UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Recomendaciones para la conservación de archivo digital en instituciones públicas

TESIS

Que para obtener el título de

Ingeniero en Computación

P R E S E N T A

Diego Granillo Zeferino

DIRECTOR DE TESIS

M.I. Angel Cesar Govantes Saldívar

Ciudad Universitaria, Cd. Mx., 2026

PROTESTA UNIVERSITARIA DE INTEGRIDAD Y HONESTIDAD ACADÉMICA Y PROFESIONAL
(Titulación con trabajo escrito)

De conformidad con lo dispuesto en los artículos 87, fracción V, del Estatuto General, 68, primer párrafo, del Reglamento General de Estudios Universitarios y 26, fracción I, y 35 del Reglamento General de Exámenes, me comprometo en todo tiempo a honrar a la institución y a cumplir con los principios establecidos en el Código de Ética de la Universidad Nacional Autónoma de México, especialmente con los de integridad y honestidad académica.

De acuerdo con lo anterior, manifiesto que el trabajo escrito titulado RECOMENDACIONES PARA LA CONSERVACION DE ARCHIVO DIGITAL EN INSTITUCIONES PUBLICAS que presenté para obtener el titulo de INGENIERO EN COMPUTACIÓN es original, de mi autoría y lo realicé con el rigor metodológico exigido por mi Entidad Académica, citando las fuentes de ideas, textos, imágenes, gráficos u otro tipo de obras empleadas para su desarrollo.

En consecuencia, acepto que la falta de cumplimiento de las disposiciones reglamentarias y normativas de la Universidad, en particular las ya referidas en el Código de Ética, llevará a la nulidad de los actos de carácter académico administrativo del proceso de titulación.

DIEGO GRANILLO ZEFERINO
Número de cuenta: 312070357

Agradecimientos

Agradezco a Dios y a la vida por permitirme llegar a culminar este camino en mi vida.

A mis padres por acompañarme y apoyarme siempre incondicionalmente en cada etapa, enseñándome, con amor y ejemplo, el valor del esfuerzo y el trabajo honestos.

A mi hermana y hermano por ser los mejores cómplices de vida y preocuparse por mí.

A la UNAM y a la Facultad de Ingeniería por forjar el profesional que siempre me propuse ser.

A todos los docentes con los que trabajé a lo largo de la carrera.

Extiendo mi gratitud a mi asesor por su paciencia, guía y compromiso con este proyecto.

Agradezco a la tres veces H Tuna de la Facultad de Ingeniería de la UNAM por darme a los amigos y experiencias que me dio durante la carrera y todavía más.

RECOMENDACIONES PARA LA CONSERVACIÓN DE ARCHIVO DIGITAL EN INSTITUCIONES PÚBLICAS

Contenido

Introducción

Durante los meses que desarrollé actividades en instituciones públicas tuve acceso a diferentes espacios que servían como “site” para la red del edificio, permitiéndome conocer de primera mano la arquitectura y funcionamiento de dicha red. Llamó mi atención el hecho de que en uno de esos sites había una división: un tercio del espacio era ocupado por el site y la parte restante era ocupada por anaqueles que contenían gran cantidad de libros, revistas, periódicos, cintas de audio y video, Cd, y discos duros etiquetados con cinta adhesiva transparente. Surgieron unas preguntas: ¿pueden consultar aun lo que contienen esas cintas y discos si es que los equipos para ello aún funcionan? ¿Por cuánto tiempo más podrán funcionar esos dispositivos en las condiciones en que están guardados?

En un primer momento, cuando se habla de la preservación de archivos inevitablemente se llega a pensar en documentos sobre papel antiguo, viejos libros con cubierta de cuero acomodados en anaqueles que ocupan gran espacio y que deben ser hojeados en un ambiente estéril utilizando guantes de látex. Por ello, retomando a (Chornet, 2014) una comparación (Tabla 1) entre la conservación tradicional de los documentos sobre papel y los nuevo retos de la preservación digital ayudará a comprender lo que demandan estos últimos para mantenerlos utilizables a lo largo del tiempo.

DOCUMENTO EN PAPEL	DOCUMENTO ELECTRÓNICO
El soporte puede durar muchos años	El soporte tiene una vida corta
Aun defectuoso o no restaurado se puede interpretar (leer)	Si está defectuoso, impide la interpretación (lectura)
El organismo debe establecer un plan de conservación y restauración	El organismo debe establecer un plan de preservación
El organismo debe establecer un plan contra el robo o sustracción ilegal	El organismo debe establecer un plan contra el robo o sustracción ilegal
Si está dañado, se puede restaurar mediante injertos, limpiezas y otras técnicas de carácter químico; tiene gran dependencia del soporte	Si está dañado, es casi imposible de recuperar; excepcionalmente, algunos programas pueden extraer parte de la información; tiene gran dependencia del formato (se prefieran formatos que incluyan la compatibilidad retrospectiva)
Se puede conservar durante muchos años sin intervención o uso, en condiciones ambientales adecuadas (poco exigentes)	Se necesita de la intervención humana periódica para realizar una política de migraciones y asegurar la conservación de la información por la obsolescencia tecnológica (hardware y software)
Su autenticidad está asegurada por la política de custodia, el sello del organismo o la firma de los autores	Su autenticidad está asegurada por la política de custodia, la firma electrónica u otro sistema de encriptación con clave asimétrica
Su identificación en la organización se realiza mediante técnicas de descripción (analógica o electrónica) y localización (estanterías, cajas, tejuelos descriptivos, etc.)	Su identificación en la organización se realiza mediante metadatos en el entorno digital
No suele cambiar de sitio físico, y su traslado supone un elevado coste humano y económico	Suele trasladarse con frecuencia a otros sitios físicos, mediante el transporte de sus soportes o mediante la transferencia telemática
Conocimientos o perfil profesional del con-servador: química, biología, historia, paleografía, etc.	Conocimientos o perfil profesional del con-servador: informática (software y hardware), gestión de documentos electrónicos
Los archivos conservan documentación de productores propios y de productores desaparecidos	Los archivos, a corto término, empezarán a conservar documentos digitales de productores propios, y a largo término deberán contemplar la conservación de los organismos desaparecidos
El acceso es presencial (laboratorios, salas de consulta, etc.); los lugares deben cumplir requisitos de conservación física y de seguridad contra la sustracción	El acceso es en línea (intranet, internet, etc.); la red debe cumplir requisitos de seguridad, usabilidad y accesibilidad, para evitar la sustracción o infección por virus informático

Tabla 1 Diferencias y similitudes en la conservación de documentos

De acuerdo con (Rodríguez Reséndiz et al., 2017), lo que antes eran archivos documentales se han convertido en su mayoría en archivos digitales no sólo gracias a la digitalización de documentos físicos sino también a que cada vez más se opta por trabajar con documentos creados a través de herramientas digitales desde su origen. Sin embargo, indican los autores que estudios recientes advierten que no existe una única tecnología para preservar grandes cantidades de documentos digitales, que los soportes digitales son altamente vulnerables y la obsolescencia tecnológica es más temprana que en los soportes tradicionales.

Por otro lado, enfrentamos el reto de que la preservación y conservación de los archivos digitales a largo plazo implica proveer acceso indefinido a los documentos o a su contenido como mínimo, además de que en el caso de documentos electrónicos también es importante la preservación del contexto de creación pues dota de valor al documento (Soler Jiménez, 2012). En México, de acuerdo con la Ley General de Archivos [LGA] (última reforma DOF 19-01-2023), ese largo plazo no excede los 25 años como tiempo máximo que se debe preservar un documento.

Por si esto fuera poco, existe otro problema: cada día aumenta la cantidad de contenidos digitales en archivos, museos y bibliotecas y con ello ha quedado en evidencia la falta de tecnología, infraestructura, conocimiento y personal capacitado que maneje los grandes volúmenes de información (Rodríguez Reséndiz et al., 2017).

Con esto en consideración, con un enfoque descriptivo y como resultado de una indagación en diversas fuentes, el presente trabajo busca aportar al o los responsables de la preservación y conservación de los archivos digitales en cada institución, herramientas que van más allá de sus actividades cotidianas con el fin de que sus decisiones lleven a buen puerto el

cumplimiento de las disposiciones legales que apliquen según sea el caso. Atacar a pequeña escala para fortalecer a gran escala.

Se busca que la indagación aquí presentada no sea especifica a un solo contexto pues va dirigida al general de las instituciones públicas, y que sea de utilidad dentro del marco legislativo aplicable en México aun cuando este marco llegase a cambiar a lo largo del tiempo.

En el primer capítulo se exponen los términos que serán de importancia contextual para comprender y aplicar las recomendaciones que se brindan. Estos conceptos se retoman tanto de la legislación mexicana como de diversos autores. Cabe mencionar que, aunque algunos tienen su aplicación en la archivística tradicional; se consideran también conceptos que se aplican en el campo digital. Más adelante se expone la importancia que tienen las políticas de seguridad en una institución y la participación de los colaboradores en la aplicación de ellas. Continuando, la importancia que tiene la conservación de los archivos digitales. Así, para el final del primer capítulo se afina el objeto de estudio de este trabajo.

En México, para Voutssás, el panorama de los archivos y su práctica ha cambiado radicalmente. Antes las practicas archivísticas eran prácticamente nulas, aspectos como la seguridad y la organización no interesaban y no fue sino hasta el advenimiento de las leyes de Transparencia (2002) y de Archivos (2012), que las instituciones cayeron en cuenta de que debían dar un trato más serio y profesional a sus archivos para responder a los lineamientos legales, puesto que los servicios gubernamentales registran cada vez más trámites oficiales que guardan información digital acerca de los usuarios (2015, p. 21-23).

En el segundo capítulo se expone la situación mexicana referente a la conservación de documentos de archivo digital teniendo como base la Ley General de Transparencia y Acceso a la Información Pública, y la Ley General de Archivos retomando de esta última el instrumento de control con el que todas las instituciones públicas deben contar, el Catálogo de Disposición Documental. En este catálogo se definen los tiempos que se debe preservar un archivo de acuerdo con la valoración que haya hecho cada institución. Posteriormente, se expone de forma general la estructura y funcionamiento del Modelo OAIS, que sirve como referencia para la preservación, conservación y acceso a largo plazo de la información. Adicionalmente, se exponen los factores físicos, tecnológicos y económicos que repercuten en la conservación de documentos de archivo digital en instituciones públicas.

Por último, en el tercer capítulo, considerando diversos autores y estándares en materias de organización y administración de centros de datos, administración de redes de datos, seguridad de la información y dispositivos de almacenamiento; se formulan una serie recomendaciones físicas, tecnológicas y económicas para la conservación de archivo digital en instituciones públicas.

Al término del capítulo, siguiendo la línea de las recomendaciones hechas, se sugieren diferentes políticas y lineamientos para la consulta, manipulación de los soportes documentales, vigencia de formatos y conservación de los archivos digitales. Dichas recomendaciones, políticas y lineamientos tienen como fin coadyuvar en el camino hacia el diseño e implementación de procesos y estrategias adecuados para cumplir lo estipulado por la ley de acuerdo con el contexto y posibilidades de cada institución.

Para concluir, se marca la necesidad de nuevo conocimiento respecto al tema de la conservación de soportes documentales digitales y la preservación de la información

contenida en documentos digitales. Además, se propone una nueva línea de indagación si se considera al almacenamiento en la nube dentro del contexto abordado en este trabajo.

CAP I: Conceptos y definiciones sobre conservación de archivos digitales

Definiciones

Inicialmente, resulta fundamental definir los conceptos que serán el cimiento para la buena comprensión de esta propuesta y de su completa implementación en las instituciones. Enfatizamos la importancia de difundir y hacer comprensibles estos conceptos a todo el personal de forma clara y sencilla.

Las siguientes definiciones derivan en la gestión de archivos en formato físico, pero proponemos aplicar estos conceptos al manejo de archivos en medios digitales, como se menciona en la definición de conservación de archivos. Además, se toman en cuenta definiciones establecidas en la Ley General de Archivos [LGA] (última reforma DOF 19-01-2023), ya que la mayoría de los fundamentos de este trabajo se derivan de esta ley.

Institución

Según la definición del Diccionario de la lengua española de la Real Academia Española (RAE), una institución se describe como un "organismo que cumple una función de interés público, especialmente benéfica o educativa." (ASALE & RAE, 2022) Además, se identifica "organización" como un sinónimo. En este trabajo, utilizaremos ambos conceptos de manera intercambiable debido a su equivalencia según la mencionada definición.

Documento

Según la Real Academia Española (RAE, 2024), es un "escrito en que constan datos fidedignos o susceptibles de ser empleados como tales para probar algo."

Un documento es cualquier elemento que alberga información que describe, comunica o representa un evento, sin importar su naturaleza, medio, formato, método de creación o tipo de firma que tenga (Téllez, 2009, p. 289).

Documento de archivo

Documento elaborado o recibido durante el curso de una actividad práctica ya sea como instrumento o derivado de esa actividad y que es separado (apartado, guardado) para acción posterior o como referencia (InterPARES, 2008, p. 2).

Documento de archivo electrónico o digital

"Un documento digital que es tratado y manejado como un documento de archivo" (InterPARES Terminology Database 2012)

Archivo

"Al conjunto organizado de documentos producidos o recibidos por los sujetos obligados en el ejercicio de sus atribuciones y funciones, con independencia del soporte, espacio o lugar que se resguarden" (LGA, 17/09/2023, a. 4, fr. III).

Archivo de trámite

"Al integrado por documentos de archivo de uso cotidiano y necesario para el ejercicio de las atribuciones y funciones de los sujetos obligados" (LGA, 26/01/2024, a. 4, fr. V)

Archivo de concentración

"Al integrado por documentos transferidos desde la áreas o unidades productoras, cuyo uso o consulta es esporádica y que permanecen en él hasta su disposición documental" (LGA, 17/09/2023, a. 4, fr. IV).

Archivo histórico

“Al integrado por documentos de conservación permanente y de relevancia para la memoria nacional, regional o local de carácter público” (LGA, 17/09/2023, a. 4, fr. VIII).

Repositorio

“Espacio físico o virtual en el que se organiza y preserva información en diversos soportes documentales” (Quintos et al., 2022, p. 27).

Catálogo de disposición documental

“Al registro general y sistemático que establece los valores documentales, la vigencia documental, los plazos de conservación y la disposición documental” (LGA, 17/09/2023, a. 4, fr. VXIII).

Conservación de documentos de archivo digital

Acciones tomadas para anticipar, prevenir, detener o retardar el deterioro del soporte de obras digitales con objeto de tenerlas permanentemente en condiciones de usabilidad; comprende la estabilización tecnológica y la migración a nuevos soportes, sistemas y formatos digitales para garantizar la trascendencia de los contenidos (Voutssás, Barnard, 2014, p 148).

Preservación de documentos de archivo digital

El proceso específico para mantener los materiales digitales durante y a través de las diferentes generaciones de la tecnología a lo largo del tiempo, con independencia de los soportes donde residan (Voutssás, Barnard, 2014, p 174).

Soportes documentales

“A los medios en los cuales se contiene información además del papel, siendo estos materiales audiovisuales, fotográficos, fílmicos, digitales, electrónicos, sonoros, visuales, entre otros” (LGA, 17/09/2023, a. 4, fr. LIV).

Políticas

“Orientaciones o directrices que rigen la actuación de una persona o entidad en un asunto o campo determinado” (RAE, 2022b).

Procedimientos

El conjunto de reglas escritas y no escritas y/o los pasos formales para seguirlas que rigen la conducta y etapas para llevar a cabo una cierta transacción (Voutssás, Barnard, 2014, p 178).

Importancia de las políticas de seguridad.

En nuestra vida cotidiana llevamos a cabo diversas actividades relacionadas con el cuidado. Por ejemplo, al lavar los edredones que utilizamos, solemos revisar la etiqueta que nos proporciona información sobre los materiales con los que están hechos y algunas recomendaciones para su cuidado. Similarmente, al guardar los alimentos que compramos en el mercado o supermercado, estamos al tanto de qué productos deben almacenarse en la despensa y cuáles es mejor conservar en el refrigerador. En todas estas situaciones, y muchas otras, existe un denominador común: tenemos un conocimiento previo sobre lo que deseamos conservar.

En el ámbito de las instituciones, es fundamental tener un conocimiento preciso de los activos que se desean proteger. Primero se debe tener en cuenta el tipo de seguridad para la que se diseñan las políticas de seguridad: (Terán, 2014, p. 59-60)

a) Medidas de seguridad activa: Aquellas cuyo propósito es eliminar o disminuir los riesgos existentes o sus efectos para el sistema una vez que se producen.
b) Medidas de seguridad pasiva: Están destinadas para actuar si llega a producirse un desastre.

Según (Cebrián, 2014):

> Para definir las políticas de seguridad, lo primero que se debe hacer es un análisis de las posibles amenazas que puede sufrir un sistema informático, un estudio de las pérdidas que podrían suponer estos ataques y otro estudio valorando las posibilidades que hay de que un ataque ocurra. (p. 72)

En la literatura especializada, diversos autores coinciden de manera consistente en que para lograr que las políticas de seguridad alcancen sus objetivos es esencial que sean aceptadas y comprendidas por todos los colaboradores en la institución, tanto en el área de informática como en las demás áreas.

- "Una empresa debe tener un documento perfectamente elaborado sobre el tema de política de seguridad, siendo puesto a disposición de todos los empleados" (Cebrián, 2014, p. 75).
- "Las políticas de seguridad son pautas y procedimientos que dan soporte a la seguridad conforme a requisitos legales y de negocio. Deben revisarse, actualizarse y darse a conocer a todo el personal de la organización para su fiel cumplimiento" (Postigo, 2020, p. 5).

Comprendiendo la importancia de que los colaboradores de la organización estén familiarizados con las políticas de seguridad emitidas por el área de informática, es momento de identificar las características que una política de seguridad debe reunir. Estas características servirán como base para la formulación de procedimientos de seguridad apropiados.

De acuerdo con (Cebrián, 2014):

> Para constituir una política de seguridad completa esta debe cumplir la siguiente normativa:
>
> - ❖ Debe definir qué es la seguridad de la información, cuáles son sus objetivos principales y la importancia en la organización.
> - ❖ Establecer responsabilidades respecto a la seguridad de la información.

- Definir la filosofía a seguir respecto al acceso de los datos, archivos, etc.
- Compromiso a cumplir de todos los usuarios, en especial de los altos cargos.
- Establecer la base para diseñar las normas y los procedimientos referidos a:
  - Administración de los equipos.
  - Prevención y detección de los virus.
  - Seguridad física y en el ambiente de trabajo.
  - Seguridad de las personas.
  - Clasificación y control de los datos almacenados.
  - Organización de la seguridad.

Importancia de la conservación de documentos de archivo digital

La información almacenada en empresas es un valioso activo en la actualidad y su valor va más allá de la accesibilidad rápida. El crecimiento rápido de datos no debe excusar la falta de organización por importancia o cantidad. La falta de orden en la información crea obstáculos en su procesamiento debido a tiempos de acceso diferentes (Cantone, 2012).

Al ser las organizaciones fuentes inagotables de información, en ocasiones tienen dificultades para manejar el flujo intenso de datos generados dentro y fuera de ellas. Esta concurrencia puede superar la capacidad de tratamiento de esta, esto a pesar de las inversiones en infraestructura y tecnologías modernas (Hernández y Martínez, 2019, p. 52).

Contexto de aplicación de la propuesta

Institución pública

A diferencia de lo que se podría pensar, las normas no se limitan a ser aplicadas únicamente por las instituciones privadas. Cualquier tipo de entidad, con el fin de alcanzar un nivel óptimo en la calidad de sus funciones a largo plazo, debe consultar y seguir las regulaciones vigentes. Recordemos que las normas son directrices que se deben cumplir para establecer políticas destinadas a mejorar los procesos y la productividad.

Por otro lado, las instituciones de interés en este estudio no están exentas de la aplicabilidad de las normas, especialmente en el contexto de tecnologías de la información, ya que cuentan con procesos, departamentos o áreas que involucran un considerable uso de recursos informáticos. La pregunta es: ¿las normas internacionales se aplican al gobierno local? Esta interrogante puede generar ambigüedad si no definimos con precisión el enfoque dentro de las organizaciones, además de considerar las diferencias entre una institución pública y una privada.

Para comenzar, comprendamos ciertas características que permiten categorizar las organizaciones. Esto contribuirá a una comprensión más sólida de los impactos que este trabajo busca lograr en la sociedad. Una de las características fundamentales es el tipo de beneficiario principal, ya que esto constituye la razón de ser de las organizaciones.

Las organizaciones públicas, a diferencia de las privadas, se caracterizan por proporcionar servicios públicos a la ciudadanía. Su administración generalmente recae en el Gobierno en funciones, aunque en ocasiones se les otorga cierta autonomía al designar gestores independientes para dirigir la institución.

Beneficiario principal	Tipo de organización	Ejemplos
Los propios miembros de la organización	Asociación de beneficiarios mutuos	Asociaciones profesionales, cooperativas, sindicatos, fundos mutuos, consorcios
Los propietarios o accionistas de la organización	Organizaciones de intereses comerciales	Sociedades anónimas o empresas familiares
Los clientes	Organizaciones de servicios	Hospitales, universidades, organizaciones religiosas y filantrópicas, agencias sociales
El público en general	Organizaciones del Estado	Organización militar, correos y telégrafos, seguridad pública, saneamiento básico, organización jurídica y penal

Tabla 2 Tipología de las organizaciones de Blau y Scott

(Chiavetano, 219, p. 167) resume en la Tabla 2 la tipología de Blau y Scott basada en el beneficiario principal (principio de cui bono), es decir, en quién recibe los beneficios de la organización. Esta clasificación tiene la ventaja de resaltar la influencia y el poder que el beneficiario ejerce sobre las organizaciones, llegando incluso a condicionar su estructura y sus metas.

En este trabajo nos centraremos en las organizaciones cuyo principal beneficiario es el público en general; es decir, las organizaciones del Estado.

Ciclo de vida de los documentos electrónicos

Hasta este momento, hemos identificado el tipo de organizaciones a las que se dirige este trabajo. Ahora es importante definir el aspecto específico del proceso de gestión documental que abordaremos. Para lograrlo, examinaremos el ciclo de vida de los documentos

electrónicos con el respaldo de documentación publicada por el Archivo General de la Nación (AGN) y otros autores.

El concepto de ciclo de vida de los documentos electrónicos está experimentando una rápida evolución en la industria de la información. La base de este concepto radica en la idea de la cadena de valor que posee una determinada información desde su creación hasta su posterior acceso, en mayor o menor medida. A lo largo de estos accesos, la información atraviesa una serie de procesos cuya finalidad es agregar valor para aquellos que la utilizarán hasta que cumpla su función por completo (Cantone, 2012).

En la (LGA, 17/09/2023, a. 4, f. XIV) se define como ciclo vital "a las etapas por las que atraviesan los documentos de archivo desde su producción o recepción hasta su baja documental o transferencia a un archivo histórico".

Por otro lado, Quintos et al. (2022), en el *"ABC de términos archivísticos"* detallan las fases del ciclo de vida desde que se producen los documentos hasta que se determina su destino final como sigue:

- Fase activa: cuando son recibidos o producidos en el ejercicio de las atribuciones y el desempeño de las funciones que realiza la institución. Estos documentos se encuentran el Archivo de trámite, es decir, en el área que los produce.
- Fase semiactiva: es el periodo de vida de los documentos cuando el asunto o trámite está concluido y se cierra el expediente porque dejan de ser útiles para el trabajo y las funciones cotidianas del área; sin embargo, deben mantenerse disponibles para su consulta con fines informativos, aclaratorios, de evaluación o de auditoría. Por este

motivo, se realiza la transferencia primaria, para pasar la documentación del archivo de trámite al archivo de concentración de la institución.

- Fase inactiva: es el periodo final de vida de los documentos que cuentan con valores secundarios (informativo, evidencial y testimonial) y relevancia social, científica o tecnológica. Estos documentos se consideran patrimonio documental y, por medio de una transferencia secundaria, pasan del archivo de concentración al archivo histórico para su resguardo permanente y para su consulta pública directa.

A partir de lo abordado en este capítulo, podemos sintetizar que el enfoque de este trabajo se centra en la **conservación del archivo histórico**; es decir, de los documentos en su fase inactiva, generado por los sujetos obligados por la **Ley general de Archivos** durante el período especificado en el Catálogo de Disposición Documental (CADIDO), que comentaremos en secciones posteriores.

Adicionalmente, en la Figura 1 se muestra un resumen a grandes rasgos del proceso para generar los procedimientos para la conservación del archivo digital en poder de una institución pública; indicando en qué actividades recaen los temas que se desarrollan a lo largo de esta propuesta.

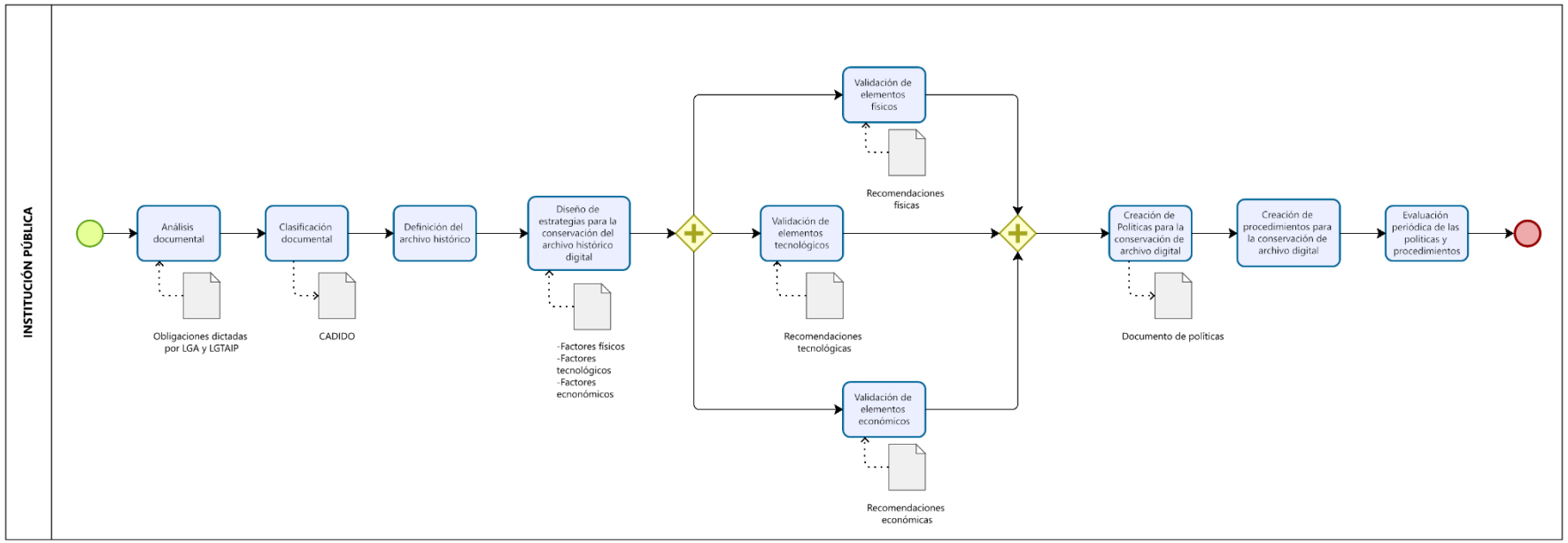

Figura 1 Incidencia en el proceso de elaboración de políticas de conservación

CAP II: Conservación de documentos de archivo digital

Situación en México

El artículo 6° de la (Constitución Política de los Estados Unidos Mexicanos [CPEUM], 20/01/2024, art. 6,) establece que "Los sujetos obligados deberán documentar todo acto que deriven del ejercicio de sus facultades, competencias o funciones" y que "deberán preservar sus documentos en archivos administrativos actualizados". Asimismo, se destaca que, al interpretar el derecho de acceso a la información, deberá primar el principio de máxima publicidad.

Las dos leyes fundamentales que constituyen la base de este trabajo en el ámbito de transparencia y archivos son:

Ley General de Transparencia y Acceso a la Información Pública (LGTAIP) (última reforma DOF 20-05-2021)

Cuyo objetivo es establecer los principios, bases generales y procedimientos para garantizar el derecho de acceso a la información en posesión de cualquier autoridad, entidad, órgano y organismo de los poderes Legislativo, Ejecutivo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad de la Federación, las Entidades Federativas y los municipios. (LGTAIP, 20/01/2024, art. 1)

Ley General de Archivos (última reforma DOF 19-01-2023)

> Que tiene por objeto establecer los principios y bases generales para la organización y conservación, administración y preservación homogénea de los archivos en posesión de cualquier autoridad, entidad, órgano y organismo de los poderes Legislativo, Ejecutivo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad de la federación, las entidades federativas y los municipios.
>
> Así como determinar las bases de organización y funcionamiento del Sistema Nacional de Archivos y fomentar el resguardo, difusión y acceso público de archivos privados de relevancia histórica, social, cultural, científica y técnica de la Nación. (LGA, 20/01/2024, art. 1)

El artículo 37 de la LGA indica que los sujetos obligados deberán cumplir los plazos de conservación establecidos en el CADIDO y que en ningún caso deben exceder los 25 años. (LGA, 12/03/2024, art. 37). Además, la LGA considera el "conjunto de documentos de interés público, histórico o cultural, que se encuentran en propiedad de particulares, que no reciban o ejerzan recursos públicos ni realicen actos de autoridad en los diversos ámbitos de gobierno". (LGA, 26/01/2024, art. 4, fr. IX). No obstante, estos documentos no serán objeto de estudio en el presente trabajo.

De acuerdo con Voutssás (2015), la implementación de las leyes mencionadas ha generado la necesidad para las instituciones gubernamentales de organizar sus archivos de manera más profesional. Esto es esencial para cumplir con los requisitos establecidos por dichas leyes y poder responder de manera efectiva a sus disposiciones.

Catálogo de Disposición Documental

> Formato en el que se registran todas las atribuciones de una institución (secciones documentales) y los procesos (series documentales) que ayudan a cumplir con estas atribuciones, en los cuales se produce documentación que se integra en expedientes. En este formato se indican los valores documentales (la utilidad o el uso que tiene el documento), la vigencia (durante cuánto tiempo tiene efecto) y los plazos y medidas de conservación (el tiempo que debe permanecer en el archivo de trámite y de concentración, así como la manera en que pasará al histórico) (Quintos et al., 2022, p. 13).

No es objeto de este trabajo detallar las fases para elaborar el CADIDO, sin embargo, resumiendo lo descrito en el "Instructivo para la elaboración del Catálogo de Disposición Documental" (AGN, 2012, págs. 10 a 15):

1. Identificación: investigar y analizar las características de los elementos clave que componen la serie documental, la función, el sujeto productor y el documento de archivo.
2. Valoración: analizar y determinar los valores primarios (administrativo, legal, fiscal y contable) y secundarios (informativo y evidenciales o testimoniales)de la documentación para establecer plazos para el acceso, la transferencia, la conservación o la eliminación.
3. Regulación: elaborar e integrar en un formato electrónico susceptible de actualizarse permanentemente el Catálogo de disposición documental determinando con toda claridad los plazos de conservación y las técnicas de selección.

4. Control: validar y aplicar el Catálogo de disposición documental.

Modelo OAIS

Como ya vimos, la preservación de los documentos digitales es más complicada a causa de que la obsolescencia de los soportes es más rápida, la seguridad implica más atención de la que generalmente se le presta, no se tiene un correcto proceso desde la generación de los documentos. Ignorar los problemas planteados por la preservación de la información en forma digital conduciría inevitablemente a su pérdida (Mundet & Carrera, 2016).

Es en estas problemáticas que sienta sus bases OAIS: Sistema de Información de Archivo Abierto; (Térmens Graells, 2013) explica que es un modelo teórico que indica qué funciones han de soportar los sistemas de preservación digital, sim importar qué tipo de datos custodian ni a qué tipo de actividad u organización se refieren. Además, describe los bloques que lo componen mostrados en la Figura 2 (p. 34-39):

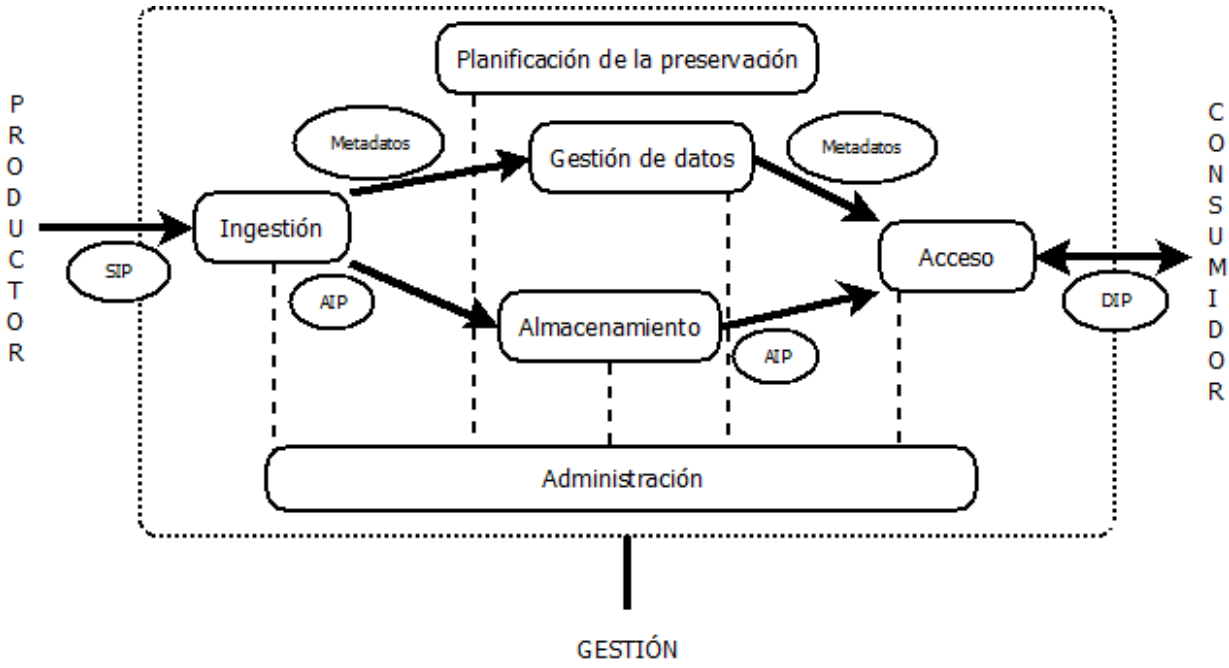

Figura 2 Esquema funcional del modelo OAIS

1. **Ingestión.** A los ficheros que llegan de los productores se les aplica una serie de controles antes de ingresarlos al sistema de preservación. Algunos controles son:
    a) Control de procedencia e integridad: no faltan ni sobran ficheros y estos no se han corrompido desde su origen.
    b) Control antivirus: Los ficheros no contienen virus.
    c) Control de formatos: identificar de forma clara el formato y versión de cada fichero.

Después de la ingestión el sistema extrae metadatos técnicos del fichero y crea una firma digital, estos son enviados al proceso de *Almacenamiento* mientras que los metadatos son enviados a *Gestión de datos*.

2. **Almacenamiento.** Proceso encargado del almacenar físicamente los ficheros de datos. Está controlado por protocolos de copias de seguridad y redundancia de datos.

3. **Gestión de datos.** En este proceso se mantienen los metadatos de los ficheros: los creados durante la ingestión y los que se generen a lo largo de la vida del fichero. Tiene por objetivo disponer las informaciones que puedan facilitar la conservación y uso de cada fichero; es importante registrar todas las incidencias que sufra a lo largo del tiempo.
4. **Acceso.** Se han de habilitar procedimientos que permitan el acceso de los usuarios a los contenidos preservados. Aquí es preciso recordar dos puntos importantes:
    a) Que determinados datos y documentos hayan sido preservados no significa que vayan a ser de libre acceso en el futuro. En *Acceso* se deberán integrar políticas de derechos de acceso a los contenidos pertinentes para cada usuario.
    b) Los formatos en que fueron almacenados los ficheros no tienen por qué ser los mismos en los que el usuario del futuro consulte el contenido. A nivel técnico, se deberán disponer de los mecanismos para migrar los formatos y proporcionar, si es necesario, los visores o el software cliente para abrir los ficheros.
5. **Preservación.** Los responsables de un sistema de preservación deben mantener una vigilancia tecnológica que los alerte sobre la obsolescencia, fin de vida de un formato y la necesidad de migrar a otro formato; de problemas en la operatividad de un formato o software de la disponibilidad de nuevas herramientas de visualización o de emulación, etc. En *Preservación* también deberá considerarse la actualización o migración del propio sistema de preservación, pues este también está sujeto a software y hardware que se vuelve obsoleto.
6. **Servicios comunes.** Este proceso es de soporte técnico a los anteriores.

OAIS también define cómo se mueven los datos entre cada uno de los bloques de procesos; ello porque los bloques pueden estar constituidos por diferentes sistemas informáticos e incluso en ubicaciones físicas diferentes.

- SIP (*Submission Information Package*) o Paquete de Información Enviada. Incluye los ficheros de datos que se envían al sistema de preservación, acompañado de aquellos metadatos que puedan ser útiles para comprobar la integridad y autenticidad de estos ficheros.
- AIP (*Archival Information Package*) o Paquete de Información de Archivo. Este tipo de paquete tiene una composición y función parecida al anterior, pero aplicadas a la interacción entre los bloques de ingestión y almacenamiento, a fin de asegurar que los ficheros validados en la ingesta son los mismos que se almacenan.
- DIP (*Dissemination Information Package*) o Paquete de Información de Diseminación. Incluye los ficheros que se entregan a un usuario como respuesta a una petición de consulta. Es posible que también se entregue alguna advertencia sobre los usos permitidos sobre estos datos.

De acuerdo con el propio documento que lo explica, (*Reference Model for an Open Archival Information System (OAIS)*, 2002) este modelo de referencia no especifica un diseño ni una implementación. Cada organización puede agrupar y distribuir las funcionalidades de maneras diferentes. Además, puede ser aplicado a cualquier archivo. Está dirigido a organizaciones que tienen la necesidad de tener la información disponible a largo plazo.

El modelo OAIS, incluidos los conceptos de modelización funcional y de la información, son relevantes para la comparación y el diseño de instalaciones que almacenan información de forma temporal, por dos razones:

- Si se tiene en cuenta el rápido ritmo de los cambios tecnológicos, existe la posibilidad de encontrar que parte o la mayor parte de la información en instalaciones pensadas para uso temporal, en realidad requieran atención para su conservación a largo plazo.
- Aunque algunas instalaciones que almacenan información pueden ser temporales, parte o la totalidad de la información contenida podría necesitar conservarse indefinidamente.

Factores físicos de la conservación de documentos de archivo digital

En este apartado, se aborda la conservación desde la perspectiva de la seguridad de las instalaciones físicas donde se almacenan los documentos de archivo digital. Aunque pueda parecer un tema trivial, la realidad es que a menudo se presta menos atención a la seguridad física, a pesar de ser tan crucial como la seguridad lógica. La seguridad física busca prever amenazas como desastres naturales, desastres causados por el hombre o sabotajes como robo o fraudes (Cebrián, 2014, p. 83).

Por lo tanto, se deben tener en cuenta los siguientes aspectos de las instalaciones físicas para garantizar una mayor seguridad de los dispositivos de almacenamiento que contienen los documentos de archivo digital: (Olguín, 1997, págs. 79-102)

- Necesidades de espacio: espacio para archivar los dispositivos de almacenamiento en el centro de datos.

- Disposición en planta: ubicación de la bóveda de almacenamiento.
- Capacidad del equipo de aire acondicionado: Debido al calor generado por los distintos dispositivos de cómputo, es necesario contar con aire frío durante todo el año.
- Condiciones de temperatura y humedad: Rango de temperatura de 18 a 22 grados centígrados. Humedad relativa (HR): 50% ± 5%.
- Protección contra incendios: el centro de datos debe estar en un edificio o habitación resistente al fuego. El techo de la sala de almacenamiento debe ser impermeable y se debe considerar un sistema de drenaje en el piso firme. Así como contar con sistema de detección de humo.
- Almacenamiento de información: los dispositivos de almacenamiento se deberán almacenar en una habitación separada con acceso al centro de datos. Esta habitación debe estar equipada con todos los dispositivos de seguridad posibles, tanto para condiciones ambientales como para extinción de incendios, con una garantía de 10 horas porque la información almacenada tiene más valor que el mismo equipo de cómputo.

Factores tecnológicos de la conservación de documentos de archivo digital

Obsolescencia tecnológica

En la literatura generalmente podemos encontrar dos enfoques de la obsolescencia tecnológica. Uno se refiere a una técnica por la que, según Moncada (2023), un fabricante analiza y estima la duración limitada de vida de un producto electrónico o componente,

desarrollándolo con base en ese periodo temporal predefinido. Esto deriva en que el producto queda obsoleto (no inservible) ante otro producto que ofrece mejoras.

El otro enfoque refiere que la obsolescencia es producida por el desgaste físico del producto donde influyen factores como la frecuencia y condiciones de uso. Esto se conoce como "obsolescencia absoluta funcional" (Granberg, 1997),

La obsolescencia de medios de almacenamiento documental, como CD y discos duros, cobra importancia al considerarla en el marco del CADIDO de cada organización. Es crucial garantizar que los archivos almacenados en estos soportes estén disponibles para su consulta cuando sea necesario y dentro del período de conservación establecido en el CADIDO. Es normal que se piense en cuánto va a durar, en términos temporales, un CD o un disco duro, pues durante mucho tiempo la conservación de estos soportes se guiaba por la consideración de la duración de los soportes en papel. En los últimos años, ha surgido un cambio en la perspectiva al considerar los soportes de manera más independiente de sus predecesores, centrándose cada vez más en el verdadero desafío de los medios tecnológicos actuales: la obsolescencia tecnológica (Voutssás, 2009. p. 69).

No se sugiere ni se aconseja abordar la obsolescencia mediante la compra de los productos más recientes cada que salen al mercado. Esta práctica resulta costosa, poco rentable para la organización y, a largo plazo, tiene repercusiones negativas en términos de sostenibilidad ambiental. Por el contrario, se recomienda: Go4IT Solutions (2023)

- Examinar los sistemas disponibles en la compañía con el objetivo de identificar posibles problemas futuros. Esta evaluación permite preparar de manera anticipada un plan de actualización que aborde cualquier eventualidad que pueda surgir.

- Disponer de una estrategia completa de mantenimiento; esta es una de las mejores maneras de evitar la obsolescencia tecnológica. Además, dedicar tiempo al mantenimiento de componentes específicos proporciona la ventaja adicional de identificar problemas de manera preventiva, incluso antes de que se manifiesten.
- Considerar el uso de productos de código abierto, pues posibilitan una frecuencia de actualizaciones más elevada, sin costos asociados. También facilita la implementación de una infraestructura más eficiente y escalable. Al no depender de licencias, se elimina la restricción impuesta por criterios económicos, permitiendo al equipo técnico buscar la mejor solución posible sin limitaciones financieras.
- Contar con la asistencia de especialistas en la modernización de sistemas. Estos profesionales se encargan de evaluar la condición de los equipos y las herramientas de software utilizadas por la empresa, determinando si es necesario reemplazarlas de inmediato o en un futuro cercano. Al obtener su ayuda, se obtiene la información esencial para mantener el sistema actualizado y prevenir interrupciones por averías o fallos de software inesperados.

Además de las recomendaciones ya expuestas, es necesario también mantenerse alerta ante los cambios en los soportes para transferir la información que aún esté almacenada en los dispositivos antiguos. Asimismo, dado que los formatos también evolucionan, se recomienda, en la medida en que la tecnología lo permita, realizar la conversión de formatos antiguos a los más actuales. Esto asegura que la información sea visualizable en el futuro (de la Cuadra, 2013, p. 81).

Factores económicos de la conservación de documentos de archivo digital

De acuerdo con Voutssás (2009), puede dar la impresión de que la principal preocupación en la conservación de documentos de archivo digital es exclusivamente un problema tecnológico, pero en realidad abarca diversos aspectos. Entre ellos, el aspecto económico se presenta como crucial para el éxito de estos proyectos.

La "jerarquía de almacenamiento" que se muestra en la Figura 3, donde se destaca que a medida que aumenta la velocidad de acceso a los datos, también lo hace el costo por megabyte (*$/MB*) almacenado. Sin embargo, como mencionamos previamente, este trabajo se enfoca en el archivo histórico de las instituciones públicas y como en este tipo de archivo el acceso rápido no es prioritario, nos referimos a dispositivos de almacenamiento como discos duros (mecánicos o sólidos) y de almacenamiento ópticos (CD).

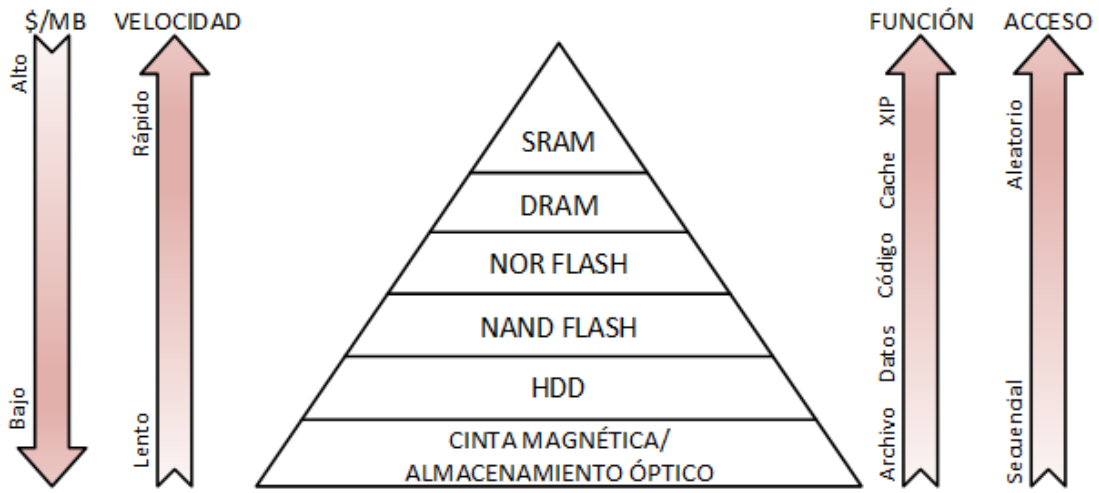

Figura 3 Jerarquía de almacenamiento

Aunque los factores antes expuestos no conforman el todo de lo que influye en la conservación de archivos digitales, sí valen como un punto inicial en camino a observar y

entender qué cosas se deben tener en cuenta al momento de tomar decisiones sobre la estructura, organización y actividades de los sistemas de información; sin dejar a un lado las disposiciones legales emitidas en México. Entendiendo que la conservación es una tarea que no debe tomarse a la ligera, que debe ser analizada, evaluada, rediseñada y retroalimentada periódicamente, pasaremos a presentar algunas recomendaciones físicas, tecnológicas y económicas; así como políticas, que formen parte inicial en el diseño e implementación de los procedimientos adecuados según cada institución.

CAP III: Recomendaciones para la conservación de archivo digital en instituciones públicas

Recomendaciones físicas

Para estas recomendaciones, tomamos en cuenta que el edificio que alberga el centro de datos ya está construido y que debemos adaptarnos a él. Para esto se deben consultar los planos de construcción y de servicios a fin de determinar, con ayuda de un experto en diseño y construcción de centros de datos, el espacio idóneo para la instalación del centro de datos considerando siempre aspectos como la seguridad física y lógica que se requiera para su protección. Sin embargo, si el edificio aún no ha sido construido, es necesario diseñar las instalaciones del centro de datos desde la etapa de planificación del edificio, con la asistencia de un experto en diseño y construcción de centros de datos.

En la Figura 4 se muestra un general del proceso de validación de los elementos físicos indicando en qué fase se deben considerar las recomendaciones físicas aquí hechas.

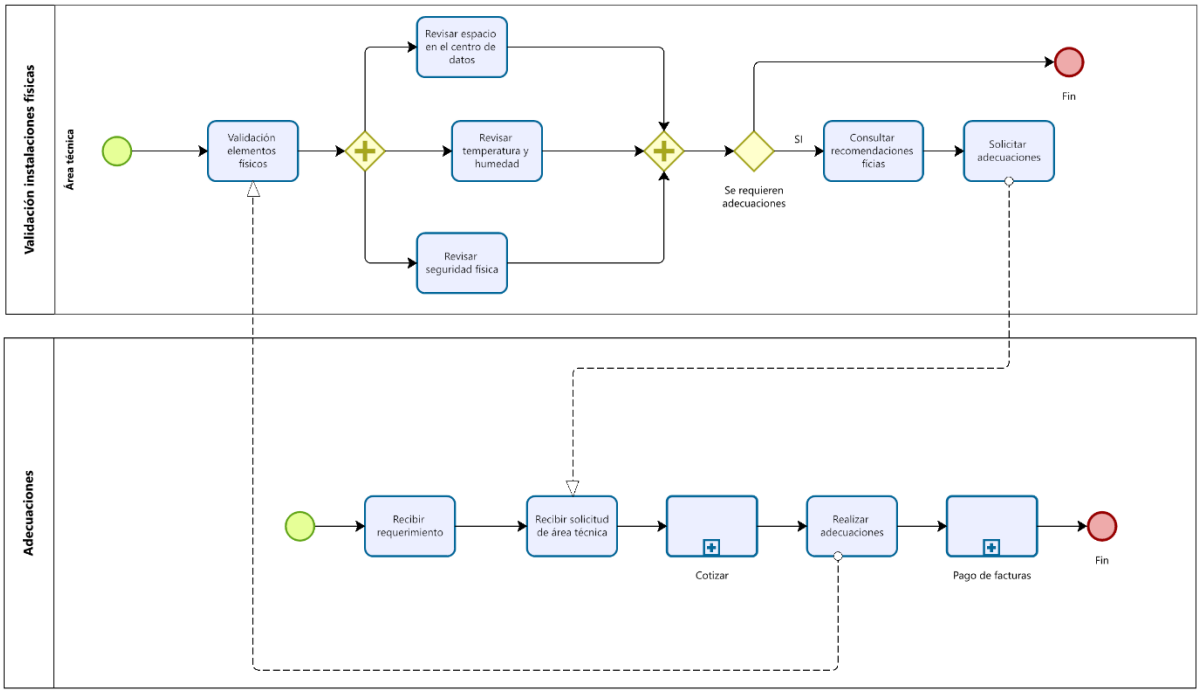

Figura 4 Validación de elementos físicos

Espacio en el centro de datos

El espacio dentro del centro de datos es el primer aspecto por considerar dada su criticidad, ya que debe albergar no solo los elementos habituales como racks con equipos de telecomunicaciones y sistemas de respaldo de energía, sino también la bóveda de almacenamiento o los muebles que contienen los soportes documentales. Además, se requiere espacio para almacenar insumos de los equipos de cómputo como tóner, cables, dispositivos periféricos y otros equipos. Por todo esto es necesario garantizar suficiente espacio para que los operarios puedan realizar sus tareas de manera cómoda y eficiente. Para ello, consideramos:

1. La puerta de acceso al centro de datos debe tener un ancho mínimo de 95cm (Padilla, 2015) y una altura de al menos 220cm para que el ingreso de equipos y racks no presente dificultades.
2. Definir claramente las rutas de acceso y movilidad del personal dentro del centro de datos, evitando la instalación de escalones o rampas (Padilla, 2015). Las rutas deberán estar debidamente identificadas.
3. Definir claramente la localización y área dentro del site para el almacenamiento de insumos de cómputo (Olguín, 1997). Considerar las dimensiones de los muebles por adquirir, así como una "simulación" de la distribución de los mismos.
4. Definir claramente la ubicación y el tamaño de la bóveda de almacenamiento, la cual debe estar separada del centro de datos principal. Además, establecer cómo se accederá a esta bóveda desde el centro de datos (Olguín, 1997; Padilla, 2015).

Temperatura y humedad

Considerar que este tema no impacta directamente a la preservación de los documentos digitales es un error muy común pues este tema ha sido de gran debate en los últimos años ya que existe una gran preocupación sobre la duración de los soportes actuales, los cuales, en general, no son más duraderos que los anteriores a la electrónica (Voutssás Márquez, 2009). La Tabla 3**¡Error! No se encuentra el origen de la referencia.** muestra la duración en años de algunos soportes digitales en función de la humedad y temperatura.

Humedad Relativa Dispositivo | Temperatura	25% H.R. 10° C	30% H.R. 15°C	40% H.R. 20 °C	50% H.R. 25°C	50% H.R. 28°C
Cinta Magnética D3	50 años	25 años	15 años	3 años	1 año
Cinta/Cartucho Magnético	75 años	40 años	15 años	3 años	1 año
Cd-ROM / DVD	75 años	40 años	20 años	10 años	2 años
Cd-R	30 años	15 años	3 años	9 meses	3 meses

Tabla 3 Duración de soportes de almacenamiento en función de humedad y temperatura

Los equipos de aire acondicionado se pueden dividir en dos grupos: de confort, diseñados para la comodidad de las personas; y de precisión, diseñados para operar en ambientes determinados. Para el caso de centros de datos es inevitable cuestionar qué equipo de precisión es el más apropiado teniendo en cuenta el espacio y el presupuesto disponible. Sin embargo, el asegurar la continuidad y confiabilidad del servicio y los archivos digitales es justificación suficiente para cualquier inversión (Suarez Cruz et. al., 2019, 135).

¿Es una buena opción utilizar equipos de aire acondicionado de confort para enfriar los cuartos de equipos? Suarez (2019) explica que el porcentaje de calor sensible (el que se genera en equipo eléctricos y aumenta la temperatura del aire a su alrededor) que puede extraer un equipo de precisión ronda el 95% mientras que uno de confort está entre 60% y 70%. Esto desperdicia hasta un 30% de su capacidad pues el equipo intenta extrae el calor latente (asociado con la humedad en el aire y la transpiración humana) que no se está generando y que puede resultar en una disminución de la humedad del aire; es decir, aumenta el aire seco, que se traduce en carga estática que puede dañar los equipos (p. 138).

Aunque muchos equipos pueden funcionar fuera de los rangos de temperatura y humedad recomendados, es importante tener en cuenta que prolongar estos períodos de trabajo puede acortar o incluso poner fin a la vida útil de los equipos. Se recalca la recomendación de mantener niveles óptimos de temperatura y humedad en el centro de datos para reducir fallos

en los equipos y proporcionar un ambiente cómodo de trabajo para los operarios. Estos niveles óptimos se sitúan entre los 21-23 °C de temperatura y el 40-50% de humedad relativa (Postigo, 2020, p. 43).

Seguridad física y ambiental

La seguridad es tema importante en la conservación de los soportes documentales, más aún cuando las catástrofes naturales suelen ser causa de pérdidas totales de la información. Aunque no son predecibles sí hay medidas, de acuerdo con la situación que se presente, para anticiparse a sus efectos y aminorar los daños provocados a los documentos (Almarza y González, 2019).

El área de tecnología de la institución debe diseñar y difundir entre sus colaboradores un Plan de Recuperación ante Desastres (DRP por sus siglas en inglés) que describa los procedimientos y herramientas necesarios para restaurar los sistemas de la institución después de un desastre.

Protección contra incendios

Debe existir un programa de protección contra incendios que de acuerdo con el estándar NFPA (*NFPA LiNK® - 2024 NFPA-76 - Chapter 4 Risk Considerations*, 2024) se establece tomando en cuenta cuatro factores:

1. Amenaza de exposición a los ocupantes, público en general y a la propiedad debido a un incendio en, junto a o dentro de las instalaciones.
2. La importancia de la continuidad del servicio de telecomunicaciones para respaldar la seguridad pública a través de comunicaciones de emergencia (como el 911), transmisión de video de operaciones médicas críticas y otros datos vitales.

3. Los métodos empleados por un proveedor de servicios como parte de una estrategia de gestión de riesgos o continuidad del negocio permiten que el servicio siga siendo viable durante y después de un evento, o que pueda ser reemplazado o restaurado.
4. La posibilidad de que una estrategia de protección determinada resulte en una interrupción del servicio o inhiba la capacidad del proveedor de servicios para restaurar el servicio de manera oportuna después del evento.

Por otro lado, referente a la construcción del espacio que alberga el centro de datos y la sala de almacenamiento de los soportes documentales del archivo histórico.

- Todas las paredes interiores deberán ser de construcción no combustible o de combustible limitado proporcional a la exposición, pero no menos de 1 hora (*NFPA LiNK® - 2024 NFPA-76 - Chapter 8 Fire Protection Elements*, 2024). Si el centro de datos tiene una o más colindancias con un edificio susceptible de incendio, se recomienda el uso de ventanas irrompibles para mejorar la seguridad tanto del personal como de los equipos.
- El centro de datos no debe ubicarse junto, debajo o encima de áreas donde se procesen, fabriquen o almacenen materiales inflamables o explosivos.
- Se instalarán detectores de humo puntual o puertos para monitorear el aire que circula en el centro de datos (*NFPA LiNK® - 2024 NFPA-76 - Chapter 8 Fire Protection Elements*, 2024).
- Se deben proporcionar extintores portátiles listados y adecuados para su uso en equipos de telecomunicaciones energizados.

En la protección contra incendios, la prevención es la principal forma de combatir un incendio antes de que ocurra, además de las medidas mencionadas anteriormente. Por lo

tanto, según lo establecido en (*NFPA LiNK® - 2024 NFPA-76 - Chapter 9 Fire Prevention*, 2024), mencionamos las principales acciones a tomar para prevenir un desastre de este tipo:

- Los materiales combustibles, como materiales de embalaje y suministros de oficina, no se almacenarán en áreas que expongan equipos de telecomunicaciones críticos y componentes relacionados, a menos que estos materiales estén ubicados en gabinetes no combustibles o dentro de áreas de equipos que no sean de telecomunicaciones provistas de sistemas de extinción de incendios.
- Las áreas alrededor del exterior de la instalación deberán estar libres de combustibles.
- No se permitirá fumar, transportar o depositar cualquier sustancia encendida o ardiendo en equipos de telecomunicaciones y áreas de soporte del edificio y en todas las áreas adicionales identificadas por la administración local como un riesgo para la operación de la red.
- Los cables de extensión eléctricos se utilizarán sólo cuando sea necesaria una conexión flexible y temporal, y nunca para cableado permanente. No se permitirán cordones debajo de alfombras, tapetes o tapetes para sillas.
- Todos los empleados de la institución recibirán información sobre las políticas, procedimientos y riesgos de seguridad contra incendios y para la prevención de incendios.

Aunque nos centramos en los dispositivos de almacenamiento con memoria no volátil, es decir, aquellos que retienen la información incluso sin suministro eléctrico, no dejamos la oportunidad para destacar la importancia de contar con una planta generadora de energía eléctrica para emergencias. Esto debido a que los controles de acceso y la iluminación de la sala no pueden permitirse estar fuera de funcionamiento, asegurando así la seguridad en ella.

Además, un sistema redundante de suministro eléctrico puede ayudar a prevenir problemas como pérdida de ingresos, pérdida de productividad y daño a la reputación de la organización pues los centros de datos son servicios críticos y es fundamental que se garantice su funcionamiento aún después de un fallo eléctrico (El Generador De Energía Adecuado Para La Infraestructura De Un Centro De Datos., 2023).

Recomendaciones tecnológicas

La LGA establece que los sujetos obligados deben adoptar medidas y procedimientos para proteger la información, independientemente del medio en el que se encuentre. Esto incluye la protección de la tecnología utilizada para administrar y conservar los archivos contra la obsolescencia tecnológica a través de actualizaciones, políticas de seguridad, gestión de riesgos, seguridad física y ambiental (LGA, 07/05/2024, a. 60).

En la Figura 5 se muestra un general de las acciones a realizar para aplicar las recomendaciones tecnológicas aquí presentadas.

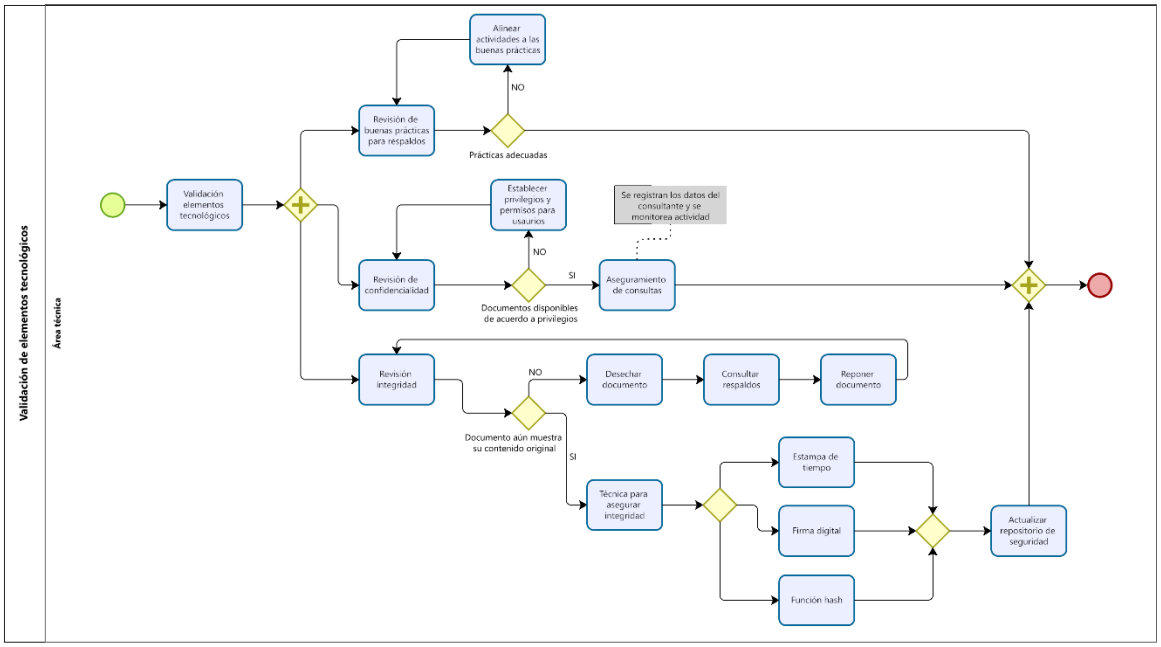

Figura 5 Validación de elementos tecnológicos

Para abonar a las acciones que las instituciones deben realizar para cumplir con lo establecido en la LGA, las recomendaciones hechas en esta sección van enfocadas al aseguramiento de los tres principales aspectos de la seguridad de la información: confidencialidad, disponibilidad e integridad.

Respaldos

La confiabilidad de los sistemas de gestión de documentos depende de la creación de copias de la información almacenada en medios seguros, el uso de hardware y medios de almacenamiento que protejan la información de cambios y la capacidad de restituir la información en caso de pérdida, estableciendo una cadena de responsabilidades a través de una política de seguridad de la información (Instituto Colombiano de Normas Técnicas y Certificación, 2019, p. 2-3)

Como buena práctica de la creación de respaldos se tiene la tarea de almacenar los respaldos de la información en una o varias ubicaciones distribuidas. Así, si ocurre algún siniestro en la ubicación principal podemos recuperar la información almacenada desde otra ubicación. Como necesidad para esta tarea, se deben considerar:

- Los medios y recursos mínimos necesarios para el traslado de los soportes documentales que contienen las copias de los respaldos obtenidos.
- Los medios y recursos necesarios para realizar el almacenamiento de las copias de los respaldos obtenidos de manera remota o automatizada.

Confidencialidad

Esta característica tiene que ver con el hecho de que los registros documentales deben estar disponibles siempre, pero sólo para las personas autorizadas, durante las circunstancias y bajo condiciones válidas y preestablecidas. No deberá ser posible obtener ninguna información de los archivos fuera de esas condiciones (Voutssás, 2010)

El aseguramiento de que las consultas al archivo histórico se lleven a cabo conforme las condiciones establecidas por la institución pueden ser ayudadas por una o varias de las siguientes actividades:

- ➔ registro de datos y motivos del consultante
- ➔ carta responsiva por daños a la información
- ➔ supervisión continua del consultante por un responsable del área
- ➔ grabación y monitoreo de las actividades del consultante sobre el equipo utilizado para consultar el soporte documental

➔ límite de tiempo para realizar la consulta solicitada

Disponibilidad

Esta característica no tiene que ver con que el documento deba estar disponible siempre que se quiera acceder a él, sino a la facilidad de acceso al documento. La disponibilidad nos dirá quién, cómo, cuándo y dónde puede accederse al documento de acuerdo con las reglas que cada organización establece (Voutssás, 2010)

Integridad, autenticidad y fiabilidad

Esta es la cualidad que tiene un documento de estar completo en su esencia original. Aun cuando el documento cambie físicamente, si su esencia refleja lo escrito en el original podemos decir que es un documento íntegro. En documentos electrónicos lo que recuperamos es una copia del documento original y es normal que ésta no sea idéntica a la original pues se han modificado con el tiempo, por actualización de formatos, versiones de software y sistemas operativos, etcétera. En este contexto no conservamos documentos digitales, sino la capacidad de reproducirlos una y otra vez (Duranti y Thibodeau, 2005)

En función de la integridad de un documento podremos también establecer su autenticidad ayudándonos de elementos como:

Estampas de tiempo:

Esta estampa constata la existencia de unos datos y que no se han alterado en un periodo de tiempo determinado Es ofrecido por un proveedor de confianza que testifica la existencia de datos electrónicos en una fecha y hora concretos. Además de ayudar en la garantía de integridad de un documento, proporciona validez jurídica al documento toda

vez que prueba que este se ha mantenido inalterable desde que se aplicó este método de seguridad (EDICOM, 2021)

- Firmas electrónicas:

En la legislación mexicana se define como el conjunto de datos y caracteres que permite la identificación del firmante, que ha sido creada por medios electrónicos bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos, la cual produce los mismos efectos jurídicos que la firma autógrafa (Ley de Firma Electrónica Avanzada 30/04/2024, art2, f. XIII).

Firmas digitales

Una firma digital es un sello de autenticación electrónico cifrado en información digital, como mensajes de correo, macros o documentos electrónicos. La firma constata que la información proviene del firmante y no se ha modificado aportando así garantía de autenticidad, integridad y de no rechazo (Microsoft, 2024)

Funciones hash:

Recordemos que el objeto de estudio de este trabajo es el archivo histórico cuyo principal uso es la consulta y ya no su edición; implicando que el contenido de los documentos no tendría por qué modificarse. Ahora bien, ¿basta con guardar los documentos en formatos que no permitan la edición de su contenido, como PDF? Aquí sugerimos el uso de firmas hash como una medida de bajo costo que la propia institución puede implementar para mejorar el aseguramiento de la integridad, autenticidad y fiabilidad de los documentos.

Las funciones resumen, funciones de compresión unidireccional o funciones hash reciben como entrada mensajes de cualquier tamaño y entregan una salida siempre de tamaño fijo (Postigo, 2020, p. 134).

Sepúlveda et al. (2006) señalan que estas funciones pueden escribirse tal que

$$h = f(M)$$

donde *h* es la salida de la función hash y *M* es el mensaje de longitud variable a la entrada. Y que estas funciones deben cumplir las propiedades de

1. Dado *M* es muy fácil calcular *h*.
2. Dado *h* es muy difícil obtener *M* tal que *h=f(M)*.
3. Dado M es muy difícil generar otro mensaje *M'* tal que *f(M')=f(M)*.

Con estas propiedades se asegura la unidireccionalidad y que las funciones sean libres de colisiones.

En el contexto de asegurar la integridad de los archivos digitales, los documentos almacenados, que son mensajes de longitud variable, servirán como entrada a las funciones. La salida de estas funciones será el resultado de la función hash, que llamaremos firma hash. Por lo tanto, al aplicar las propiedades de las funciones hash para garantizar la integridad de los documentos digitales, se tiene lo siguiente:

1. Dado un documento es fácil calcular su firma hash.
2. Dada la firma hash de un documento es muy difícil obtener el documento original.
3. Dado un primer documento es muy difícil generar un segundo documento que tenga la misma firma hash que el primero.

Es difícil no considerar la cantidad de documentos que una institución genera y la magnitud que alcanzaría el registro de todas las firmas hash de cada uno. Por ello, la institución puede optar entre generar la firma hash de cada documento almacenado o la firma hash del soporte en el que están almacenados los documentos. La duración de este proceso variará según la cantidad de gigabytes de almacenamiento disponibles y ocupados.

El software *QuickHash-GUI*, es una herramienta gratuita para el firmado hash, tiene funcionalidades para obtener la firma de un documento, de un directorio con documentos y de una unidad de almacenamiento. También otorga la posibilidad de comparar la firma hash guardada de un documento con una recién obtenida para verificar si han existido cambios en el documento.

Ya sea que se opte por obtener la firma hash de cada documento o la firma del volumen de almacenamiento se debe asegurar que las firmas obtenidas se resguarden de manera segura preferentemente en una base de datos de la que se obtengan respaldo periódicamente.

Recomendaciones económicas

En principio, la parte tecnológica y la parte económica trabajarán de manera conjunta pues orientados con el análisis de los expertos en tecnología, el área económica, como resultado de los análisis pertinentes, decidirá cuál será la inversión destinada a adquirir qué equipamiento para el almacenamiento, consulta, transporte, respaldo y conservación de los archivos digitales.

Las recomendaciones tecnológicas presentadas en la sección anterior no buscan imponer una guía estricta sobre el tema, sino servir como punta para definir correctamente una estrategia

tecnológica para la conservación del archivo digital, que esté dentro de las posibilidades económicas de cada institución.

En las recomendaciones tecnológicas, comentamos la actualización de la tecnología empleada para la conservación como una medida para abordar la obsolescencia tecnológica. Esta actualización deberá realizarse idealmente de forma periódica y respaldada por un plan de mantenimiento y reposición.

De igual manera, como se mencionó en secciones anteriores, no es recomendable la compra de soportes documentales de última generación sin antes haber hecho un estudio de las características de la información a almacenar en el archivo histórico: no es prioridad un tiempo de acceso a la información rápido, la velocidad de escritura es irrelevante en este caso pues una de las características del archivo histórico es que no puede ni debe ser editado.

Por último, se recomienda, en la medida de lo posible, utilizar software libre de licenciamiento para todas las tareas posibles desde que se genera un documento hasta que se cataloga y almacena; para su consulta, migración de soporte o formato, identificación, aplicación del método preferido para asegurar su integridad.

Políticas para la conservación de archivo digital en instituciones públicas

Antes de comenzar, el enfoque general de estas políticas se debe a que el alcance de este trabajo no se centra en una institución en particular; sino a todos los sujetos obligados por la LGA a los que pueda convenir el enfoque de esta propuesta. Por otro lado, aunque se dirigen al área coordinadora de archivos de las instituciones, remarcamos la necesidad de que una vez elaboradas y aprobadas las políticas en esta materia por cada institución en su particularidad, deben ser dadas a conocer a todos los colaboradores sin excepción para poder garantizar el cumplimiento de los procedimientos que de ellas se deriven.

Buenas prácticas de consulta de los archivos digitales

Objetivo: La confidencialidad del documento

Consideraciones:

- La asignación de responsabilidad de los miembros de área administradora de archivos.
- Los privilegios que se otorgan a los miembros del área coordinadora de archivos sobre los documentos; es decir, quién tiene autorización para ver qué.
- El cumplimiento de las condiciones bajo las que se autoriza la consulta de los archivos digitales si y sólo si se cumplen dichas condiciones.
- Los motivos y/o justificación del consultante.

Objetivo: La disponibilidad del documento
Consideraciones:

- Horarios en que estará disponible el archivo digital.
- Espacios destinados a consulta.
- Equipamiento adecuado destinado exclusivamente a consulta de los archivos digitales.
- Configuración de los equipos para consulta que apliquen.
- El uso de software de código abierto en los casos donde aplique.
- Control de acceso de los solicitantes al espacio de consulta.

Objetivo: La integridad del documento
Consideraciones:

- Formatos compatibles de presentación.
- Software adecuado para la lectura de los archivos digitales.
- Control de firmas digitales, firmas hash o firmas electrónicas de los documentos digitales, según sea el caso.

Objetivo: Registrar las solicitudes de uso de los soportes documentales
Consideraciones:

- El registro escrito o digital de los consultantes antes y después de acceder al archivo digital.
- Los privilegios que se otorgan a los consultantes externos al área administradora de archivos sobre los archivos digitales; es decir, quién tiene autorización para ver qué.

Buenas prácticas para la manipulación y de los soportes documentales

Objetivo: La integridad física del soporte documental que aplique

Consideraciones:

- La línea de vida útil de dicho soporte documental (dicho por proveedor o por estudios de mercado).
- Rango de temperatura en la que pueden trabajar los soportes (especificado por fabricante).
- Limpieza del lugar o superficie donde se manipulen los soportes documentales.
- Uso de equipo antiestático (pulsera).
- Área segura de manipulación, alejada de fuentes de fuego, cuartos eléctricos, químicos, gases.

Objetivo: La correcta destrucción de los soportes documentales inservibles o que han terminado su vida útil

Consideraciones:

- Una estación de trabajo y el equipo adecuado exclusivos para formatear correctamente los soportes documentales, si aplica.
- El manejo de posibles residuos químicos.
- El correcto manejo de la basura electrónica generada.
- Asignación de responsables únicos que autoricen la destrucción de los soportes documentales.
- Asignación de responsables que ejecuten la destrucción de los soportes documentales.

Buenas prácticas para el aseguramiento de la vigencia en los formatos de los documentos digitales

Objetivo: La migración de formatos y soportes de los archivos digitales

Consideraciones:

- El uso de software de código abierto en los casos donde aplique.
- La capacitación y actualización del personal responsable de los archivos digitales.
- La "estandarización" de los formatos a utilizar para almacenar los documentos digitales.
- la actualización del software y hardware necesario para la lectura de formatos específicos.
- la retrocompatibilidad entre los formatos y el software y hardware que los soporta.

Recomendaciones de lineamientos para conservación del archivo digital

Estos lineamientos deberán tomar como fundamento las políticas que la institución haya aprobado y que se relacionen con la conservación de los soportes documentales. Asegurando la conservación de estos últimos se da un paso más hacia la conservación de los archivos digitales en resguardo de la institución.

Dicho lo anterior, listamos una serie de lineamientos con base en las buenas prácticas propuestas en la sección anterior.

Lineamientos para la consulta de los archivos digitales

- ☑ todo miembro del área coordinadora de archivos tiene la responsabilidad de salvaguardar los archivos digitales que resguarda la institución en el alcance de sus funciones.
- ☑ los privilegios de cada miembro del área coordinadora de archivos que tiene sobre los documentos digitales no serán los mismos para cada puesto dentro del organigrama del área o de la institución; es decir, para la consulta de los documentos digitales, diferentes miembros de la institución podrán realizar sólo ciertas acciones sobre estos.
- ☑ Se debe aplicar el principio de cero confianza a todo consultante externo a la institución.
- ☑ Toda solicitud de consulta deberá ser aprobada por el área administradora de archivos a través del personal responsable.
- ☑ Las consultas tendrán una duración establecida y supervisada por el encargado en turno de la bóveda de almacenamiento.
- ☑ Los consultantes, sin excepción no podrán ingresar con equipo de cómputo persona ni ningún tipo de dispositivo de almacenamiento externo.
- ☑ Se creará un perfil con permisos reducidos de configuración y lectura en los equipos de cómputo que se utilicen para consulta. Dichos perfiles tendrán bloqueado el uso de puertos USB y unidades de disco si es el caso; es decir, no podrán escribir desde o hacia un soporte documental externo.
- ☑ La reproducción de uno o varios documentos digitales deberá ser llevada a cabo conforme a la legislación vigente.
- ☑ Al ingresar a la bóveda de almacenamiento se debe levantar un registro, sin excepción, de la o las personas que ingresan considerando datos como nombre,

institución de la que proviene (según sea el caso en consultantes ajenos a la institución), hora de entrada y de salida, firma.

- ☑ En caso de una falla, el consultante no podrá manipular el hardware o software utilizado para su consulta, sino que deberá solicitar el apoyo del personal calificado para el soporte técnico de los equipos para consulta.
- ☑ Si aplica, la periodicidad de la obtención de firmas hash, digitales o electrónicas será establecida por el área coordinadora de archivos, así como los métodos para este fin.

Recomendaciones para la manipulación de los soportes documentales

- ☑ En caso de falla en el funcionamiento del soporte documental, se reportará de inmediato al área coordinadora de archivos para que esta a su vez evalúe el daño y determine si el dispositivo debe ser retirado para su destrucción.
- ☑ Al ingresar al área destinada para consultas, la institución deberá proporcionar el equipo antiestático que el consultante debe utilizar durante todo el tiempo de su consulta y que devolverá al salir.
- ☑ La limpieza del área de consulta y de los equipos para este fin deberá realizar sin el uso de químicos o solventes que puedan dañarlos.
- ☑ La destrucción de los soportes documentales deberá quedar constada en un acta que informe el motivo de la destrucción, quién ejecutó la tarea, lugar y fecha en que se realizó.
- ☑ No se deben desarmar ni soportes documentales ni equipos de consulta sin autorización del área coordinadora de archivos a través de su personal responsable.

- ☑ La actualización o instalación de nuevo software deberá realizarse dentro de una ventana de mantenimiento establecida con anterioridad avisando que en ese tiempo no se llevarán a cabo tareas de consulta en el o los equipos involucrados.

CAP IV: CONCLUSIONES

En virtud de lo presentado, se puede concluir que aun cuando diversos conceptos de la archivística pueden ser extrapolados a los documentos digitales, aún se requiere la generación de conocimiento sobre el manejo de archivos digitales no sólo en su producción, manejo, catalogación o valoración sino en su conservación. No basta con "poner bajo llave" los dispositivos de almacenamiento, no basta con usar contraseñas en las computadoras utilizadas en su consulta.

La conservación de los archivos digitales va más allá de tener un cuarto de anaqueles llenos soportes documentales al que sólo unas cuantas personas pueden tener acceso, va más allá de copiar el mismo archivo en una USB y en un SSD y guardarlos en ubicaciones diferentes. La conservación de archivos digitales se debe tomar con seriedad; las instituciones públicas no deben perder de vista que la información es el bien más preciado que pueden tener. Información que dependiendo de su giro puede tener implicaciones importantes para sí mismas, para su entorno, para la población… para el país.

Salvaguardar el contenido de los archivos a través del tiempo no es una tarea de una sola vez. Una institución que cumple con lo estipulado por la LGA sin revisar, evaluar, rediseñar, mejorar y actualizar sus procesos para el manejo de la información digital inevitablemente caerá en un desorden que volverá a la conservación una tarea cara, tediosa e ineficiente trayendo consecuencias adversas para la propia institución.

Por otro lado, la creciente involucración de los sistemas de almacenamiento en la nube plantea otro escenario a considerar: ¿dónde se almacena la información que las instituciones generan? aunque la LGA permite este almacenamiento en la nube, ¿las instituciones que se

sirven de estos servicios cumplen realmente las tareas inherentes como usuarios para garantizar un uso responsable y adecuado?; es decir, ¿los colaboradores cuentan con la capacitación adecuada para elegir, operar y auditar los servicios de almacenamiento en la nube que utilizan?

Entonces, además de lo considerado en este trabajo y que llevó a las recomendaciones presentadas:

- Físicas: de espacio, instalaciones básicas y de seguridad en los centros de datos
- Tecnológicas: apuntando a reforzar la confidencialidad, disponibilidad e integridad de la información
- Económicas: que se relacionan estrechamente con las recomendaciones tecnológicas.

Se propone como líneas adicionales de investigación los siguientes aspectos:

- La integración de una cadena de *blockchain* que considere elementos indicados por el modelo OAIS en relación con el tratamiento de los metadatos de los documentos que se generan, así como de los detalles de las consultas realizadas al archivo histórico.
- Agregaciones al marco legal referente a la conservación de archivo digital que considere las buenas prácticas en el desarrollo, puesta en operación y mantenimiento de los sistemas de gestión de archivo con el objetivo de garantizar la seguridad de la información
- El análisis de la preservación de la información cuando esta haya tenido un origen no humano; es decir, cuando hayan intervenido herramientas de inteligencia artificial en la elaboración parcial o total de los documentos.

Con lo expuesto en este trabajo y retomando a (Rodríguez Reséndiz et al., 2017) aún queda conocimiento por generar en relación a la preservación de la información digital considerándola una consecuencia de la preservación de los soportes documentales. Sirve de poco tener los mejores sistemas de seguridad física y lógica en los centros de datos, si la institución no se preocupa por transmitir el valor que tiene la información con la que trabajan y si el personal encargado o los usuarios no comprenden la importancia de seguir un procedimiento o política en la manipulación de los soportes y la información en sí.

Bibliografía

Almarza Franco, Y., & González García, V. (2019). *Conservación y Preservación en soportes físicos y digitales* (primera). Dirección General de Gestión de la Información y Estudios del INAI.

Alpuche de la Cruz, E., & Bernal López, J. L. (2015). La Institución y la Organización: Un análisis centrado en el actor. *Intersticios sociales*, *10*, 1-29. http://www.scielo.org.mx/scielo.php?script=sci_abstract&pid=S2007-49642015000200002&lng=es&nrm=iso&tlng=es

ASALE, R.-, & RAE. (2022a). *Dato | Diccionario de la lengua española*. «Diccionario de la lengua española» - Edición del Tricentenario. https://dle.rae.es/dato

ASALE, R.-, & RAE. (2022b). *Estándar | Diccionario de la lengua española*. «Diccionario de la lengua española» - Edición del Tricentenario. https://dle.rae.es/estándar

ASALE, R.-, & RAE. (2022c). *Institución | Diccionario de la lengua española*. «Diccionario de la lengua española» - Edición del Tricentenario. https://dle.rae.es/institución

ASALE, R.-, & RAE. (2022d). *Norma | Diccionario de la lengua española*. «Diccionario de la lengua española» - Edición del Tricentenario. https://dle.rae.es/norma

ASALE, R.-, & RAE. (2022e). *Político, política | Diccionario de la lengua española*. «Diccionario de la lengua española» - Edición del Tricentenario. https://dle.rae.es/político

ASALE, R.-, & RAE. (2022f). *Procedimiento | Diccionario de la lengua española*. «Diccionario de la lengua española» - Edición del Tricentenario. https://dle.rae.es/procedimiento

AULA 13—Microprocessadores—Graduação—Wiki do IF-SC. (219d. C., noviembre 12). Instituto Federal Santa Catarina. https://wiki.ifsc.edu.br/mediawiki/index.php/AULA_13_-_Microprocessadores_-_Gradua%C3%A7%C3%A3o

Caballero Muñoz-Reja, I., Gómez Carretero, A. I., Gualo Cejudo, F., Merino García, J., Rivas García, B., & Piattini Velthuis, M. (2018). *Calidad de Datos*. RA-MA.

http://unam.bibliotecasdigitales.com.pbidi.unam.mx:8080/read/9788499647814/index

Camara de Diputados del H. Congreso de la Unión. (2018, junio 15). *Ley General de Archivos*. https://www.diputados.gob.mx/LeyesBiblio/pdf/LGA.pdf

Campardo Numonyx, G., Tiziani Micron, F., & Iaculo Micron, M. (2011). Modern Hard Disk Drive Systems: Fundamentals and Future Trends. En *Memory Mass Storage* (primera, pp. 169-173). Springer.

Camps Paré, R. (2002). *Los Datos: Conceptos introductorios*. UOC Papers. https://www-digitaliapublishing-com.pbidi.unam.mx:2443/visor/5817

Cantone, D. (2012). *Administración de Storage y Backups* (Primera). Alfaomega Grupo Editor.

Carrillo Sánchez, B. E., López García, K. G., & Torres Blanco, J. (2019, marzo). *Modelo de ciclo de vida de la información*. INE, Unidad Técnica de Transparencia y Protección de Datos Personales. https://ine.mx/wp-content/uploads/2021/05/SSPPDP-Modelo-ciclovidainf.pdf

Castañeda de León, L. M. (2004). Interoperabilidad; estándares. *Revista Digital Universitaria*, *5*(10). http://www.revista.unam.mx/vol.5/num10/art67/int67.htm

Cebrían Marín, D. (2014). *Sistemas de almacenamiento: Administración de bases de datos* (Primera). IC. https://ebookcentral.proquest.com/lib/bibliodgbsp/reader.action?docID=4184160

Chiavetano, I. (2019). *Introducción a la teoría general de la administración: Una visión integral de la moderna administración de las organizaciones* (Décima). McGraw-Hill Interamericana. https://ebookcentral.proquest.com/lib/bibliodgbsp/reader.action?docID=5808931

Chornet, V. G. (2014). Criterios ISO para la preservación digital de los documentos de archivo. *Revista CODICES*, *10*(II), 16-16. https://cnb.gov.co/ojs/index.php/codices/article/view/99

CISCO Latam. (2016, junio 28). *¿Qué es la obsolescencia tecnológica?* ¿Qué Es La Obsolescencia Tecnológica? https://gblogs.cisco.com/la/que-es-la-obsolescencia-tecnologica/

Coordinación de la Estartegia Digital Nacional. (2021, agosto 15). *DOF - Diario Oficial de la Federación*.

https://dof.gob.mx/nota_detalle.php?codigo=5628886&fecha=06/09/2021#gsc.tab=0

de la Cuadra Colmenares, E. (2013). *Documentación cinematográfica* (Primera). Universitat Oberta de Catalunya. https://www-digitaliapublishing-com.pbidi.unam.mx:2443/viewepub/?id=29168

Dirección del Sistema Nacional de Archivos. (2012, abril 16). *Instructivo para la elaboración del Catálogo de disposición documental*. Archivo General de la Nación. https://www.gob.mx/cms/uploads/attachment/file/54332/INSTRUCTIVO_PARA_LA_ELABORACI_N_DEL_CAT_LOGO_DE_DISPOSICI_N_DOCUMENTAL.pdf

Duranti, L., & Thibodeau, K. (2006). The Concept of Record in Interactive, Experiential and Dynamic Environments: The View of InterPARES*. *Archival Science*, *6*, 13-68. https://doi.org/10.1007/s10502-006-9021-7

Egaña Baraona, R. (2015). FORTALECIMIENTO INSTITUCIONAL: UNA MIRADA DESDE LA EXPERIENCIA. *XX Aniversario del Congreso CLAD*. https://biblioteca.digital.gob.cl/bitstream/handle/123456789/745/2015%20Fortalecimiento%20Institucional%20-%20Egana.pdf?sequence=1&isAllowed=y

El Generador De Energía Adecuado Para La Infraestructura De Un Centro De Datos. (2023, marzo 30). Cómo elegir el generador de energía adecuado para una infraestructura de un centro de datos. https://bnhgenerators.com/es/how-to-choose-the-right-power-generator-for-data-center-infrastructure/

Fels, A., Falk, B., & Schmitt, R. (2016). *Social Media Analysis of Perceived Product Obsolescence*. *50*, 571-576. https://doi.org/10.1016/j.procir.2016.04.147

Firmas digitales y certificados—Soporte técnico de Microsoft. (s. f.). Recuperado 30 de abril de 2024, de https://support.microsoft.com/es-es/office/firmas-digitales-y-certificados-8186cd15-e7ac-4a16-8597-22bd163e8e96

Hahn, H. (1994). *El gran libro del CD-ROM* (J. C. Cardona Cadirat, Trad.). Marcombo.

Hernández Rangel, M. de J., & Martínez Hernández, M. L. (2019). Desafíos de la información

sistematizada y comunicación en el fortalecimiento de organizaciones públicas. *Universidad de Zulia. Revista de Ciencias Sociales*, *XXV*(4), 51-64. https://produccioncientificaluz.org/index.php/rcs/article/view/30516

InterPARES Project. (2004, febrero 3). *The InterPARES 2 Project Dictionary*. http://www.interpares.org/ip2/display_file.cfm?doc=ip2_dictionary.Pdf&CFID=259655&CFTOKEN=35461332

ISO. (2022). *ISO - Normas*. ISO. https://www.iso.org/standards.html

Leacock, S. (1924). *Elementos de ciencia política*. Victoria. https://biblio.juridicas.unam.mx/bjv/detalle-libro/608-elementos-de-ciencia-politica

Lima, R. S., Medina, F. D. A., & Sierra, L. C. (2006). ESCENARIOS TÍPICOS DE FALLAS DE SEGURIDAD RELACIONADAS CON LA INTEGRIDAD DE DATOS. (Spanish): Servicios Electrónicos Para la Sociedad de la Información. Desarrollo de Grandes Aplicaciones Distribuidas Sobre Internet. *Servicios Electrónicos Para la Sociedad de la Información. Desarrollo de Grandes Aplicaciones Distribuidas Sobre Internet*, 73-81. http://pbidi.unam.mx:8080/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=edb&AN=43861752&lang=es&site=eds-live

Mejía Jervis, T. (2022, febrero 8). *Instituciones gubernamentales: Qué son, características, funciones*. Lifeder. https://www.lifeder.com/instituciones-gubernamentales/

Micheloni, R., Marelli, A., & Eshghi, K. (2013). *Inside Solid State Drives (SSDs)*. Springer Nature.

Moncada, A. (2023, mayo 29). *OBSOLESCENCIA TECNOLÓGICA: DAÑOS A USUARIOS Y EMPRESAS*. OBSOLESCENCIA TECNOLÓGICA: DAÑOS A USUARIOS Y EMPRESAS. https://www.vertigopolitico.com/internacional/notas/obsolescencia-tecnologica-danos-usuarios-y-empresas

Mundet, J. R. C., & Carrera, C. D. (2016). Sistema de Información de Archivo Abierto (OAIS): Luces y sombras de un modelo de referencia. *Investigación Bibliotecológica: archivonomía, bibliotecología e información*, *30*(70), 221-247.

https://doi.org/10.1016/j.ibbai.2016.10.010

NFPA LiNK®—2024 NFPA-76—Chapter 4 Risk Considerations. (2024). https://link.nfpa.org/publications/76/2024/chapters/4#ID000760000109

NFPA LiNK®—2024 NFPA-76—Chapter 8 Fire Protection Elements. (2024). https://link.nfpa.org/publications/76/2024/chapters/8

NFPA LiNK®—2024 NFPA-76—Chapter 9 Fire Prevention. (2024). https://link.nfpa.org/publications/76/2024/chapters/9

Olguín, H. (1997). *Organización y Administración de Centros de Cómputo* (primera). Facultad de Ingeniería, UNAM.

Orozco Tenorio, J. M., Santoyo Bastida, B., & Landeros Rosas, M. del R. G. (2015). *Archivos: Transparencia y democracia, retos actuales y futuros*. Simposio de Archivos, México. Distrito Federal. https://iibi.unam.mx/voutssasmt/documentos/prof_arch_enba.pdf

Padilla, E. (2015). *Administración de Centros de Cómputo*. https://www.academia.edu/10310642/Administraci%C3%B3n_de_Centros_de_C%C3%B3mputo

Parro Fernández, I. (2018). *Copias de seguridad y tratamiento de la información* (Primera). Editorial Zumaque.

Postigo Palacios, A. (2020). *Seguridad Informática* (Primera). Ediciones Parainfo. http://www.ebooks7-24.com.pbidi.unam.mx:8080/stage.aspx?il=18108&pg=&ed=

Quintos, M., Zárate, C., & Guzmán, J. (2022). *ABC de términos archivísticos* (Primera). Archivo General de la NAción.

RAE. (2024, enero 19). *Documento | Diccionario de la lengua española (2001)*. «Diccionario de la lengua española (2001)». https://www.rae.es/drae2001/documento

Reference Model for an Open Archival Information System (OAIS). (2002).

Robbins, S., & Judge, T. (2017). *Comportamiento organizacional* (L. Pineada Ayala, Trad.; Decimoséptima). Pearson Educación de México. https://bookshelf-

ref.vitalsource.com/reader/books/9786073239851/pageid/0

Rodríguez Reséndiz, P. O., Ríos Ortega, J., & Ramírez Velázquez, C. A. (2017). *Archivos Digitales Sustentables. Conservación y acceso a las colecciones sonoras y audiovisuales para las sociedades del futuro* (Primera). UNAM, Instituto de Investigaciones Bibliotecológicas y de la Información. https://ru.iibi.unam.mx/jspui/bitstream/IIBI_UNAM/L141/2/archivos_digitales_s.pdf

Serie 27k. (s. f.). Recuperado 13 de marzo de 2023, de https://www.iso27000.es/iso27000.html

Soler Jiménez, J. (2012). *La preservación de los documentos electrónicos*. Universitat Oberta de Catalunya. http://www.digitaliapublishing.com.pbidi.unam.mx:8080/a/20327/la-preservacion-de-los-documentos-electronicos

Suarez Cruz, I. L., Escobar Díaz, A., & Vacca González, H. (2019). Unidades de climatización para centro de datos. *Revista Vínculos*, *16*(1), 128-147. https://doi.org/10.14483/2322939X.15273

Terán Pérez, D. M. (2014). *Administración Estratégica de la Función Informática* (Primera). Alfaomega Grupo Editor, S.A. de C.V.

Térmens Graells, M. (2013). *Preservación digital* (Primera). Universitat Oberta de Catalunya. https://www-digitaliapublishing-com.pbidi.unam.mx:2443/viewepub/?id=28419

Uvalle Berrones, R. (2000). *Institucionalidad y profesionalización del servicio público en México. Retos y perspectivas.* (Primera). Plaza y Valdés.

Ventajas del uso del sello electrónico de tiempo en sus documentos| EDICOM MX. (s. f.). Recuperado 30 de abril de 2024, de https://edicom.mx/blog/ventajas-del-uso-del-sello-electronico-de-tiempo-en-sus-documentos

Voutssás Márquez, J. (2009). *Preservación del patrimonio documental digital en México* (Primera). UNAM, Centro Universitario de Investigaciones Bibliotecológicas.

Voutssás Márquez, J. (2010, abril). Preservación documental digital y seguridad informática. *INVESTIGACIÓN BIBLIOTECOLÓGICA*, *24*(50), 127-155. http://rev-

ib.unam.mx/ib/index.php/ib/article/view/21416/20180

Voutssás Márquez, J., & Barnard Amozorrutia, A. (2014). *Glosario de preservación archivística digital versión 4.0* (Primera). UNAM, Instituto de Investigaciones Bibliotecológicas y de la Información.

Wang, S. X., & Taratorin, alexander M. (1999). *Magnetic Information Storage Technology* (Primera). Academic Press.

Westreicher, G. (2022, enero 19). *Entidad gubernamental*. Economipedia. https://economipedia.com/definiciones/entidad-gubernamental.html