital repositories," es fundamental en la preservación digital y la gestión de repositorios digitales confiables. Este estándar establece los requisitos para auditar y certificar la confiabilidad de los repositorios digitales que almacenan datos espaciales, sensibles e información crítica. Su propósito es garantizar que estos repositorios utilizados cumplan con estándares internacionales de confiabilidad, autenticidad, integridad y disponibilidad a lo largo del tiempo (International Organization for Standardization, 2012).

Este estándar sirve como cimiento para establecer prácticas y procedimientos que aseguren la trazabilidad y la integridad de los datos a lo largo de su ciclo de vida. Esto incluye aspectos como la gestión de metadatos, la preservación de formatos de archivo, la seguridad de la información y la planificación para la migración a tecnologías futuras. En lo relacionado al almacenamiento de la información digital establece principios y métodos para gestionar la información digital a lo largo de su ciclo de vida, incluido el almacenamiento a largo plazo—. Este estándar es fundamental en el campo de la preservación digital porque proporciona pautas para garantizar la integridad, autenticidad y accesibilidad a largo plazo de la información digital.

ISO 16363:2012 (Trustworthy digital repositories)

“Requisitos del auditor para sistemas de gestión de confianza digital para repositorios confiables”: Define los requisitos de certificación para repositorios digitales confiables para garantizar la confiabilidad, confiabilidad e integridad de los documentos digitales a lo largo del tiempo. Al cumplir con los requisitos establecidos por este estándar, las organizaciones aseguran que sus sistemas de gestión de documentos digitales cumplan con los requerimientos para retener de manera efectiva y confiable los documentos digitales a lo largo del tiempo. Voutssás (2009) plantea que “el objetivo de MoReq fue definir de forma general las características que debe tener una aplicación destinada a la gestión de documentos electrónicos de archivos, tradicionales o digitales (p.150).

ISO 15489:2001 (Gestión de documentos)

Proporciona un modelo para la gestión documental y la preservación digital, especialmente en la cadena documental. Este estándar proporciona pautas detalladas para gestionar registros y garantizar su disponibilidad, confiabilidad y preservación a largo plazo. ISO 15489 es importante para establecer políticas y procedimientos que garanticen la integridad y autenticidad de los documentos digitales que crea su organización. Además, este estándar ayuda a las organizaciones a identificar el entorno regulatorio que afecta sus actividades. Este estándar es esencial para garantizar la confiabilidad y la preservación a largo plazo de los documentos digitales en el campo de la gestión documental y el archivo digital a largo plazo. Voutssás refiere que “este estándar se derivó de MoReq que incluye 390 requisitos y 127 elementos de metadatos para garantizar la adecuada gestión, preservación y disponibilidad a largo plazo de los documentos electrónicos producidos por una organización (2009, p.150).

Relación con la preservación a largo plazo

Para mantener la preservación a largo plazo de la cadena de custodia documental digital, es crucial implementar prácticas y tecnologías adecuadas, como la gestión de registros electrónicos, la criptografía, el almacenamiento seguro y la utilización de estándares y formatos abiertos y no licenciados. Además, se deben establecer políticas y procedimientos claros para la gestión y el mantenimiento de la cadena de custodia a lo largo del ciclo de vida del documento digital.

Principalmente establecer políticas y procedimientos claros para gestionar y mantener la cadena de custodia durante todo el ciclo de vida de los documentos digitales. El software

utilizado para el manejo de los documentos y almacenamiento debe de cumplir normas de ISO's para asegurar que los archivos tienen la integridad, autenticidad y accesibilidad a largo plazo.

La relación entre la preservación a largo plazo y la cadena de documentos digitales es importante para garantizar la integridad, autenticidad y accesibilidad de los documentos digitales a lo largo del tiempo. La preservación a largo plazo tiene como objetivo garantizar la durabilidad y accesibilidad de los documentos digitales, mientras que el proceso de archivo de documentos digitales detalla cada paso por el que pasa un documento para garantizar su integridad y autenticidad y uso futuro. Como expone Voutssás: Preservar información digital a largo plazo requiere de sistemas, instituciones, modelos técnicos y de organización, personal calificado y experimentado lo suficientemente robustos para sortear fallos tecnológicos, cambios sucesivos de plataformas de cómputo, obsolescencia de medios y formatos de almacenamiento, errores humanos, negligencia y ataques malintencionados, cambios a la misión institucional de las organizaciones, fallas e interrupciones en su dirección y financiamiento, por mencionar algunas amenazas (2010, p. 9).

Se requiere personal especializado para el manejo de tecnología y archivos digitales y físicos para garantizar su preservación a largo plazo con todas las características que solicitan los estándares internacionales.

El objetivo es mantener registros precisos. La cadena de custodia de documentos digitales asegura que estos se almacenen de manera eficaz para su revisión y uso futuro. Las prácticas de preservación a largo plazo, junto con una cadena de custodia documental digital supervisada e implementada adecuadamente, garantizan que los documentos digitales conserven su valor auténtico y puedan ser utilizados de manera segura en una variedad de contextos, incluyendo entornos legales, forenses, de archivos y de gestión documental.

Desafíos y tendencias

La responsabilidad de los organismos es desarrollar modelos teóricos y técnicos que mitiguen el riesgo de pérdida de información, mediante la creación de estrategias centradas en la preservación digital. Estas estrategias deben enfocarse en la gestión de recursos técnicos, documentos, archivos e infraestructura.

Existen desafíos y tendencias en la cadena de custodia digital, como lo son:

Obsolescencia tecnológica

El rápido avance en hardware y software plantea retos significativos para la preservación digital a largo plazo, debido a la obsolescencia de formatos, sistemas e infraestructura. Para abordar estos desafíos, se requieren estrategias y propuestas de formatos de conservación, como el PDF, que sirvan como formatos base para documentos, imágenes y sonidos. Es crucial que la migración de documentos sea lo más transparente posible, minimizando la manipulación de los archivos. Además, el acceso a los documentos debe garantizarse sin dificultades para quienes los gestionan o revisan.

El rápido avance tecnológico plantea desafíos en la preservación a largo plazo de documentos digitales debido a la obsolescencia de formatos y sistemas, lo que requiere estrategias de migración y actualización constantes.

Seguridad de la Información

Garantizar la integridad y autenticidad de los documentos digitales a lo largo del tiempo es un desafío clave. Es esencial implementar medidas que aseguren que los documentos producidos por instituciones o personas durante sus actividades conserven su valor probatorio y puedan ser utilizados con confianza en diversos contextos. La ciberseguridad de una organización debe mantenerse actualizada en línea con las mejores prácticas y estándares de seguridad, abordando las vulnerabilidades y protegiendo contra posibles siniestros, ya sean humanos, tecnológicos o naturales.

Gestión del cambio

La gestión efectiva del cambio tecnológico y normativo es fundamental para mantener actualizadas las prácticas de preservación digital y adaptarse a nuevas regulaciones y estándares. Las tecnologías emergentes y la tecnología en la nube ofrecen oportunidades para mejorar la gestión y preservación de la cadena de custodia documental digital. La interoperabilidad, seguridad y privacidad son cruciales para fortalecer la integridad y trazabilidad de los documentos digitales, conservando la autenticidad de la información a pesar de los avances tecnológicos y los cambios en las prácticas técnicas. Establecer políticas y prácticas que garanticen la usabilidad a lo largo del tiempo es esencial para mantener la autenticidad e integridad de los documentos digitales.

Conclusiones

La preservación de documentos digitales no se limita a seleccionar, apartar y almacenar documentación que se considera relevante por su contenido. En realidad, es una tarea compleja que depende de múltiples procesos, acuerdos, políticas, software, hardware, planificación y un firme compromiso con los estándares internacionales en el manejo de la información documental. Es crucial entender que esta acción está estrechamente vinculada a otros procesos que contribuyen a obtener resultados precisos. La cadena de custodia documental digital debe ser documentada cuidadosamente, lo que implica seleccionar software adecuado para gestionar y almacenar todos los documentos digitales que se preservarán. Este proceso garantiza que la documentación se mantenga íntegra, auténtica y con la trazabilidad necesaria durante todo su ciclo de vida. No se debe pasar por alto la seguridad de la información ni los recursos tecnológicos necesarios para el manejo, almacenamiento y disponibilidad de los documentos digitales.

-Los estándares como ISO 14721:2012 (OAIS), ISO 16363:2012 e ISO 15489:2001 son fundamentales para el manejo de la documentación digital en la preservación utilizando la cadena de custodia documental digital. Estos estándares proporcionan directrices para garantizar que los procesos de almacenamiento y gestión se realicen de manera puntual y segura, asegurando la autenticidad de los documentos a lo largo de todo su ciclo de vida. Además, es crucial contar con personal capacitado, tanto en bibliotecología como en tecnología, para asegurar que cada proceso de preservación se lleve a cabo con la calidad y el manejo requerido. El personal debe estar entrenado en todas las fases del ciclo de vida de un documento y ser capaz de actualizar y crear políticas que mantengan la vigencia de las prácticas de preservación digital. Asimismo, es importante estar al día con las tecnologías emergentes y las actualizaciones en documentación para garantizar una migración consciente y ordenada. Conocer los estándares de formatos, metadatos, manipulación y migración permite a la organización anticipar y gestionar cambios en los procesos de preservación, tomando decisiones informadas que afecten la integridad y accesibilidad de los documentos en sus repositorios.

Referencias

- Acronis International GmbH (2021). *¿Qué es la integridad de los datos?*. Acronis.
<https://www.acronis.com/es-mx/blog/posts/data-integrity/>
- Barnard, A., Delgado, A., y Voutssás, J. (2017). *Un marco de referencia para la preservación digital* (1ª ed., p. 49). Ciudad de México: Archivo General de la Nación.
https://iibi.unam.mx/archivistica/InterPARES_1_020617.pdf
- Carreño-Alvarado, G. (s/f). *La importancia de la conservación de los archivos para estudios de la historia de empresas, organizaciones de la sociedad civil, y de instituciones privadas en México*. Itaipue.org.mx, 104
<https://itaipue.org.mx/cia/docs/viernes14/mesa7/1250%201310%20La%20importancia%20de%20la%20conservaci%C3%B3n%20de%20los%20archivos%20Gloria%20Carre%C3%B1o.pdf>
- Flores, D. (2020). *La Cadena de Custodia de Archivos Digitales - CCDA combinada con Preservación Digital Sistémica - PDS para Archivos*. (Sin información). Dpconline.org; Digital Preservation Coalition. S/P.
<https://www.dpconline.org/blog/wdpd/blog-daniel-flores-wdpd>
- Iberdrola, (2024). *La brecha digital en el mundo y por qué provoca desigualdad*. Iberdrola, S.A. <https://www.iberdrola.com/compromiso-social/que-es-brecha-digital>
- International Organization for Standardization. (2012). *ISO 14721:2012: Space data and information transfer systems — Open archival information system (OAIS) — Reference model*. (2ª ed., 2012) <https://www.iso.org/standard/57284.html>
- Space Data System Practices Reference model for an open archival information system (OAIS). ISO.ORG <https://www.iso.org/standard/57284.html>
- Oliva, J. y Pérez, S. (2022). *Formatos digitales, cuál elegir en cada ocasión*. Editorial EOC
<https://www.editorialuoc.com/news/21/>
- Ortiz, A. E. (2020). *¿Qué es la obsolescencia tecnológica? Significado, concepto*. Blog HostDime Latinoamérica, servidores dedicados. <https://www.hostdime.la/blog/que-es-la-obsolescencia-tecnologica-significado-concepto/>
- Sánchez, A. y Ileana R. (2016). *La Sociedad de la Información, Sociedad del Conocimiento y Sociedad del Aprendizaje. Referentes en torno a su formación*. 12(2), 235-243). Dialnet plus. de <https://dialnet.unirioja.es/servlet/articulo?codigo=5766698>
- Unión Internacional de Telecomunicaciones (UIT). (2023). *La población mundial sin conexión sigue disminuyendo hasta los 2 600 millones de personas en 2023*. ITU., de

<https://www.itu.int/es/mediacentre/Pages/PR-2023-09-12-universal-and-meaningful-connectivity-by-2030.aspx>

Voutssás, M. J. (2009). *Preservación del patrimonio documental digital en México*. UNAM-CUIB.

https://iibi.unam.mx/voutssasmt/documentos/preservacion_digital_y_cadena.pdf

Voutssás, M, J. (2010). *La cadena de preservación en archivos digitales*. UNAM-CUIB.

https://ru.iibi.unam.mx/jspui/bitstream/IIBI_UNAM/L49/1/preservacion_patrimonio.pdf

Voutssás, M.J. (2010). Preservación documental digital y seguridad informática. *Investigación bibliotecológica*, 24(50), 127-155

https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2010000100008.