UNIVERSIDAD DE COSTA RICA
FACULTAD DE CIENCIAS SOCIALES
ESCUELA DE HISTORIA
SECCIÓN DE ARCHIVÍSTICA

MEMORIA DE SEMINARIO DE GRADUACIÓN PARA OPTAR POR EL GRADO DE LICENCIATURA EN ARCHIVÍSTICA

MARCO DE EVALUACIÓN PARA SOLUCIONES DE PRESERVACIÓN DE DOCUMENTOS DIGITALES EN COSTA RICA

DIRECTORA: RAQUEL UMAÑA ALPÍZAR

ESTUDIANTES:
MARIANA ALVARADO CRUZ, B20268
JOSÉ HERNÁNDEZ MORALES, B23204
KENNETH MONDRAGÓN CORDERO, B44363
NAZARETH TORRES LORÍA, B46995
JACQUELINE VARGAS LEÓN, B47363

2022

Trabajo final de graduación para optar por la licenciatura en Archivística, presentado el miércoles 23 de marzo de 2022, mediante la plataforma ZOOM, con el siguiente tribunal examinador:

M.Ls. María Teresa Bermúdez Muñoz
Presidenta del Tribunal Examinador

M.Sc. Raquel Umaña Alpízar
Directora

Lic. Kenneth Marín Vega
Profesor invitado

M.Sc. María Gabriela Castillo Solano
Lectora

M.Sc. Alexander Barquero Elizondo
Lector

Sustentantes:

Mariana Alvarado Cruz
B20268

José Hernández Morales
B23204

Kenneth Mondragón Cordero
B44363

Nazareth Torres Loría
B46995

Jacqueline Vargas León
B47363

Dedicatoria

A mi madre, padre y hermanos por el apoyo, amor y compañía brindados en esta etapa, que me ayudaron a cumplir este nuevo objetivo, gracias por ser el mejor equipo que en la vida se puede tener.

-Mariana Alvarado Cruz

A mi mamá por siempre preocuparse por mí para que yo pueda alcanzar una meta más en mi vida, a mis hermanos y sobrina por el apoyo.

-José Hernández Morales

A mi mamá, quien con su amor, esfuerzo y dedicación me permitió alcanzar un objetivo más, gracias por ser un ejemplo de superación y fortaleza.

-Kenneth Mondragón Cordero

A mi madre y a mi padre, por su amor, confianza, apoyo y entrega desmedida, por ser siempre mi lugar seguro y feliz.

-Nazareth Torres Loría

A mi familia, por su acompañamiento y amor incondicional. A mis amigas, por su apoyo y cariño.

-Jacqueline Vargas León

Agradecimientos

A la profesora Raquel, nuestra directora de proyecto, por sus invaluables aportaciones académicas, por su confianza y apoyo en todo momento y por siempre acompañar el proceso de investigación con una actitud amable e inspiradora.

A nuestros lectores, la profesora Gabriela Castillo y el profesor Alexander Barquero, quienes destinaron parte de su valioso tiempo para brindarnos la mejor retroalimentación posible.

A Jorge Sánchez, por su contribución y las recomendaciones brindadas.

A Roberto Taylor por el tiempo y guía para crear la HEI.

A todas las personas que de alguna u otra forma brindaron algún aporte para el desarrollo de este proyecto.

TABLA DE CONTENIDO **N° página**

Tabla de contenido de cuadros **N° página.**

Tabla de contenido de figuras **Nº página.**

Tabla de contenido de gráficos **Nº página.**

Abreviaturas y acrónimos

ADN: Archivo Digital Nacional

AIP: ArchivalInformationPackage

AUROL: Archivo Universitario Rafael Obregón Loría

CISED: Comité Institucional de Selección y Eliminación de Documentos

CNSED: Comisión Nacional de Selección y Eliminación de Documentos

CNTD: Código Nacional de Tecnologías Digitales

DIP: Dissemination Information Package

DPC: Digital Preservation Coalition

DPM: Modelo de Gestión de la Preservación Digital

DRAMBORA: Digital Repository Audit Method Based On Risk Assessment

HEI: Herramienta de Evaluación Integral

ICA: International Council on Archives

ISAAR-CPF: Norma Internacional sobre los registros de autoridad de archivos relativos a instituciones, personas y familias

ISAD-G: Norma Internacional General de Descripción Archivística

ISO: Organización Internacional de Estandarización

InterPARES: The International ResearchonPermanentAuthenticRecords in Electronic System

METS: MetadataEncoding&TransmissionStandar

NAA: National Archives Australian

OAIS: Sistema Abierto de Información de Archivo

PREMIS: PreservationMetadata: ImplementationStrategy

SGD: Sistema de Gestión para Documentos

SGDE: Sistema de Gestión de Documentos Electrónicos

SGDEA: Sistema de Gestión de Documentos Electrónicos de Archivo

SIP: SubmissionInformationPackage

SNA: Sistema Nacional de Archivos

Resumen

Alvarado Cruz y otros. (2022). Marco de Evaluación para Soluciones de Preservación de Documentos Digitales en Costa Rica. Para optar por el grado de Licenciatura en Archivística, Universidad de Costa Rica.

Palabras clave: Preservación digital, marco de evaluación, objetos digitales.

Actualmente las organizaciones están experimentando un acelerado y constante cambio tecnológico, en consecuencia, es cada vez más recurrente que se generen documentos de archivo digitales que requieren de una adecuada gestión y custodia para garantizar su valor jurídico y evidencial durante el tiempo que sea requerido.

Sin embargo, la mayoría de las instituciones y empresas se encuentran adquiriendo sistemas informáticos que no incorporan las funcionalidades necesarias para asegurar la preservación de los objetos digitales a largo plazo, exponiéndose a la pérdida de información y a la imposibilidad de preservar las características de fiabilidad que componen a los documentos de archivo. Es por esa razón, que el presente proyecto de investigación propone un marco de evaluación para soluciones de preservación de documentos digitales.

Bajo esa perspectiva, se constituyó una Herramienta de Evaluación Integral (en adelante HEI) encargada de reunir una serie de requisitos considerados como indispensables y deseables que debe cumplir una solución de preservación de documentos digitales, generando una puntuación con relación al cumplimiento de los requisitos, permitiéndole a las organizaciones tomar una decisión informada y objetiva al momento de elegir entre las diferentes opciones disponibles en el mercado.

Por consiguiente, el presente proyecto de investigación puede tener un impacto directo a nivel económico y legal para las organizaciones que decidan implementar la HEI, pues podrán comprobar la idoneidad de cada una de las opciones evaluadas, teniendo mayor seguridad sobre la inversión realizada y sobre el cumplimiento de las funcionalidades requeridas para la preservación de los documentos digitales.

Introducción

Con la incorporación de las Tecnologías de Información y Comunicación (TIC) en los procesos de trabajo de las organizaciones se ha generado un incremento exponencial de la información digital, este crecimiento desmesurado ha traído consigo una serie de problemas e inconvenientes que inciden directamente en la preservación de los objetos digitales, por lo que resulta indispensable que las instituciones adquieran soluciones para la preservación digital que garanticen el acceso a información fiable durante el plazo que sea requerido.

En ese sentido, el presente proyecto de investigación propone un marco de evaluación que le permita a las organizaciones, públicas y privadas, valorar las funcionalidades de las soluciones tecnológicas destinadas a la preservación digital con base en una serie de requisitos tecnológicos y funcionales, facilitando de esa forma el proceso de toma de decisiones inmersas en la adquisición.

No obstante, la preservación de documentos digitales no sólo debe abordarse desde una perspectiva en donde únicamente se tomen en consideración los factores tecnológicos, pues debe estar acompañada de un conjunto de políticas y estrategias destinadas a prolongar la usabilidad y acceso a los objetos digitales, por lo tanto, también cubre los factores administrativos, económicos y culturales.

Con el propósito de abordar los diversos factores relacionados con el proceso de preservación, se realiza un diagnóstico de la situación en la que se encuentra el Sistema Nacional de Archivos (SNA) en relación a la preservación de los documentos en soporte digital, el cual abarca en primera instancia el análisis del marco normativo nacional que cubre la preservación digital, además se examinan los proyectos de preservación digital desarrollados en el país con el fin de comprender sus aportes y limitaciones, seguido de la presentación de los resultados obtenidos en la encuesta aplicada a las instituciones del SNA que aseguraron tener repositorios para documentos en soportes digitales y expone las diversas opciones disponibles en el mercado de soluciones de preservación y almacenamiento.

A partir del análisis realizado en la etapa del diagnóstico se desprende la evaluación de los riesgos asociados a los objetos digitales en ausencia de la preservación digital sistémica en el SNA, los cuales fueron analizados y valorados en proporción a los niveles de probabilidad y de impacto, obteniendo el grado de criticidad del riesgo y las consecuencias a lasque se está expuesto.

Finalmente, se presenta la Herramienta de Evaluación Integral (HEI) para la adquisición de soluciones para la preservación digital, la cual reúne los requisitos funcionales y tecnológicos que debe cumplir una solución para garantizar la fiabilidad, seguridad y acceso de los objetos digitales custodiados, a los cuales se les asignó un nivel de cumplimiento y se les asoció uno o varios riesgos derivados del análisis anterior.

CAPÍTULO I.

OBJETO DE LA INVESTIGACIÓN

1. Tema

1.1 Título

Marco de evaluación para soluciones de preservación de documentos digitales en Costa Rica

1.2 Justificación

De la mano con el avance vertiginoso que han tenido las Tecnologías de la Información y la Comunicación (TIC) en las últimas décadas, surgen también diversas dudas, inquietudes y preocupaciones, con respecto al futuro acceso y preservación de la información digital.

Actualmente las instituciones están adquiriendo sistemas informáticos incapaces de preservar objetos digitales, dejando ver un peligroso desconocimiento y manejo despreocupado sobre la importancia de la gestión digital preventiva, así como de los procedimientos formales que permiten la preservación y acceso a la información digital a largo plazo.

La preservación digital como actividad formal garantiza el acceso a la información contenida en los documentos digitales a lo largo del tiempo y la permanencia de las características de integridad, autenticidad y accesibilidad; además prevé la gestión de riesgos digitales para la continuidad digital ante la obsolescencia tecnológica.

La obsolescencia tecnológica es un fenómeno que pone en peligro la preservación de los objetos digitales; la rápida evolución tecnológica y de los recursos digitales ocasionan la descontinuación acelerada de soportes de almacenamiento y formatos digitales, provocando pérdida de valiosa información, que repercute en la identidad histórica de una sociedad, en los derechos de los individuos y en la evidencia de los ciudadanos frente al Estado y viceversa.

Tal como lo advierte “La carta sobre la preservación del patrimonio digital” (UNESCO, 2003) y la declaración de Vancouver sobre “La memoria del mundo en la era digital: digitalización y preservación” (UNESCO/UBC, 2012), la preservación de

la información y la continuidad digital se ven amenazadas por la desaparición de los medios de almacenamiento y la evolución de los formatos, haciendo imposible la accesibilidad e integridad de la información digital a generaciones actuales y futuras.

Teniendo presente este panorama, resulta imprescindible disponer de una guía para que las instituciones puedan verificar o evaluar si una solución de preservación digital apunta a la gestión y garantía de acceso por un largo plazo, haciendo uso de técnicas, estándares y estrategias de manera sistémica y, si está adaptada a las circunstancias cambiantes, con el fin de garantizar la seguridad informática, la protección de los datos y el acceso a la información, respetando la normativa nacional.

El reto y los riesgos a los que se enfrentan hoy en día el patrimonio digital de la humanidad y los garantes del acceso a la información son reales, por lo que invisibilizar o no asumir el desafío resulta irresponsable. Debido a esto, surge la presente propuesta, la cual pretende elaborar un marco de evaluación para las soluciones que serán encargadas de la preservación de documentos digitales. El marco de evaluación tiene el suficiente grado de abstracción que le permita tener alcance nacional y además incorpora los principales modelos, estándares, estrategias y mejores prácticas internacionales.

La propuesta resuelve, de alguna manera, el vacío normativo e informacional que existe en el país con respecto a la preservación digital y permite a las instituciones verificar si las soluciones de preservación son idóneas o si por el contrario ponen en riesgo la información digital que custodian.

1.3 Delimitación

1.3.1 Delimitación espacial

La investigación se delimita en Costa Rica, en el sector público y privado, ya que la propuesta del marco de evaluación ofrece una herramienta disponible en línea que facilite la toma de decisiones en cuanto a la adquisición de soluciones de preservación digital.

1.3.2 Delimitación temporal

Esta investigación se delimita temporalmente en el periodo comprendido entre 2012 con la publicación de la Política de Formatos Oficiales de los Documentos Electrónicos Firmados Digitalmente, con la cual se definen las características que conforman los formatos oficiales de los documentos digitales en Costa Rica.

Finaliza en el año 2022, con la propuesta del Marco de evaluación para soluciones de preservación de documentos digitales en Costa Rica.

2. Problema

El documento electrónico nace como consecuencia de un proceso irreversible de la virtualización, que mueve hacia un plano digital la mayoría de las tareas desarrolladas por la humanidad y por consiguiente sus evidencias. En Costa Rica su uso es regulado desde el año 2005 por la Ley 8454 de Certificados, firmas digitales y documentos electrónicos, la cual faculta al Estado y todas las entidades públicas para crear, utilizar y gestionar los certificados, las firmas digitales y los documentos electrónicos.

No obstante, el documento electrónico en el país llega a tener un uso más extendido hasta la segunda década del siglo XXI, directamente relacionado con las acciones del Estado por promover la estrategia de Gobierno Digital y Gobierno Abierto, las cuales buscan aprovechar al máximo las tecnologías de información y comunicación con el fin de agilizar el funcionamiento de las entidades de la administración pública, automatizando los diferentes procesos y coadyuvando a la transparencia y la rendición de cuentas en la función pública.

Además, a raíz de lo anterior muchas instituciones han desarrollado a lo interno programas o políticas hacia oficinas *cero papel*, promoviendo de forma directa el uso del documento electrónico.

Por su parte, el plan maestro de Gobierno Digital de la República de Costa Rica establece también como meta “automatizar y estandarizar el proceso de administración gubernamental e intercambiar la información entre las diversas

agencias gubernamentales para aumentar la eficiencia y la efectividad" (2010, p. 132). Y con el objetivo de dar respuesta a dicha acción estratégica, muchas instituciones públicas han promovido el desarrollo o adquisición de sistemas informáticos que no cumplen con las características y funcionalidades necesarias.

Por esta razón es necesario aclarar que gestionar documentos electrónicos va más allá de sistemas informáticos y procesos automatizados, sí son componentes necesarios, pero no suficientes; por lo que resulta imprescindible establecer estrategias y políticas de preservación e implementar mecanismos de preservación de documentos a largo plazo de manera sistémica, y contar con un repositorio institucional que cuente con requisitos específicos para la gestión y preservación digital, a saber, un sistema de gestión de documentos electrónico de archivo SGDEA

Es claro que el Estado ha promovido el uso del documento electrónico en la administración pública, paralelamente, también ha pretendido aplicar los principios de Gobierno Abierto a través de los cuales busca una mayor participación activa de los ciudadanos en la toma de decisiones, por medio del acceso y uso de los datos y documentos públicos; sin embargo, estos esfuerzos e iniciativas no se han visto reflejadas en garantizar la preservación digital de la información contenida en los documentos de archivo, lo cual termina resultando contradictorio, teniendo en cuenta que el principal objetivo de la preservación digital es permitir el acceso y uso de información fiable a través del tiempo.

La preservación de la información digital es una práctica que se ha tomado con irresponsabilidad e inconsciencia por las autoridades responsables del tema en el Estado costarricense, esto puede ser debido a desconocimiento, desinterés, desinformación o debido al vacío normativo existente a nivel nacional en materia de preservación digital; por lo que se considera un verdadero riesgo y problema, ya que parte de la información digital se debe conservar a mediano, largo plazo o indefinidamente, ya sea debido a obligación normativa o desde la perspectiva práctica, tales como fallos judiciales, sucesión de derechos, historiales médicos, entre otros. Por lo tanto, resulta necesario un trabajo constante e interdisciplinario con el

fin de garantizar los requisitos necesarios e indispensables para la preservación y acceso a la información digital.

De no disponer con estrategias de preservación en un corto plazo el acervo documental de las instituciones podría verse amenazado y correr el riesgo de pérdida de información, pues al Estado no garantizar la aplicación de procesos sistémicos de preservación digital basados en estándares de calidad y en buenas prácticas, está atentando irremediablemente contra la integridad, autenticidad y fiabilidad de la información.

Además, no se trata únicamente de velar por las características de los documentos, sino que gestionar documentos digitales sin una adecuada preservación digital pone en riesgo las bases de un Estado de Derecho, ya que se debe recordar que por definición un documento de archivo, independientemente de su soporte, tiene como misión informar o evidenciar una actividad, llevada a cabo por una organización o individuo en el ejercicio de sus funciones.

Por lo que alterar o perder la información contenida en los documentos, amenaza también los derechos de los ciudadanos, muchos de estos fundamentales e inalienables, ya que en los documentos se pueden plasmar eventos de gran relevancia en la gestión y economía de un país, pero también en la vida de una persona, tal es el caso de la resolución de un juicio, recursos de amparo, la patria potestad de un menor de edad, o bien el expediente clínico que tiene una incidencia directa con las decisiones médicas y por ende en la salud de un individuo.

Así entonces y debido a que los documentos son la base de la transparencia y la rendición de cuentas en las instituciones, así como un instrumento garante de derechos para los ciudadanos, se debe velar por una mejora continua en las actividades y procesos que se estén llevando a cabo, así como garantizar su acceso, integridad y autenticidad a largo plazo.

De lo anterior, se plantearon las siguientes interrogantes como parte del problema de investigación:

¿Son suficientes las medidas establecidas en el marco normativo nacional para garantizar una adecuada preservación de documentos digitales de archivo a largo plazo?

¿Qué criterios técnicos son tomados en consideración, actualmente, por las instituciones públicas para el diseño de estrategias destinadas a la preservación de documentos digitales?

¿Qué consecuencias pueden producirse en las instituciones públicas que generan y tramitan documentos digitales, al no disponer de las especificaciones técnicas que permitan regular y fiscalizar la labor de los actuales proveedores del servicio de preservación de documentos digitales?

A raíz de las preguntas anteriores, se evidencia que uno de los temas que más incertidumbre genera es establecer un parámetro para definir la idoneidad de un producto como herramienta para la preservación digital; aspecto no resuelto en Costa Rica.

Finalmente, al no disponer el país de guías detalladas y de normativa actualizada, la creación de un marco de evaluación de preservación digital permitió reunir los requisitos, las características, las estrategias, las mejores prácticas y los estándares internacionales con los que debe cumplir una organización para garantizar que la información se está preservando de manera sistémica, y que está preparada para hacer frente a los riesgos que implica la obsolescencia tecnológica y de formatos y a los desafíos propios de la era digital.

3. Objetivos

3.1 Objetivo general

Proponer un marco de evaluación para soluciones de preservación digital en Costa Rica, que permita a las organizaciones disponer de una guía para valorar la pertinencia en la adquisición de soluciones de preservación digital que garanticen el acceso, autenticidad, integridad y disponibilidad de la información a largo plazo.

3.2 Objetivos específicos

- Realizar un diagnóstico en materia de preservación digital en Costa Rica, mediante la revisión y evaluación de normas, políticas, estrategias y repositorios existentes que permitan identificar la situación actual con respecto a la preservación digital en el país.

- Realizar una evaluación de riesgos asociados a la preservación digital que permita disponer de los criterios de evaluación necesarios para conocer cuáles son las vulnerabilidades de la información digital en el Sistema Nacional de Archivos.

- Establecer los requisitos técnicos necesarios con los que debe cumplir una solución de preservación digital, por medio de una herramienta disponible en línea, que permita a las organizaciones evaluar un sistema de preservación digital.

4. Limitaciones

En el desarrollo de la investigación se presentaron las siguientes limitaciones:

- Del cuestionario aplicado para el diagnóstico de los archivos institucionales que pertenecen al Sistema Nacional de Archivos, en el periodo que estuvo habilitado el formulario, solamente contestaron51 de 74 archivos que formaban parte de la muestra de la población total que respondió afirmativamente a la pregunta No. 68 del Índice de Desarrollo Archivístico

2018-2019, el cual indicaba que si en la institución existen repositorios documentales para los documentos en soporte digital.

- Para el diagnóstico de la situación actual del mercado, con respecto a servicios de almacenamiento y repositorios digitales, se les solicitó a varias empresas privadas e instituciones públicas como el Instituto Costarricense de Electricidad, por medio de un oficio emitido por la Sección de Archivística, información referente a las especificaciones de los servicios que ofrecen, pero ninguna de ellas contestó la solicitud.

5. Estado de la cuestión

En este apartado se abordan los diversos avances y aportes vinculados con el tema de investigación, se analizan trabajos o publicaciones que han realizado diferentes autores, con el fin de verificar desde qué perspectivas se ha indagado y el grado de profundidad de lo investigado, detectar vacíos, inconsistencias, así como diversos planteamientos y tendencias existentes, sobre el tema.

Con base en la revisión de las fuentes de información bibliográficas relacionadas con el tema de estudio, se lograron determinar las principales perspectivas plasmadas por diversos autores, tanto a nivel internacional como nacional, sobre el tema de preservación de documentos digitales y su respectiva normalización.

5.1 Ámbito internacional

5.1.1 Normas internacionales

Al hablar de normalización es necesario mencionar a la Organización Internacional de Estandarización (ISO), la cual ha desarrollado estándares internacionales voluntarios, abarcando una amplitud de temas y áreas, entre ellas no escapa el ámbito de la archivística en general y de la preservación digital y la evaluación de la conformidad en particular; así las cosas, conviene hacer mención a las principales normas ISO aplicables a la preservación digital, así como cualquier otra norma que se relacione con el tema de la presente investigación. La información se expone por temas:

I. Gestión de documentos

En respuesta al aumento exponencial de los documentos electrónicos, se ha evidenciado la necesidad de estándares que ofrezcan requisitos mínimos de calidad, para la normalización desde la producción de documentos fidedignos, garantizando su acceso y funcionalidad a largo plazo; lo que se convierte en un insumo medular para garantizar una óptima preservación digital.

La norma de buenas prácticas UNE-ISO 15489-1 fue publicada en primera instancia en el año 2001, sin embargo, se han ido generando nuevas ediciones hasta llegar a la versión del año 2016. La norma proporciona las directrices para la gestión de documentos en las organizaciones, mediante el establecimiento de principios y requisitos básicos para que un sistema de gestión documental mejore sistemáticamente la producción, mantenimiento, uso y disposición de los documentos, garantizando la autenticidad, integridad, confiabilidad y acceso a largo plazo.

La norma UNE-ISO/TR 26122 IN: 2008, describe la aplicación práctica de la teoría expuesta en la UNE-ISO 15489, es decir, ofrece la orientación para el análisis de los procesos de trabajo para la gestión de documentos.

Por otra parte, se encuentra la familia de normas UNE-ISO 30300, es dedicada propiamente a los Sistemas de Gestión para los Documentos (SGD), brindando las claves para la implementación de un SGD basado en la mejora continua:

- UNE-ISO 30300: 2021. Sistema de gestión para los documentos: Fundamentos y vocabulario. Define el vocabulario a utilizar en el resto de las normas y además justifica el enfoque de la serie de normas 30300.

- UNE-ISO 30301: 2019. Sistema de gestión para los documentos: Requisitos. Propone un sistema de gestión para los documentos basado en la mejora continua.

- UNE-ISO 30302: 2015. Sistema de gestión para los documentos: Guía para la implementación.

Por último, la norma UNE-ISO 16175-1: 2012, se encarga de recopilar los principios y requisitos funcionales en cuanto al software que se utiliza para crear y gestionar documentos electrónicos en entornos de oficina electrónica, mientras que la norma UNE-ISO/TR 15801 IN: 2019 describe las recomendaciones para que los sistemas de gestión de documentos que almacenan y ponen a disposición información almacenada electrónicamente (IAE) lo hagan de una manera fiable y confiable.

II. Metadatos

La creación, gestión y uso de los metadatos en los documentos electrónicos de archivo, es un elemento de gran relevancia dentro de la preservación digital, ya que disponer de un marco de metadatos, facilita no solo el acceso a los documentos, sino también coadyuva a la integridad, usabilidad, acceso y disposición de los documentos y sus relaciones en un contexto determinado.

Una de las principales normas en el campo de los metadatos es la UNE-ISO/TR 23081-3 IN: 2017, la cual se basa específicamente en metadatos para la gestión de documentos, y está estructurada en tres partes, abarcando principios y aspectos tanto conceptuales como de implementación y un método de autoevaluación del marco de gestión de metadatos para la gestión de documentos. Por su parte, es importante rescatar que la norma en cuestión se encuentra relacionada con la norma UNE-ISO 15489 sobre gestión de documentos.

III. Migración y conversión

Preservar documentos digitales a menudo implica la ejecución de los procesos de migración y conversión de formatos digitales; para ello se tiene la norma UNE-ISO 13008: 2013 que estandariza dichos procesos, y permite de manera adecuada y segura garantizar el mínimo impacto negativo al contenido, contexto, estructura de la información resguardada y el acceso por parte de los usuarios, procurando velar que toda acción y actividad que se realice con los documentos quede debidamente registrada. La norma destaca la relevancia que posee una adecuada planificación de las diversas áreas que se encuentran involucradas en procesos de conversión o

migraciones, entendiéndose la parte documental, tecnológica y administrativa de una organización.

IV. Preservación digital

Debido al vertiginoso avance de las Tecnologías de Información y al reto de la obsolescencia de formatos se encuentra el tema de la preservación digital, al cual ISO también ha dedicado esfuerzos para su normalización. Como evidencia de dichos esfuerzos se encuentran la norma UNE-ISO 14721: 2015, la cual define el modelo de referencia para un sistema abierto de información de archivo (OAIS), la norma tiene un doble propósito, conservar la información y facilitar su acceso a través del tiempo.

Open Archive Information System (OAIS), es promovido en un inicio por la *National Aeronautics and Space Administration* (NASA) y que desde el año 2003 se transformó en la Norma ISO 14721: *Space Data and Information Transfer Systems* (OAIS). Este modelo propone encontrar, presentar, comprender e interpretar el documento electrónico a largo plazo por medio del encapsulado y empaquetado de la información.

Asimismo, es importante mencionar la norma UNE-ISO 14641-1: 2015, ya que describe métodos y técnicas que se utilizan para implementar un sistema de información electrónico que optimice la preservación de documentos a largo plazo, así como su archivado, acceso e integridad. En la misma línea, se encuentra la UNE-ISO/TR 18492 IN: 2008 la cual presenta una metodología para la conservación y recuperación a largo plazo de la información electrónica basada en documentos.

V. Repositorios digitales

La preservación digital abarca una gran cantidad de acciones a tomar en cuenta para garantizar el acceso a la información contenida en los documentos digitales, entre ellas, disponer de un repositorio de preservación digital confiable. Un repositorio no es solamente un medio de almacenamiento, ni un programa de gestión de documentos, sino una serie de servicios, mecanismos y acciones que garantizan la preservación y el acceso a la información a mediano y largo plazo.

En cuanto a los requisitos necesarios en los que debe estar basado un repositorio, tanto a nivel de sistema como de operación, para garantizar que los documentos mantengan sus características y se encuentren disponibles a través del tiempo, se encuentra la aplicación del modelo OAIS de la norma antes mencionada, UNE-ISO 14721.

Además, se encuentra la norma UNE-ISO 16363 sobre auditorías y certificación de repositorios digitales de confianza, la norma en cuestión brinda un marco de análisis de la calidad, de la consistencia y de la integridad de la información custodiada en los repositorios, la norma además tiene el compromiso de garantizar el acceso y la conservación de la información contenida a largo plazo. Por otra parte, se encuentra la norma UNE-ISO/TR 17068, la cual señala los requisitos para un repositorio de terceros de confianza, apoyando el servicio de custodia de información de una manera íntegra, auténtica y confiable.

VI. Seguridad de la información y gestión de riesgos

La ISO también ha creado normas para la seguridad de la información y la gestión de los riesgos:

- UNE-ISO/IEC 27000, 27001 y 27002. Fue publicada en primera instancia la norma 27001 en el año 2005, posteriormente la serie 27000 ha ido evolucionando con la incorporación de nuevas normas como la ISO 27002 y la actualización de nuevas versiones. Describen en qué consiste un Sistemas de Gestión de la Seguridad de la Información dentro de las organizaciones y su importancia en el resguardo de la información. Asimismo, se desprende la relevancia de la oportuna y adecuada identificación de los requisitos de seguridad de la información de la entidad, con la finalidad de reconocer los posibles riesgos asociados y, por ende, minimizar el daño o pérdida de información, mediante el establecimiento de controles. Aunado, también a la supervisión y ratificación con una mejora continua.
- UNE-ISO/TR 18128 IN: 2014. La norma realiza la identificación de los riesgos relacionados con los sistemas y procesos de gestión documental, mediante distintos criterios llamados áreas de incertidumbre, con el fin de

evaluar y mitigar los potenciales riesgos que impiden garantizar a los documentos continuar siendo íntegros, fiables y accesibles durante el tiempo.

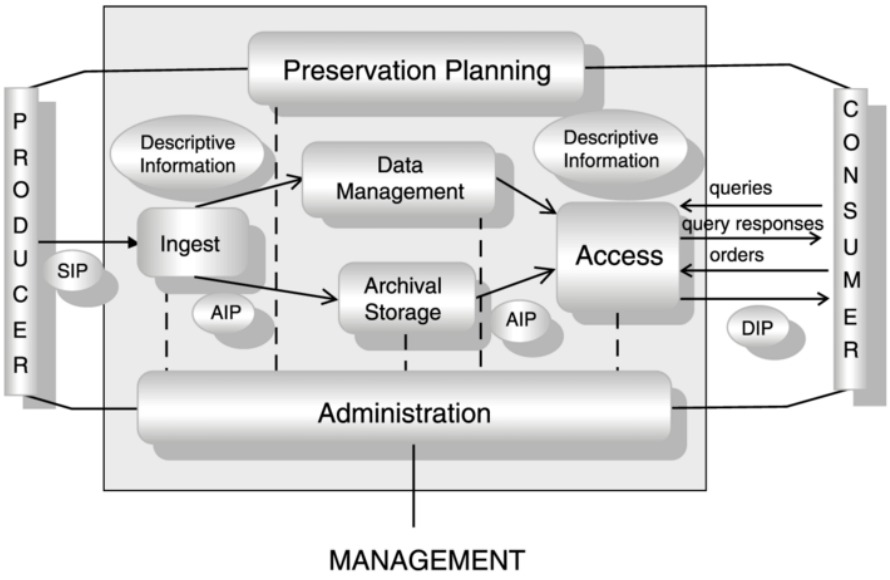
- UNE-EN ISO/IEC 27037: 2016. La norma establece técnicas de seguridad, por medio de pautas específicas para la identificación, recopilación, adquisición, documentación y preservación de las evidencias electrónicas, procesos necesarios en las investigaciones para mantener la integridad de la evidencia electrónica. Esta norma internacional busca complementar las normas UNE-ISO/IEC 27001 y 27002, y en particular los requisitos de control relacionados con la posible adquisición de evidencia electrónica al proporcionar orientación de implementación adicional.
- UNE-ISO 31000: 2018. Esta norma tiene como objetivo proporcionar principios y directrices sobre la gestión de riesgos en las organizaciones, la misma propone un enfoque general y exhaustivo para integrar, diseñar, implementar, evaluar y mejorar la gestión de riesgos, independientemente de la industria, ámbito o sector de la organización.

5.1.2 Modelos para la preservación digital

I. Sistema Abierto de Información de Archivo (OAIS)

Es un modelo de referencia que proporciona las características y requerimientos que debe tener un sistema de preservación de documentos, este ha sido adoptado como estándar internacional por ser, hasta el momento, el más completo y exhaustivo en la materia. Es un estándar amplio y detallado, que describe una combinación de personas y sistemas para la preservación e incluye un modelo funcional, un modelo de información y un modelo ambiental. No tiene como objetivo describir una implementación en particular, sino más bien una estructura intelectual.

Figura 1. Esquema Intelectual del Sistema Abierto de Información de Archivo (OAIS)

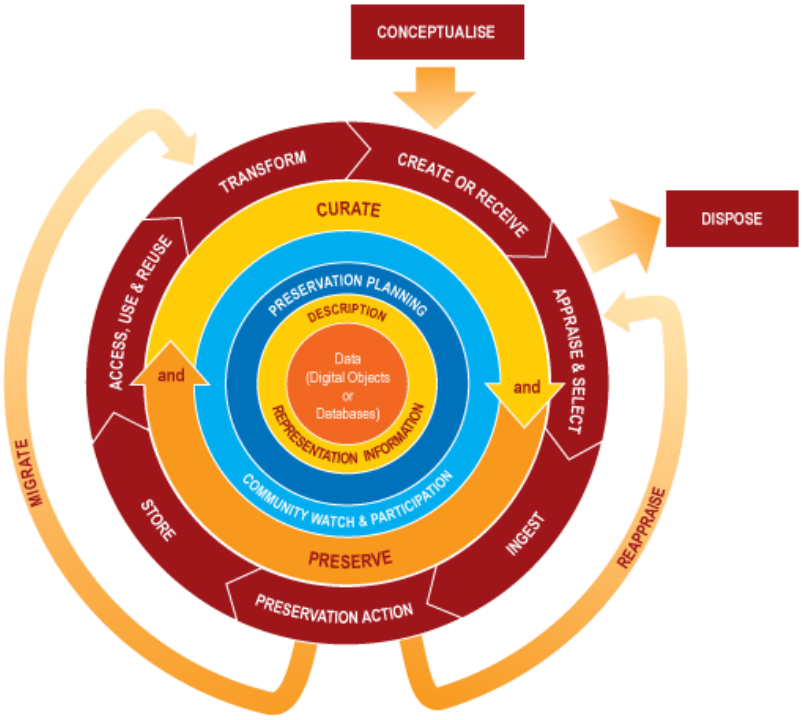


Fuente: UNE-ISO 14721:2015: Sistemas de transferencia de datos e información espaciales. Sistema abierto de información de archivo (OAIS). Modelo de referencia.

II. Modelo de Ciclo de Vida del Centro de Curación Digital (DCC)

El modelo de ciclo de vida DCC proporciona una descripción gráfica de las etapas necesarias para la preservación del contenido digital desde la creación o recepción inicial a través de un ciclo de preservación iterativo, con un enfoque particular en los datos de investigación. El ciclo de vida puede ayudar a planificar sus procesos de preservación, asegurándose de que sean completos.

Figura 2. Ciclo de Vida de la Curación Digital. Modelo elaborado por el Digital Curation Centre



Fuente: Curation Lifecycle Model.

III. Modelo de Gestión de la Preservación Digital de la Coalición de Preservación Digital (DPC)

Es un modelo de madurez organizativo, útil para comenzar con el tema de la preservación digital. Establece tres áreas principales de trabajo para las actividades de preservación digital:

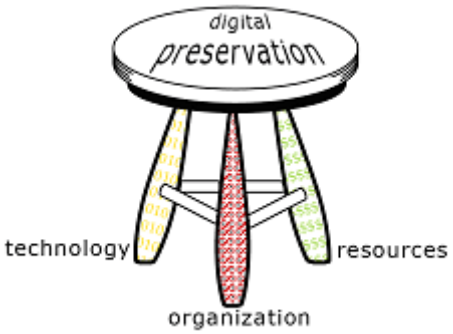
- **Tecnología**: almacenamiento, sistemas de repositorios, herramientas y seguridad.
- **Organización**: política, estrategia, procedimientos, riesgos y beneficios, y dotación del personal.
- **Recursos**: planificación empresarial, costos, fondos, sostenibilidad y habilidades del personal.

Además de identificar las áreas clave donde se requiere actividad, el modelo también describe cinco niveles de respuesta organizacional:

- **Reconocimiento**: entender que la preservación digital es una preocupación local;
- **Actuar**: iniciar proyectos de preservación digital;
- **Consolidar**: segmentar de proyectos a programas;
- **Institucionalizar**: incorporar el entorno más amplio; y
- **Externalizar**: adoptar la colaboración y la dependencia interinstitucional.

Los cinco niveles favorecen la planificación de un programa de preservación digital. Así como también permitirán identificar en qué nivel se encuentran las organizaciones en materia de preservación digital, y monitorizar su progreso.

Figura 3. Modelo de Gestión de la Preservación Digital (DPM)



Fuente: Digital PreservationCoalition.

Además, este Modelo de Gestión de la Preservación Digital de la DPC, ofrece una Herramienta de Evaluación Rápida (DPC RAM) diseñado para permitir una evaluación comparativa de la capacidad de preservación digital de una organización, como indica la DPC, es una herramienta de modelado de madurez de preservación digital que tiene como objetivo ser aplicable a organizaciones de cualquier tamaño en cualquier sector y para todo el contenido de valor a largo plazo.

5.1.3 Proyectos de preservación digital

I. Archivo Nacional de Australia: plantilla de evaluación de riesgo

Hoy en día la subcontratación del almacenamiento digital es una realidad, dicho servicio trae consigo una serie de beneficios para las organizaciones, sean económicos, logísticos o tecnológicos, sin embargo, también implica una serie de riesgos que conviene considerar antes de realizar una contratación, por ello el Archivo Nacional de Australia considera que una de las estrategias para mitigar los riesgos, es realizar una evaluación adecuada de los proveedores antes de celebrar un contrato, para ello desarrollaron la plantilla de Evaluación de Riesgos de Gestión de Documentos.

Dicha plantilla abarca los principales riesgos que conviene evaluar antes de adquirir un servicio de almacenamiento digital, la plantilla se encuentra estructurada en cinco grandes categorías de riesgos, la primera es el cumplimiento y la gobernanza, evaluando en esta el cumplimiento de la normativa, los acuerdos y la gestión de auditorías, otra de las categorías son los riesgos técnicos, esta toma en cuenta la pérdida de legibilidad y usabilidad, las interrupciones de red, las copias de seguridad, el monitoreo del sistema y otros. Las siguientes dos categorías evalúan los riesgos y el acceso a los datos y la última de las categorías evalúa los riesgos organizacionales del proveedor. Esta plantilla abarca los riesgos más comunes en cuanto a la subcontratación del servicio de almacenamiento digital, por lo que es considerada una guía a la cual se le pueden agregar otros riesgos de acuerdo con el contexto, demandas y necesidades de la organización que la utilice.

II. Catalogue of Criteria for Trusted Digital Repositories, Nestor Working Group (Alemania)

Este catálogo recoge los criterios a utilizar para diseñar, planificar e implementar un repositorio digital confiable a largo plazo. Se puede utilizar también para la auditoría.

III. Documentos de Archivo en la Nube (DAN)

Es una iniciativa de InterPARES y la Universidad Columbia Británica, Canadá. Pretende investigar los beneficios y riesgos de almacenar documentos de archivo en la nube y así desarrollar políticas y modelos procedimentales para la integración de la tercerización hacia la nube.

IV. Digital Repository Audit Method Based on Risk Assessment (DRAMBORA)

Esta iniciativa busca evaluar un depósito digital, basado en el análisis de riesgos y evaluar y calcular los riesgos, así como la definición de medidas de gestión de riesgos.

V. E-Journal Archiving, Council on Library and Information Resources (CLIR)

Por medio de este proyecto se proporciona una serie de investigaciones destinadas al establecimiento de criterios básicos para la preservación de revistas electrónicas, por lo tanto, la mayoría de sus investigaciones han sido destinadas a temas como la infraestructura tecnológica, el flujo de trabajo y modelos sostenibles de acceso y negocio.

VI. Electronic Records Archive (ERA)

Electronic Records Archive, es un sistema de archivo de documentos electrónicos para recibir y almacenar documentos con carácter federal, presidencial y del Congreso utilizando contenedores AIP de tipo METS; de igual manera, permite realizar la transferencia y preservación de documentos digitales al NARA, la cual se encarga de garantizar la integridad y el acceso de los documentos digitales.

VII. Estrategia de conversión (Dinamarca)

El caso de Dinamarca y su estrategia de preservación de documentos electrónicos de archivo se entiende a partir de su Sistema Nacional de Archivos; la estrategia de conversión es un proceso donde a cada una de las instituciones del Estado Danés, le

corresponde transferir al Archivo del Estado de Dinamarca los documentos electrónicos con valor permanente, cada cinco años, para ello y para garantizar la constancia de los mismos durante el tiempo, se estableció remitir versiones de archivo, o en otras palabras, una copia de los datos en formato especial.

La estrategia de conversión utilizada en Dinamarca se centra en que esta conversión se hace sobre los datos y no precisamente sobre los formatos digitales, esto se hace con el fin de asegurar su conformidad con la tecnología a lo largo del tiempo. De igual manera, los materiales que sean transferidos deben estar almacenados previamente en formatos adecuados para las conversiones continuas sin pérdidas significativas de datos (Cruz-Mundet y Díez-Carrero, 2016).

VIII. European Framework for Audit and Certification of Digital Repositories

El objetivo de este es establecer mecanismospara garantizar que las partes ya mencionadas puedan colaborar en la creación de un marco integrado para auditar y certificar repositorios digitales. El marco consiste en una secuencia de tres niveles, para aumentar la confiabilidad de los repositorios:

- La certificación básica: se otorga a los repositorios que obtienen la certificación DSA.
- La certificación extendida: se otorga a los repositorios de certificación básica que además realizan una auto-auditoría estructurada, revisada externamente y disponible públicamente basada en la ISO 16363.
- La certificación formal: se otorga a los repositorios que además de la certificación básica obtienen una auditoría externa completa y una certificación basada en ISO 16363 o DIN 31644 equivalente.

IX. Global Digital FormatRegistry (GDFR)

Por medio de este proyecto se busca desarrollar un registro sostenible y global de formatos de objetos digitales, facilitando de esta manera alcanzar los objetivos complementarios de preservación e interoperabilidad de la información.

X. Grupo de Preservación Digital de la Universidad Nacional Autónoma de México

El Grupo de Preservación Digital de la Universidad Nacional Autónoma de México elaboró una guía de criterios básicos para valorar sistemas de preservación digital, eldocumento pretende ser un apoyo para valorar sistemas de software de preservación digital (de pago o de código abierto) disponibles en el mercado. Para la definición de los criterios se utilizó la norma ISO 25000 para la evaluación de la calidad de los productos de software, la ISO 14721 como referencia y modelo para el proceso de preservación digital, Moreq como guía en los procesos de gestión documental, específicamente alineado a la producción documental, y las métricas TRAC como referencia para la creación de repositorios digitales.

La guía está estructurada con base en 9 criterios (funcionalidad, fiabilidad, usabilidad, eficiencia, mantenimiento, portabilidad, compatibilidad, seguridad y distribución) y 74 preguntas, el documento es general y puede ser utilizado como referencia, de tal forma que quien decida utilizarlo puede darle el peso o importancia a cada criterio de acuerdo a lo establecido en su propio plan o sus necesidades específicas, siempre y cuando no se pierda de vista que lo ideal es que el Sistema de Preservación Digital considere, al menos, lo establecido en la guía como criterios básicos.

XI. Investigating the Significant Properties of Electronic Content Over Time (INSPECT)

El proyecto está basado en la identificación de las propiedades significativas del objeto digital, que son aquellos aspectos del objeto digital que deben conservarse a lo largo del tiempo para que este permanezca accesible y significativo.

XII. Manual para Auditoría de Repositorios Archivísticos Digitales Confiables

Manual brasileño elaborado por Henrique Machado en el 2018, tiene como objetivo orientar el proceso de auditoría de los repositorios archivísticos de confianza, a partir

del análisis de las normas ISO 14721 e ISO 16363. Además, pretende armonizar el diálogo entre la ISO 14721, la ISO 16363 y la Archivística, ya que ambas normas están redactadas de una manera genérica, destinadas a repositorios digitales de diversa índole, mientras que el manual en cuestión presenta un enfoque meramente archivístico.

El manual analiza de manera general el modelo OAIS y la cadena de custodia documental, ahondando más en la ISO 16363, con el fin de agregar una vista o posición archivística en torno a los requisitos utilizados para la auditoría de repositorios y de esta manera promover la auditoría, certificación y la reflexión alrededor de los repositorios archivísticos en cuestión.

XIII. National Archives of Australia (NAA)

En el año 2015, se emitió la Política de Continuidad Digital 2020 una de las estrategias implementadas, consiste en la publicación de una guía de formatos para la preservación a largo plazo.

El documento determina tres niveles, los cuales son: preferidos, aceptables y en riesgo. Los preferidos, son formatos que los archivos han determinado que tienen un riesgo muy bajo de volverse obsoletos a largo plazo. Los archivos convierten los formatos "en riesgo" en un formato de conservación "preferido", por su parte los formatos considerados como “aceptables” no se convierten, se mantienen tal como están, pero con un estricto monitoreo (National Archives of Australia, 2020).

XIV. National Archives and Record Administration (NARA)

Los Archivos Nacionales de Estados Unidos han desarrollado diversos proyectos para garantizar la preservación de los documentos electrónicos a largo plazo, entre los que se encuentra una guía para la creación de políticas destinadas a la conservación de colecciones digitales en los archivos.

Además, en el año 2007, NARA en conjunto con el *Center forResearchLibraries* (CRL) elaboraron el *TrustworthyRespositories Audit &Certification* (TRAC): *Criteria and Checklist*, consiste en una herramienta de auditoría para evaluar la

confiabilidad, el compromiso y el estado de las instituciones para asumir responsabilidades de preservación a largo plazo. También existe una metodología creada por la *National Digital Stewardship Alliance* (NDSA) de Estados Unidos, para evaluar el nivel de preservación digital de una determinada institución, esta metodología *Levels of Digital Preservation* surgió gracias al grupo de trabajo que estuvo formado, por representantes de NARA, el *Metropolitan New York Library Council*, la *Harvard Library* y la *Library of Congress*.

XV. Planning Tool for Trusted Electronic Repositories (PLATTER)

PLATTER es una herramienta elaborada por la *Digital Preservation Europe* (DPE) que proporciona una base para que un repositorio digital planifique el desarrollo de sus objetivos y metas de rendimiento a lo largo de su vida útil, además contribuye al repositorio a establecer un estado de confianza entre las partes interesadas. PLATTER está diseñado para complementar las iniciativas existentes de auditoría y certificación, como el kit de herramientas DPE y DCC DRAMBORA.

XVI. Pronom y PUIDs (Reino Unido)

El primero recopila y pone a disposición la información técnica sobre formatos de fichero y software que los soportan, y el segundo es un marco de evaluación extensible de identificadores persistentes, únicos e inequívocos para los registros de PRONOM. Los identificadores en cuestión son medulares para el intercambio y la gestión de objetos digitales.

XVII. Red de Bibliotecas de Universidades Españolas (REBIUN)

El Grupo de Repositorios de Red de Bibliotecas de Universidades Españolas elabora la guía para la evaluación de los procesos de preservación en repositorios institucionales de investigación, la cual tiene como objetivo permitir una auditoría interna para establecer posibles acciones de preservación digital en los repositorios institucionales de las universidades españolas, esta nace gracias a una encuesta realizada por el Grupo de Repositorios de REBIUN en la que se logra concluir que los repositorios no estaban aplicando las medidas técnicas de preservación, por lo que desarrollan la guía de evaluación basada en los niveles establecidos por la *National*

Digital Stewardship Alliance (NDSA), en prácticas de preservación digital y experiencias de los miembros del grupo que la desarrollaron.

La guía de evaluación no está diseñada para la certificación o competición de repositorios, sino para detectar las fortalezas, debilidades y prioridades con el fin de tomar las medidas o decisiones de mejora, tiene un enfoque meramente práctico y de autoevaluación. Para realizar la evaluación, esta guía contempla aspectos como: el plan de preservación, integridad de datos, formatos, metadatos, almacenamiento, copias, inventarios, flujos de trabajo, documentación de procesos y gestión de riesgos.

Por su parte, esta guía menciona que se puede utilizar en conjunto con la herramienta de evaluación en línea que ofrece la Asociación Iberoamericana de Preservación Digital, la cual se basa en la primera versión de los niveles de la NDSA, esta herramienta plantea una serie de preguntas para realizar la evaluación y en un periodo de 30 a 90 días envía al solicitante los resultados obtenidos y las recomendaciones prácticas en materia de preservación digital.

XVIII. Technical Guidelines for Digitizing Archival Materials for Electronic Access Creation of Production Master Files-Raster Images (Estados Unidos)

Son pautas técnicas para digitalizar materiales de archivo, define además enfoques para crear sustitutos o copias digitales para facilitar su acceso y reproducción.

XIX. The International Research on Permanent Authentic Records in Electronic Systems (InterPARES)

The International Researchon Permanent Authentic Records in Electronic Systems (InterPARES), tiene como objetivo desarrollar el conocimiento esencial para la conservación a largo plazo de documentos auténticos, producidos y mantenidos en forma digital, además pretende proporcionar la base para estándares, políticas, estrategias y planes de acción capaces de garantizar la preservación y autenticidad del material de estudio.

XX. VERS de *Public Record Office Victoria* (PROV)

Es un estándar, el cual busca garantizar la autenticidad e integridad de los documentos digitales, así como proporcionar una metodología para su preservación a largo plazo.

XXI. VidArch de la Biblioteca del Congreso (Estados Unidos)

Iniciativa para preservar el contexto y contenido de archivo de videos digitales, con la finalidad de hacerlos accesibles a las futuras generaciones.

XXII. XENA

Corresponde a un software de preservación digital, el cual convierte los archivos de datos abiertos a formatos estándar, codifica el archivo en base 64 y ajusta los metadatos asociados.

5.1.4 Herramientas de preservación digital

En cuanto a las soluciones tecnológicas disponibles en el mercado internacional se encuentran las siguientes:

Cuadro 1. Descripción de Soluciones de Preservación Digital

Herramienta	Desarrollador	Funcionalidad
ARCA	*Business Integrators Systems Limitada,* Costa Rica.	Es un repositorio de preservación para objetos digitales, desarrollado por la empresa Business IntegratorsSystems Limitada. Que se basa en la implementación del Modelo OAIS, estándares internacionales como la ISO 14721 y la ISO 15489, METS, PREMIS, EAD, EAC, EAG, para la conformación de los paquetes SIP, AIP, y DIP utilizados en los procesos de ingesta, custodia y difusión, además de otros mecanismos entre los que sobresalen el control de disposición final, la clasificación archivística, la conversión de formatos y el uso del sello institucional digital, con el fin de garantizar que los objetos digitales sean íntegros y confiables a través del tiempo.
Archivematica	*Artefactual Systems,* Canadá	Es un conjunto de herramientas de código abierto, basado en estándares internacionales como METS, PREMIS, Dublin Core, la especificación Baglt (Library ofCongress) y acorde al modelo ISO-OAIS, con el objetivo de generar fiablemente paquetes AIP (ArchivalInformationPackage) para ser grabados en un sistema de almacenamiento y de esta manera preservar el acceso a largo plazo de los contenidos digitales.
Arcsys software	Infotel, Francia	Proporciona un repositorio unificado para la conservación a largo plazo de todos los archivos de una organización, con el fin de mantener los activos, gestionar los riesgos y cumplir con el marco normativo para aumentar la confianza digital.
DAITSS	*The Florida Center for Library Automation*	Es una aplicación de software de preservación digital. DAITSS está basado en el modelo OAIS y controles estrictos para garantizar la integridad y autenticidad de los contenidos digitales.
DSpace	Hewlett-Packard. Massachusetts	Herramienta de código abierto para gestionar repositorios de ficheros (textuales, audio,

Herramienta	Desarrollador	Funcionalidad
	Institute of Technology, Estados Unidos.	vídeo), facilitando su depósito, asignando metadatos y permitiendo su difusión.
DuraCloud	DuraSpace, Estados Unidos.	Es una herramienta de almacenamiento que permite almacenar contenido en la nube, el cual agrega funciones que permiten la preservación digital, el acceso e intercambio de datos.
FEDORA (Flexible Extensible Digital ObjectRepositoryArchitecture)	Fedora LeadershipGroup y DuraSpace, Estados Unidos	Es un sistema de repositorio modular y de código abierto para la gestión y difusión de contenido digital, además proporciona acceso especializado de colecciones digitales robustas y complejas de materiales históricos y culturales, así como a datos científicos garantizando su preservación a largo plazo.
LOCKSS (Lots of Copies Keep Stuff Safe)	Universidad de Stanford	Es un software que permite a las instituciones recolectar, almacenar, preservar y archivar localmente contenido digital, además de garantizar que se almacenan varias copias en diferentes organizaciones buscando la seguridad de la información.
PLANETS	Open PlanetsFoundation (OPF)	*Preservation and Long-term Access throughNetworkedServices* crea servicios y herramientas prácticas que ayuden a garantizar el acceso a largo plazo de los documentos y activos culturales y científicos digitales de la Unión Europea.
RODA	Archivos Nacionales de Portugal / Universidad de Minho	Es un repositorio digital de código abierto diseñado para preservación digital. Está respaldado por estándares existentes como OAIS, METS, EAD, Dublin Core y PREMIS.
UDFR	Universidad de California	El Registro de Formato digital Unificado consistió en unificar PRONOM y GDFR, creando una base o plataforma de código abierto, confiable y accesible que contenía representaciones de formatos de archivo de preservación digital de uso comunitario.

Fuente: elaboración propia con datos obtenidos en las páginas web de los desarrolladores de cada herramienta.

5.2 Ámbito nacional

5.2.1 Contexto normativo

En Costa Rica, el funcionamiento de los archivos del sector público y la custodia y protección del patrimonio científico cultural de la nación y los procesos de la gestión documental se encuentran regulados por la Ley N.º7202 del Sistema Nacional de Archivos (SNA), desde el 24 de octubre de 1990 con el fin de normalizar el funcionamiento de los órganos pertenecientes al SNA, que son aquellos archivos de los poderes Legislativo, Judicial y Ejecutivo, y de los demás entes públicos, así como archivos privados y particulares que deseen someterse voluntariamente a la regulación.

Debido al efecto transformador de la tecnología en la sociedad, se evidenció la necesidad de actualizar el Reglamento publicado mediante Decreto Ejecutivo N.º 24023, con el objetivo de establecer pautas más claras en la reglamentación de la Ley N.º 7202. En este sentido se decreta el Reglamento Ejecutivo a la Ley del Sistema Nacional de Archivos el 7 de septiembre de 2017.

Es precisamente por medio de este Reglamento, donde el Poder Ejecutivo establece que los archivos del SNA deben implementar los mecanismos y procedimientos necesarios para asegurar la autenticidad, integridad y disponibilidad a largo plazo de los documentos electrónicos de archivo para garantizar el acceso a la información pública.

Con fundamento en la Ley N.º 8454 y el artículo 29 del Decreto Ejecutivo N.º 33018-MICIT Reglamento a la Ley de Certificados, Firmas Digitales y Documentos Electrónicos, se informa sobre la entrada en vigor de la Política de Formatos Oficiales de los Documentos Electrónicos Firmados Digitalmente, la cual detalla las características que debe cumplir un documento electrónico firmado digitalmente para considerar que implementa el formato oficial nacional correspondiente a su clase.

La Dirección de Certificadores de Firma Digital es quien determina los formatos oficiales de los documentos electrónicos firmados digitalmente en Costa Rica, los cuales definen las responsabilidades relacionadas con la firma digital y la

verificación de su validez. Los formatos establecidos por la Dirección de Certificadores para este momento son: CAdES-X-L, PAdES Long Term (PAdES LTV) y XAdES-X-L, en sus versiones publicadas por ETSI (Instituto Europeo de Normas de Telecomunicaciones). Sin embargo, en la norma ETSI EN 319 142-1 (2016-04) se estableció desde el 2016 el formato PAdES Nivel B Long Time Archival (PAdES B-LTA).

Con base en la Estrategia de Transformación Digital hacia la Costa Rica del Bicentenario 4.0 (ETDCR4), el Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT) emitió el Código Nacional de Tecnologías Digitales, un compendio de políticas públicas que establecen los mínimos deseables para la adquisición, desarrollo y gestión de las tecnologías y los servicios digitales en el sector público costarricense. Su propósito reside en brindar los criterios técnicos para que la Comisión de Alto Nivel y la Secretaría técnica puedan valorar objetivamente cuáles proyectos tecnológicos son de importancia nacional y por ello merecen disponer de un Sello de Gobierno Digital.

Por su parte, la Junta Administrativa del Archivo Nacional de Costa Rica, como ente rector en materia archivística, ratifica la preeminencia de una adecuada gestión de los documentos electrónicos en el país, mediante la norma técnica para la gestión de documentos electrónicos en el SNA, la cual se difunde a partir del año 2018.

La norma técnica menciona que “para tener un valor probatorio, un documento debe ser considerado confiable y auténtico [...], además se debe garantizar la conservación y el acceso a los documentos durante su ciclo de vida” (2018, p. 2), para ello la norma indica una serie de medidas mínimas para la conservación de documentos electrónicos, sin embargo, como se establece son medidas mínimas en las que aún se debe profundizar.

Posteriormente, el Archivo Nacional presentó en el Congreso Archivístico Nacional XXXI del año 2019, una propuesta de Política Nacional de Archivos que pretendía el fortalecimiento y mejora continua del entorno archivístico nacional, específicamente en relación al proceso de preservación buscaba la implementación de sistemas para el

resguardo final y la conservación de los documentos electrónicos de valor científico y cultural que permitan la transferencia de los documentos electrónicos producidos por las diferentes unidades productoras a los repositorios de una manera legalmente válida, segura, ágil y confiable, no obstante esta iniciativa no se llegó a formalizar.

Finalmente, en el año 2021, el Archivo Nacional planea publicar la Norma Técnica Nacional: "Requisitos mínimos para sistemas de gestión de documentos electrónicos y su preservación a largo plazo, el cual fue presentado como ponencia en el Congreso N.º. XXXII. Su objetivo es promover el adecuado desarrollo, implementación, mantenimiento y mejora continua de sistemas institucionales para la gestión de documentos electrónicos, que permitan garantizar la adecuada adopción de los procesos archivísticos y la integridad, confiabilidad, autenticidad, valor legal y acceso a los objetos de información digital, y su preservación.

5.2.2 El derecho de acceso a la información y el Gobierno Digital

Uno de los principales objetivos planteados a través de la aplicación de procesos de preservación digital es garantizar la accesibilidad de la información por el tiempo que sea requerido, asimismo el acceso a la información constituye un derecho democrático que se encuentra amparado por la Constitución Política de Costa Rica de 1949, específicamente, por el artículo 30 en donde se señala que: "se garantiza el libre acceso a los departamentos administrativos con propósitos de información sobre asuntos de interés público. Quedan a salvo los secretos de Estado", complementariamente con otras normas de menor rango dentro del marco jurídico nacional, como decretos ejecutivos y jurisprudencia emitida por la Sala Constitucional de la Corte Suprema de Justicia.

En ese sentido, con el fin de impulsar la óptima utilización de las Tecnologías de la Información y Comunicación en la gestión pública, el Gobierno de la República emitió en el año 2017 la Directriz N.º 073-MP-MEIC-MC sobre la Transparencia y el Acceso a la Información Pública, la cual insta a la administración, por medio del artículo quinto, a que se adopten las acciones que aseguren la accesibilidad a la información de interés público mediante medios manuales y electrónicos, así como

en formato abierto que permita el uso ágil y eficiente de la información. La directriz instruye a las instituciones a adoptar la figura de los Oficiales de Acceso a la Información y de Simplificación de Trámites.

De manera complementaria, en el año 2018 se da la emisión de la directriz N.º 019-MP-MICITT, con la cual se busca dar seguimiento a la ejecución de la Estrategia del Gobierno Digital del Bicentenario, por medio de la formulación de proyectos y acciones orientadas al Gobierno Digital.

Por medio de la Directriz sobre el Desarrollo del Gobierno Digital del Bicentenario, el Estado promueve las acciones para incrementar el uso y aplicación de las tecnologías y de la firma digital, evidenciándose en el artículo tercero donde menciona que "(...) al menos un 75% de todos los documentos que se gestionan y conservan en la institución sean documentos electrónicos firmados digitalmente, antes del 1ero de diciembre 2020", como un medio de agilización en los procesos y en la transparencia de la toma de decisiones en el gobierno, con la contraparte de disminuir la producción de documentos en soporte tradicional.

La Directriz 067-MICITT-H-MEIC, del año 2014, en su artículo primero busca:

> (…) hacer efectivo el derecho a exigir igualdad en el acceso por medios electrónicos a todos los servicios que se ofrecen por medios físicos, pudiendo las personas físicas utilizar en cualquier escenario la capacidad de firma digital certificada, ya sea para autenticarse o para firmar todos los trámites con la institución por vía electrónica (p. 1).

Por consiguiente, la directriz insta a las instituciones públicas del país y a las entidades privadas que lo deseen, a invertir esfuerzos y recursos en la implementación de los mecanismos para el uso y aceptación de la firma digital. Siendo de carácter obligatorio, la aceptación en entidades públicas de documentos firmados digitalmente sin la posibilidad de repudio.

5.2.3 Aportes académicos

Se destacan dos aportes académicos a nivel nacional relevantes para el desarrollo de la presente investigación. El primero, es la Propuesta de un Modelo de Requisitos Archivísticos para un Sistema de Gestión de Documentos Electrónicos de Archivo en Costa Rica publicado en el año 2014 por Cedeño-Molina, A y otros; en el que se establecen los requisitos mínimos en materia de metadatos, tomando en consideración las principales propuestas que se han generado a nivel internacional y adaptándose a la realidad costarricense.

En esta investigación se identifican los requerimientos funcionales y no funcionales con los cuales ha de disponer un sistema de gestión de documentos electrónicos. Además de los requisitos archivísticos con los que debe considerar el sistema en cada una de las funciones o procesos archivísticos, desde la identificación hasta su posterior eliminación, conservación, acceso y disposición a los diversos usuarios.

El segundo aporte, es el Modelo de preservación de documentos digitales en la Administración Universitaria. Estudio de caso: Universidad Nacional, publicado en el año 2018 por Castillo-Solano, M y Umaña-Alpízar, R. Es el trabajo de investigación más reciente relacionado con la preservación de los documentos digitales de archivo, siendo este el primero en el país. En la investigación se propone un modelo de preservación de documentos digitales de archivo.

Este modelo establece una política de preservación digital, así como las estrategias de preservación necesarias para garantizar la autenticidad, integridad, acceso y disponibilidad a largo plazo de los documentos. Para esto, se propone un modelo funcional y tecnológico del archivo digital de la institución, considerando el contexto normativo, archivístico, administrativo que rodea a la entidad en la actualidad.

5.2.4 Archivo Digital Nacional (ADN)

Es un proyecto a cargo de un grupo de funcionarios del Archivo Nacional de Costa Rica, específicamente del Servicio Archivístico Externo (SAE), como estrategia de transformación digital, que pretende la normalización de la preservación de

documentos electrónicos de las instituciones públicas, por medio de un repositorio nacional digital basado en el modelo OAIS; ADN es una solución ofrecida bajo modelo de servicio por parte del Archivo Nacional a las instituciones que integran el Sistema Nacional de Archivos (SNA).

ADN pretende convertirse en un punto único de resguardo de documentos electrónicos del Estado costarricense, y por ende un punto centralizado para el acceso a la información de la administración pública. Además, aspira ofrecer una solución nacional para la interoperabilidad de los Sistemas de Gestión de Documentos Electrónicos, y de la preservación de documentos electrónicos por medio de la seguridad informática y el acompañamiento, asesoría y soporte técnico en preservación digital.

Cabe resaltar que la filosofía de ADN implica un cambio sobre la forma tradicional de operación de la Ley 7202, ya que la solución tecnológica permite la preservación y la garantía de acceso a la información contenida en todos los documentos de mediano o largo plazo que se custodian y no solo en aquellos que sean dictaminados como de valor científico o cultural, además de poner a disposición de las instituciones los mecanismos de aseguramiento de expedientes (proceso análogo a la foliación), control de disposición final, descripción y clasificación archivística, acorde a la legislación y normativa nacional vigente.

CAPÍTULO II.

MARCO TEÓRICO Y METODOLÓGICO

1. Marco teórico

En esta sección, se describen las principales teorías que se tomarán como fundamentación para el desarrollo del marco de evaluación para soluciones de preservación de documentos digitales; por lo tanto, se conceptualizan términos medulares para la comprensión e implementación de la presente investigación.

1.1 Documento de archivo

De acuerdo con el Consejo Internacional de Archivos (ICA por sus siglas en inglés) (2016), el documento de archivo es un instrumento de carácter contemporáneo que es creado por individuos y organizaciones en el desarrollo de sus actividades. De igual manera, advierte que los documentos de archivo son tan variados como sus formatos, encontrando documentos escritos, fotográficos, gráficos, sonoros, digitales, analógicos, entre otros (párr. 2).

El entorno de las tecnologías de la información y de la comunicación ha dado lugar a los documentos electrónicos y, por consiguiente, su uso se ha masificado cada vez más, tanto en instituciones públicas como privadas, por lo cual, se ha hecho aún más necesario normalizar y alcanzar un consenso especializado sobre las características y elementos que deben componer un documento electrónico de archivo, por lo tanto, diversas organizaciones han emprendido esta misión.

Tal es el caso del ICA (2017), el cual define documento de archivo como:

> Información producida o recibida durante el desarrollo de una actividad institucional o individual; dotado de contenido, contexto y estructura suficiente para proporcionar la evidencia de esa actividad. Este concepto cubre todos los diferentes tipos de documentos de archivo producidos en una oficina (p. 3).

Documento de archivo, hace referencia tanto a los documentos electrónicos, como a los producidos en papel, lo que cambia entre los dos es el soporte de su producción, así lo afirma Cruz-Mundet (2011) en el texto “Administración de documentos y

archivos", donde se reconocen las siguientes características propias del documento electrónico:

- **El registro y uso de símbolos:** el documento electrónico está recogido en un medio y a través de símbolos que deben ser decodificados para hacerlo accesible, por ello el medio (soporte o almacenamiento) y los símbolos (formato) son condiciones indispensables del documento electrónico.

- **Conexión entre contenido y el medio**: la información del documento electrónico puede ser separada del medio original y transferida a otro formato u otros soportes.

- **Características de la estructura física y lógica:** la estructura representable del documento electrónico depende del dispositivo de almacenamiento y del componente de programación encargado de administrar y facilitar el uso y acceso a los dispositivos de almacenamiento; la estructura lógica o formato, se identifica y representa por medio de los elementos de su estructura interna, es decir, la que le ha dado su creador. Un documento electrónico auténtico y completo debe conservar los elementos de autenticidad de esa estructura interna y los datos consignados en ella de forma íntegra.

- **Metadatos:** el documento electrónico al igual que el documento tradicional, por sí solo carece de los elementos que permiten establecer su contexto funcional y administrativo, esta tarea, que en el documento en soporte físico se consigue a través del cumplimiento de los principios archivísticos y las agrupaciones documentales, se refleja en el ámbito digital a través de los metadatos, que describen cómo se ha registrado la información, cuándo y por quién, cómo está estructurada, cuándo se ha utilizado y su relación con otros documentos.

- **Identificación:** que se consigna a través de los metadatos y no puede accederse a ella sino con medios asistidos por máquina.
- **Conservación:** que no depende sólo de la supervivencia del dispositivo de almacenamiento, sino que debe gestionar el riesgo, la rápida obsolescencia de los formatos y la tecnología (p.32-33).

1.2 Gestión de documentos

La gestión de documentos ha variado conforme ha evolucionado la sociedad, con el fin de adaptarse a los retos y necesidades de una sociedad cada vez más exigente, por lo que su definición ha variado y se ha transformado a lo largo del tiempo, dando paso al surgimiento de conceptos y modelos que en su momento fueron considerados como disruptivos, como lo fueron el recordmanagement y el recordkeeping.

El recordmanagement surgió en los Estados Unidos a mediados del siglo XX en respuesta a la explosión documental existente en la administración pública de ese país, proponiendo un modelo que busca la eficiencia y control de los documentos, dando cabida al concepto del ciclo de vida, por medio del cual se establecen una serie de etapas por las que podía pasar un documento como la producción, el mantenimiento y la disposición final, su eliminación o conservación permanente (Llansó Sanjuan, J. 2006. p. 48-49).

Posteriormente, como parte del proyecto *"Functional Requirements for Evidence in Recordkeeping"* de la Universidad de Pittsburgh, el cual pretendía establecer los requerimientos funcionales para la gestión de documentos electrónicos, se desprende el modelo australiano recordkeeping que asume la perspectiva del record continuum, de esta forma, se asume una perspectiva diferente y adecuada al fenómeno de la gestión de los documentos en formatos digitales.

En ese sentido, el record continuum se plantea como un modelo holístico e integrado de los diferentes elementos y ejes que pueden intervenir en la gestión de documentos, por lo tanto, hace una división de cuatro ejes entre los que se encuentran: la identidad asociada a los productores de documentos, la transaccionalidad generada de los

documentos como producto de las actividades, la evidencia de las funciones de la organización plasmadas en los documentos y la gestión de documentos; estos interactúan con cuatro dimensiones diferentes: la producción de documentos, la captura e incorporación de documentos al sistema, la organización de los documentos y la pluralización o diseminación de la memoria colectiva (Castillo Guevara, J y Paz Martín, S. 2019. p. 95-96).

Con base en lo anterior, y con el objetivo de normalizar la definición, y la gestión de documentos como tal, nace la norma UNE-ISO 15489 Información y Documentación Gestión de Documentos, la cual define al término en cuestión como el"área de gestión responsable de un control eficaz y sistemático de la creación, la recepción, el mantenimiento, el uso y la disposición de los documentos, incluidos los procesos para capturar y mantener, en forma de documentos la información y evidencia de las actividades y operaciones de la organización" (UNE-ISO 15489, 2016, p. 9).

La gestión de documentos se basa en los siguientes principios:

a) La creación, captura y gestión de los documentos es parte integral de la gestión de la organización en cualquier contexto.

b) Los documentos, con independencia de su forma o estructura, son evidencia fidedigna de la actividad de la organización cuando tienen las características de autenticidad, fiabilidad, integridad y usabilidad.

c) Los documentos constan de contenido y metadatos que describen el contexto, el contenido y la estructura de dichos documentos, así como su gestión a través del tiempo.

d) Las decisiones relativas a la creación, captura y gestión de los documentos están basadas en la apreciación del riesgo de las actividades de la organización, en su contexto legal, y social.

e) Los sistemas para gestionar documentos, con independencia de su grado de informatización, permiten la aplicación de los instrumentos de gestión de

> documentos y la ejecución de los procesos para la creación, identificación y gestión de dichos documentos (UNE-ISO 15489, 2016, p. 9-10).

De esta manera, la norma internacional ISO 15489 ha servido de guía en una gran cantidad de países para normalizar o estandarizar los procesos que se llevan a cabo en la gestión de documentos.

1.3 Firma Digital

Respecto al documento electrónico en Costa Rica, la Ley N.º 8454, le otorga el reconocimiento de la equivalencia funcional y valor evidencial a cualquier manifestación con carácter representativo o declarativo, expresada o transmitida por un medio electrónico o informático, estableciéndose como jurídicamente equivalente a los documentos que se otorguen, residan o transmitan por medios físicos.

La equivalencia jurídica, por su parte, es otorgada a aquellos documentos suscritos mediante firma digital, lo cual, significa que tendrán el mismo valor y eficacia probatoria que otro documento firmado en manuscrito.

Por consiguiente, cabe recalcar que para el desarrollo de la presente investigación se entenderá como documento electrónico de archivo a cualquier manifestación con carácter representativo o declarativo, expresada o transmitida por un medio electrónico y que suscriba una firma digital certificada, siendo esta misma la interpretación brindada por la normativa costarricense.

De acuerdo con el Sistema Nacional de Certificación Digital de Costa Rica, la firma digital es un método que asocia la identidad de una persona física o jurídica, con un documento electrónico, con el fin de asegurar la autoría y la integridad de este. Asimismo, la firma digital en un documento electrónico es el resultado de aplicar algoritmos matemáticos a su contenido, utilizando como insumo el conjunto de llaves públicas y privadas de un certificado digital, constituye un mecanismo clave para garantizar la integridad y autenticidad, y se convierte en un elemento importante para mejorar la agilidad de los procesos organizativos.

En Costa Rica, sin embargo, desde la promulgación de la Ley 8454 de Certificados, Firmas Digitales y Documentos Electrónicos, se estableció solamente la definición del concepto de firma digital, el cual se indica en el capítulo III, artículo 8º el alcance del concepto: "entiéndase por firma digital cualquier conjunto de datos adjunto o lógicamente asociado a un documento electrónico, que permita verificar su integridad, así como identificar en forma unívoca y vincular jurídicamente al autor con el documento electrónico" (p. 2).

El artículo 2º, inciso 25 del reglamento a la Ley 8454, también define lo que corresponde a una firma digital certificada, el cual menciona que "es una firma digital que haya sido emitida al amparo de un certificado digital válido y vigente, expedido por un certificador registrado". Asimismo, en el artículo 10º se establece la presunción de autoría y responsabilidad de la firma digital, el cual establece que: "todo documento electrónico o archivo digital asociado a una firma digital certificada se presumirá, salvo prueba en contrario, de la autoría y responsabilidad del titular del correspondiente certificado digital, vigente en el momento de su emisión" (p. 2).

Por lo tanto, para firmar un documento de manera que tenga relevancia jurídica, se requiere de un servicio de validación que indique el estado del certificado, con el objetivo de no permitir que se tramiten documentos firmados digitalmente con un certificado revocado o suspendido, así mismo se debe validar toda la cadena de confianza que respalda a la autoridad certificadora que emitió el certificado, en el caso de Costa Rica le corresponde al Sistema Nacional de Certificación Digital, y por último, tanto la persona física como jurídica, tienen la misma autoría y responsabilidad cuando realice algún procedimiento que conlleve una firma digital.

La firma digital técnicamente posee dos funciones, de acuerdo con Castillo (2016) en el artículo "La firma digital en el nuevo contexto de transformación digital" en donde se menciona que de acuerdo con la complejidad se puede dividir las funciones en:

> Las más básicas, conocidas como firma electrónica simple, se limitan a confirmar la autenticidad del documento, identificando al emisor. Por el contrario, la firma electrónica avanzada garantiza también la

> integridad, asegurando que el mensaje no ha sido modificado por ninguna persona ajena desde el momento de la firma (p. 30).

De acuerdo con Jordi Serra (2004), la firma digital a pesar de tener un papel fundamental, como uno de los elementos primordiales en un documento electrónico, ha sido considerada en materia de preservación a largo plazo, más una amenaza que un beneficio, ya que se presentan ciertas problemáticas que afecta al documento en todas las fases de su gestión, según Serra esas problemáticas serían:

> En la fase administrativa, el principal problema es la caducidad de la firma. La actualización de la firma original sólo es posible cuando se tiene acceso al documento y al sistema utilizado para firmarlo. Desde el momento en que la transferencia al archivo significa una desvinculación del entorno tecnológico original, se dificulta la actualización de la firma.
>
> En la fase de conservación a largo plazo, la firma electrónica se convierte en un factor de riesgo para mantener la legibilidad de los documentos digitales, puesto que constituye una capa tecnológica, añadida a los documentos, que mantiene vinculaciones externas determinantes para su validez (software de firma y cifrado, lista de certificados revocados, etc.). El uso de técnicas de encriptación puede dificultar posteriores migraciones, del mismo modo que la obsolescencia tecnológica puede afectar al software de firma y cifrado. Se añade que, para mantener la vigencia de la firma por un período de tiempo prolongado, es necesario conservar los elementos básicos de la infraestructura de firma (PKI) (p. 6).

Sin embargo, de igual manera Serra menciona que estas problemáticas no invalidan el uso de la firma digital. En Costa Rica, para minimizar el problema de la caducidad de la firma digital, se ha redactado normativa para normalizar los formatos en los que se debe realizar la firma digital de persona jurídica.

En el contexto nacional, la Política de Formatos Oficiales de los Documentos Electrónicos Firmados Digitalmente emitida por el MICITT del año 2012, regula los formatos avanzados para la firma digital, según la política, como aquellos formatos de firma digital "definen de manera estandarizada los atributos suficientes para garantizar la verificación de la validez del documento en el tiempo, que estén auspiciados por alguna entidad internacional reconocida, y que sus especificaciones técnicas sean de acceso público" (p. 5).

Los formatos oficiales de los documentos electrónicos firmados digitalmente son los que la Dirección de Certificadores de Firma Digital del MICITT determine. De acuerdo con la política, son los siguientes:

- CAdES-X-L: Basado en la especificación ETSI TS 101 733, en su última versión oficial. Este formato es un conjunto de extensiones de datos firmados con sintaxis de mensajes criptográficos. Válido para cualquier tipo de fichero.

- PAdES Long Term (PAdES LTV): Basado en la especificación ETSI TS 102 778, en su última versión oficial. Este formato de firma longeva permite prorrogar por tiempo indefinido la validez de las firmas en ficheros con formato PDF. Sin embargo, desde las especificaciones de la ETSI EN 319 142-1 se establece PAdES nivel B Long Time Archival (PAdES B-LTA) el cual apunta a la disponibilidad e integridad a largo plazo del material de validación de las firmas digitales a largo plazo. El nivel B-LTA permite validar la firma más allá de muchos eventos que limitan su validez (por ejemplo, la debilidad de los algoritmos criptográficos utilizados o la caducidad de los datos de validación). El uso del nivel B-LTA se considera una técnica de transmisión y conservación adecuada para datos.

- XAdES-X-L: Basado en la especificación ETSI TS 101 903, en su última versión oficial. Este formato de firma digital protege los ficheros en formatos XML.

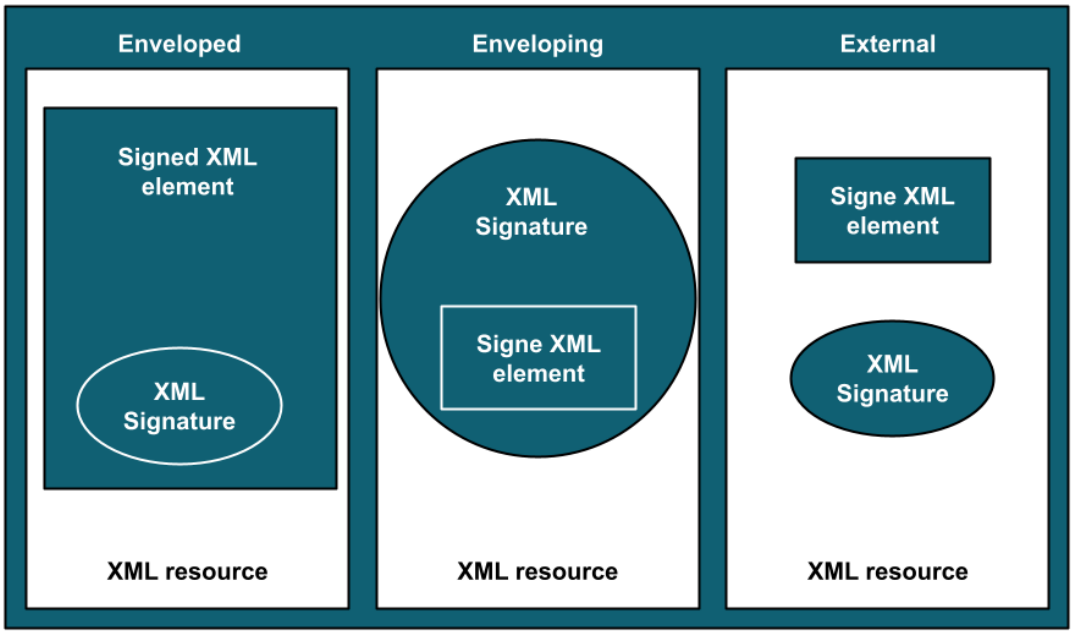
Cada formato posee diferentes versiones, según el nivel de protección ofrecido, sin embargo, la última versión oficial de dichos formatos siempre incluye y extiende a la versión previa.

Los formatos de firma cumplen con las características que permiten la utilización de algoritmos criptográficos robustos y respeto al principio de neutralidad tecnológica, se trata de formatos de estándares abiertos. Asimismo, lo que indica la política es que estos formatos puedan ser empleados en escenarios multiplataforma, disponer de una adecuada documentación técnica (emitida por ETSI) y permitir la incorporación de múltiples firmas en un documento electrónico.

Otro aspecto referente a los formatos avanzados para la firma digital es la relación entre la propia firma y los datos que se firman, por ejemplo; existen tres formas de firmar los datos:

1. La firma está incluida dentro del documento, conocido como firma envuelta (Enveloped) y funciona en los formatos XML y PDF.
2. La firma contiene al documento, conocido como firma envolvente (Enveloping) y funciona en el formato XML.
3. La firma está separada del documento, conocido como firma separada (Detached o External) y funciona en el formato XML.

Figura 4. Formas de firmar los datos



Fuente: Sánchez Martínez. D. (s.f). Formatos de firma electrónica.

También otras de las características que cumplen estos formatos avanzados es que permiten garantizar la autenticidad e integridad del documento electrónico, así como la ubicación del documento electrónico en el tiempo a través de la incorporación del elemento de "Estampado de Tiempo".

La documentación técnica especifica mecanismos normalizados para garantizar la preservación y verificación de la validez de las firmas digitales del documento electrónico en el tiempo.

En este sentido, estos formatos avanzados son mecanismos normalizados con reconocimiento a nivel mundial, que permiten garantizar la preservación y verificación de la validez de las firmas digitales del documento electrónico en el tiempo, ya que incluyen la ruta de certificación en el documento electrónico, la información de revocación y una característica fundamental: la inclusión de sellos de tiempo en el documento electrónico que permite, de acuerdo con la Política de sellado de tiempo del Sistema Nacional de Certificación Digital (2008), "asociar una representación de un dato para un tiempo concreto, estableciendo así evidencia de que el dato existía antes de ese tiempo" (p. 2).

1.4 Sistemas de información electrónica

La norma UNE-ISO 14641: 2015 designa al sistema de información electrónica "como el sistema designado para recibir, preservar, acceder y transferir varios archivos en un formato electrónico" (p. 9).

En concordancia con lo anterior, el sistema se encarga de gestionar desde el ingreso de la información hasta su eliminación o conservación, durante la gestión del documento. Es por esto que cuando se opta por la automatización de un sistema, es fundamental tener claro cuál es el fin o el propósito por el cual se crea el sistema, para tener claro el alcance, las limitaciones y, por ende, el tipo de modelo que más se adecua a la finalidad requerida. Dependiendo del tipo de modelo que se determine, ya sea docucéntrico o datacéntrico, va a variar el tratamiento archivístico que se realice a la información resguardada.

Según Serra (2005) el modelo docucéntrico:

> Parte de la posibilidad de dar forma documental a los agregados de información con valor evidencial que el sistema gestiona. El sistema o aplicación se reduce en este caso a una herramienta de generación de documentos, con las debidas garantías de seguridad y validez, pero sin la responsabilidad de contener dichos documentos y el modelo datacéntrico ante la imposibilidad de determinar qué partes de un sistema de información equivale a documentos de archivo, o en el caso de que sea estructuralmente imposible segregar estos documentos del sistema, se va considerar que todo el sistema de información corresponde a un documento de archivo (p. 6).

En el caso del modelo docucéntrico, se puede entender como los sistemas que producen y gestionan documentos o Sistemas de Gestión de Documentos Electrónicos, mientras que en el modelo datacéntrico, se basa en los datos, y utiliza un sistema de administración de bases de datos relacionales estándar. Una combinación de ambos sistemas, docucéntrico y datacéntrico, componen lo que se conoce como Sistemas de Preservación Digital, los cuales administran y preservan la

información contenida en los objetos digitales, y los datos que describen su contexto, estructura y contenido.

Es por lo anterior, que las instituciones deben tener claro lo que necesitan del sistema, debido a que de esto dependerá no solo el tipo de tratamiento que recibirá la información, sino también los requisitos legales a tener en cuenta para mantener la autenticidad e integridad de la información. Adicionalmente, no se deben obviar las políticas y lineamientos de seguridad, acceso, continuidad de negocios, el interés de las partes, entre otros.

Sin importar el tipo de modelo que se determine según las necesidades y peculiaridades de las organizaciones en los cuales se implementen, un sistema de información electrónica debe cumplir con las siguientes características, según la UNE-ISO 14641 (2015):

- Viabilidad de la preservación a largo plazo
- Integridad
- Seguridad
- Trazabilidad (p. 11).

Estas características son primordiales en cualquier sistema que produce, gestiona y preserva documentos de archivo, ya que sin estos elementos no se podría legitimar el valor probatorio de un documento ni su autenticidad.

1.5 Sistema de Gestión de Documentos Electrónicos

De acuerdo con la Norma Técnica para la Gestión de Documentos Electrónicos, emitida el 05 de mayo del 2018 por la Junta Administrativa del Archivo Nacional, se puede entender a un Sistema de Gestión de Documentos Electrónicos (SGDE) como un sistema informático cuya principal función es la de gestionar la producción, uso, mantenimiento y disposición de los documentos creados electrónicamente a efectos de proporcionar evidencia de las actividades de la institución.

Por su parte, a nivel internacional, el Modelo de Requisitos para Gestión de

Documentos Electrónicos desde el año 2010 estableció que un SGDE constituyen sistemas informáticos que se encuentran orientados al almacenamiento, administración, flujos de trabajo y procesos archivísticos, por lo cual este debe estar encaminado a organizar tanto documentos como imágenes digitales de manera centralizada, proporcionando de esta manera un acceso de manera sencilla a todos los usuarios.

Al contemplar las dos definiciones anteriores, se puede establecer que un SGDE constituye un conjunto de elementos destinados a garantizar la aplicación de procesos tales como la oficialización del documento de archivo, descripción, valoración, uso y acceso de los documentos en soporte digital, permitiendo de esta manera el uso cotidiano de los documentos dentro de una institución.

1.6 Interoperabilidad entre sistemas de información

En el contexto institucional del sector público costarricense se puede encontrar diversas organizaciones que tienen diferentes sistemas de información que soportan su quehacer cotidiano y por medio de los cuales se ejecutan las funciones asignadas, sin embargo, dentro de esta pluralidad resulta difícil identificar instituciones que apliquen estrategias y acciones que permitan la comunicación y el flujo de trabajo entre los sistemas.

Por medio de la interoperabilidad de los sistemas se logra avanzar con la preservación digital, pues permite la normalización y estandarización de los elementos tecnológicos que tienen influencia directa sobre la gestión de los objetos digitales, como pueden ser los formatos digitales y los metadatos, por nombrar algunos.

Por consiguiente, resulta de interés conocer y comprender qué es la interoperabilidad y de qué manera se puede alcanzar. El Código Nacional de Tecnologías Digitales (2020) citando a Gasco, M y otros (2010) define el concepto de interoperabilidad de la siguiente manera:

> (...) la habilidad de organizaciones y sistemas dispares y diversos para interactuar con objetivos consensuados y comunes y con la finalidad de obtener beneficios mutuos. La interacción implica que las organizaciones involucradas compartan información y conocimiento a través de sus procesos de negocio, mediante el intercambio de datos entre sus respectivos sistemas de tecnología de la información y las comunicaciones (p.99).

Asimismo, se deja claro que la interoperabilidad no consiste en un fin último, sino que representa un medio por el cual se puede alcanzar la optimización de los sistemas y por ende brindar un servicio más eficiente.

La interoperabilidad es un concepto que puede ser abarcado desde diferentes aristas, la Oficina de Cooperación de la Unión Europea en colaboración con la CEPAL (2007) definieron cuatro aspectos a considerarse, como lo son:

1. Semántica: se ocupa de asegurar que el significado de la información intercambiada sea entendible y sin ambigüedades.
2. Organizacional: define los objetivos organizacionales, se encarga de la modelación de procesos y promueve la colaboración administrativa para el intercambio de información.
3. Técnico: abarca los elementos técnicos, como el hardware, el software y telecomunicaciones, necesarios para la interconexión de sistemas computacionales.
4. Gobernanza: cubre los acuerdos tomados entre organizaciones que participan en el proceso de interoperabilidad y los compromisos adquiridos para alcanzarlos (p.13).

Para Voutssas, J (2009) la interoperabilidad representa un elemento fundamental para garantizar la accesibilidad de los documentos a largo plazo, pues este no debe estar atado a formatos específicos de un proveedor de software o de un sistema operativo, por lo tanto, considera que para alcanzar la interoperabilidad es necesario priorizar el uso de estándares abiertos y evitar los estándares propietarios (p. 82).

1.7 Repositorio de preservación

En la actualidad existen diferentes definiciones y conceptos relacionados a los repositorios, sin embargo, todas coinciden en que un repositorio es un lugar donde se resguarda, conserva y se accede a la información de manera controlada y que es interoperable con otros sistemas. No obstante, los tipos de repositorios varían dependiendo de su finalidad o del tipo de información que se desee resguardar.

En el caso de los repositorios de preservación de documentos de archivo que producen las organizaciones, estas características o requerimientos de los repositorios no varían, ya que se debe resguardar la producción documental como evidencia fiable y expresión testimonial de las actividades y funciones de la organización y sus miembros.

En este sentido, el Glosario de Preservación Archivística Digital (2014) define repositorio institucional como el "conjunto de servicios e instalaciones ofrecidos por una organización a los miembros de su comunidad para el manejo y diseminación de materiales digitales producidos por la organización y sus miembros" (Voutssas, J y Barnard, A, 2014, p. 189).

Las instituciones normalmente emplean una serie de herramientas, productos, servicios o sistemas para desarrollar sus funciones, por lo cual es fundamental garantizar y propiciar que los sistemas se logren relacionar para intercambiar información y utilizar la información de los otros sistemas, tanto para la generación y transferencia de la información como para procurar disminuir la pérdida de información o el riesgo de tener información incompleta o descontextualizada.

Una vez contemplado todo lo que conlleva y la importancia que tiene preservar y resguardar documentos digitales de archivo, es necesario tener estrategias de preservación con el fin de minimizar la aparición de riesgos que pueda tener como resultado la pérdida de información, de forma parcial o total.

Un componente de esta estrategia para evitar o minimizar el riesgo es disponer y ejecutar políticas y estrategias de preservación, acceso, metadatos, conservación,

protocolos de transferencia y planes de contingencia y continuidad del negocio; con el propósito de garantizar que los documentos estén disponibles y accesibles a largo plazo garantizando su autenticidad e integridad.

Asimismo, hay otros elementos que se deben tener presentes para decir que un repositorio digital es apto, algunas de estas se mencionan en la norma UNE-ISO 17068 (2020) cuando se establece que un repositorio, hablando en este caso, de terceros de confianza, debería estar equipado con las siguientes funciones:

- Captura, navegación y búsqueda de documentos electrónicos;
- Emisión de certificaciones (sic) y documentos electrónicos;
- Migración y recepción de documentos electrónicos;
- Conversión de formatos (sic) de documentos electrónicos;
- Comprobación de la integridad de los documentos electrónicos; y
- Cierre y disposición de los expedientes (sic) electrónicos (p. 24).

Estas características o funciones que debe poseer un repositorio desvelan las diversas áreas o ámbitos que se deben contemplar para asegurar la autenticidad, integridad, fiabilidad, acceso y trazabilidad de la información. Además de procurar que se ejecuten cada una de las funciones o procesos archivísticos.

Por su parte, la norma ISO-UNE 16363 destaca que un repositorio digital de confianza requiere de “una monitorización constante, planificación y mantenimiento, así como la implementación de estrategias y acciones conscientes para llevar a cabo su misión de conservación digital” (p. 21).

Por ende, la planificación se puede visualizar de manera integral donde se incluye aspectos económicos o de recurso humano (entiéndase compra de equipo, recurso humano calificado, licencias de software, etc), sino también lo relacionado con la logística de tiempos de acción, entrega de informes y procesos de mejora continua y actualización de las soluciones o herramientas tecnológicas y de las políticas y protocolos ya que combatir la obsolescencia tecnológica es un ejercicio continuo y no una meta que se alcanza.

Lo anterior, justifica establecer un ciclo de revisión y mejora continua de todos los componentes del repositorio, debido a que el servicio en general representa un activo estratégico de gran valor, además de que propicia la transparencia de los procesos mediante la comunicación del resultado de la auditoría o revisión de los procesos.

No obstante, muchas personas tienden a definir y decir que un repositorio digital es lo mismo que una base de datos o cumplen la misma función, cuando la realidad es otra. Según Trentin (1992), una base de datos es "un conjunto de datos estructurados y permanentes agrupados por su homogeneidad y relacionados entre ellos, organizados con la mínima redundancia para ser usados en aplicaciones diversas, de modo controlado" (p. 1).

Es decir, que uno de los principales requisitos de una base de datos es que los datos se agrupan o dividen según su homogeneidad y no así en los repositorios. En la práctica archivística es muy notable el hecho de que una característica fundamental del objeto de estudio es su carácter único e inequívoco, más sin embargo un mismo documento único puede encontrarse conformando parte de diferentes unidades documentales.

Los mejores repositorios integran o utilizan bases de datos como una herramienta importante en la persistencia y recuperación de los documentos, de forma que una base de datos es tan sólo uno de los componentes de una solución de repositorio digital, que es a su vez un componente de una solución de preservación digital.

Se dice que los mejores repositorios utilizan bases de datos para la persistencia de la información que contienen porque las bases de datos (concepto informático) aportan funcionalidades importantes a los repositorios, Trentin (1992) menciona las siguientes:

- Estarcompletamenteintegrado
- Asegurar la velocidad de acceso a la información
- Asegurar una completa gestión de los datos
- Asegurar la privacidad de la información
- Permitir un acceso competente a la información

- Asegurar la reconversión de los datos en caso de mal funcionamiento (p. 1).

También existen otros medios de almacenamiento como el servicio de alojamiento de archivos o la nube, el cual señala Delgado-Gómez, A (2013), es un modelo de almacenamiento de datos basado en redes de computadoras bajo demanda a una fuente compartida de recursos informáticos.

1.8 Archivo Digital

De acuerdo con la Norma UNE-ISO 14641-1, un Archivo Digital o Archivo Electrónico, se puede definir como el conjunto de acciones desarrolladas con el objetivo de identificar, capturar, clasificar, preservar, recuperar, visualizar y proporcionar acceso a los documentos con propósitos informativos o históricos, o de conservación requeridos para cumplir las obligaciones legales.

De igual forma, la Norma UNE-ISO 14721, como parte de sus objetivos, también define a un archivo en un entorno digital, como un archivo que una organización opera y a su vez puede formar parte de una organización más amplia, de personas y sistemas, y que además ha aceptado la responsabilidad de conservar información y mantenerla disponible para una comunidad determinada.

La persona encargada del Archivo Digital, según la norma anterior, se conoce como Senior Information Risk Owner (SIRO), el cual por lo general es un ejecutivo que conoce la política de riesgos de información de manera que lidera la gestión del riesgo de la información, lo que significa que su rol es de preservación documental.

Teniendo en cuenta las definiciones anteriores, se puede establecer una diferenciación entre el funcionamiento de un SGDE y el de un Archivo Digital, pues como lo exponen Cedeño-Molina, A., Granados-Peraza, N y otros (2015) un SGDE tiene por objetivo esencial facilitar el uso cotidiano de los documentos en el desarrollo de las actividades de la organización, por consiguiente soporta procesos de incorporación de documentos, registro de documentos, clasificación de documentos, evaluación de documentos, uso y trazabilidad; esto resulta posible por medio de la normalización de dichos procesos en la gestión de este tipo de sistemas, mientras que

un Archivo Digital ejecuta las estrategias y políticas necesarias para garantizar el acceso a información íntegra, fiable y usable, a través del tiempo.

1.9 Preservación Digital

La definición de preservación digital es explicada en el Glosario de Preservación Archivística Digital en la versión 4.0, desarrollado por Voutssas y Barnard (2014), en donde se señala que consiste en "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" (p. 174).

La conservación de documentos, término utilizado frecuentemente para dirigirse también a la preservación de documentos, (aunque no son lo mismo), también es definido por el Reglamento a la Ley N.º 7202, específicamente en el artículo 49, en donde se establece como: "la función cuyo objeto específico es evitar, detener y reparar el deterioro y los daños sufridos por los documentos, incluyendo la aplicación de métodos y técnicas de preservación y restauración" (p. 18).

Esto evidencia una serie de diferencias entre ambos términos, en donde la conservación se entiende como una función general que engloba a su vez métodos de preservación de documentos y la restauración de los mismos, mientras que la preservación involucra una serie de estrategias de índole preventivo ante posibles daños o pérdidas de documentos, que según las Directrices para la preservación del patrimonio digital (2003), en el caso del documento digital, no tiene sentido hablar de procesos de restauración, ni de detener el deterioro, ya que es imposible detener el proceso de obsolescencia tecnológica, por ello las estrategias de índole preventivo para garantizar el acceso a los datos íntegros y auténticos contenidos en los documentos digitales son las únicas aplicables. Se entiende programa de preservación como: "cualquier conjunto coherente de disposiciones tomadas para preservar materiales digitales" (p. 18).

Otro factor para la preservación de los documentos y que se debe tomar en consideración es la interoperabilidad de los sistemas, esto se refleja en los procesos de difusión y acceso suscritos en la ISO 14721, porque la interoperabilidad entre el

sistema de gestión de documentos y el repositorio de documentos, debe ser adecuada para no perder los metadatos, ni la información de descripción al momento de transferir los documentos, así como permitir su acceso a través del tiempo.

El Código Nacional de Tecnologías Digitales (2020) menciona que "se deben tomar en cuenta las mejores prácticas de interoperabilidad y los estándares internacionales para garantizar que los diferentes desarrollos de infraestructura puedan interactuar, conectarse y funcionar con otros sistemas del Estado sin ningún problema" (p. 73).

El factor principal en el tema de la preservación es la gestión de la obsolescencia tecnológica, según Sastre (2015), la obsolescencia se refiere a:

> La incapacidad de utilizar los elementos informáticos a causa de la propia evolución tecnológica. Un documento puede quedar inutilizado, no porque se haya deteriorado o haya dejado de funcionar, sino porque hayan desaparecido los elementos tecnológicos de su entorno original. Es lo que se conoce como documento huérfano (p. 8).

Por eso, analizar y seleccionar el formato en el que se almacenarán los documentos electrónicos, es la primera técnica preventiva para la pérdida de información por la obsolescencia, en el artículo titulado "Formatos de difusión y formatos de preservación de contenidos digitales" (2011), se define formato digital como:

> El sistema de codificación de la información para su posterior almacenamiento o tratamiento en un soporte informático (documentos trabajados desde los programas del ordenador) o digital (captura de imágenes, por ejemplo, desde un escáner, una cámara de fotos digital) (p. 11).

No obstante, la selección adecuada de formato por sí sola no es suficiente para gestionar la obsolescencia tecnológica, para ello es importante los métodos o técnicas complementarias de preservación digital en toda la gestión del objeto digital.

1.10 Objetos digitales

Con el cambio de paradigma experimentado en el contexto archivístico con la incursión de los soportes digitales en la producción y preservación de documentos, resulta de suma importancia la comprensión de este término y su diferenciación con otros conceptos.

Tanto el proyecto InterPARES como el modelo de preservación OAIS consideran al objeto digital como un objeto compuesto por una secuencia de bits, no obstante, InterPARES amplía este término y menciona que se puede tratar de una o más cadenas de bits con datos acerca del objeto documental representado, así como de los metadatos acerca de sus propiedades y, cuando sea necesario, los métodos para realizar operaciones sobre el objeto.

Por su parte, Barnard. A, Delgado. A y Voutssas (2014) agregan que también pueden ser conocidos como "objetos de información", además aseguran que un objeto digital autocontenido debe tener al menos los siguientes grupos de información:

- Información del propio contenido: consiste en la información propiamente dicha del documento: su texto, imagen, audio, etc. Es decir, el documento ensímismo.
- Información de la descripción para la preservación: contiene la información necesaria para la preservación apropiada del documento. La misma, de acuerdo con el modelo que se utilice, puede contener:
    - Información referencial o identificadores asociados a la información del contenido.
    - Información de la proveniencia o historia del documento (origen, cadena de custodia, acciones de conservación implementadas y sus efectos).
    - Información de contexto o las relaciones de la información del contenido con su entorno.
    - Información de autenticidad tecnológica, cuya función es indicar los mecanismos de autenticación aplicados sobre el documento.

- Información de empaquetado: une el contenido digital con sus metadatos asociados, permitiendo su identificación.
- Información descriptiva: facilita el acceso al contenido del documento (p. 210).

1.11 Estrategias de Preservación Digital

De acuerdo con el Glosario de Preservación Archivística Digital Versión 4.0 de InterPares (2014) la estrategia de preservación digital es un conjunto de objetivos y métodos coherentes para salvaguardar la autenticidad y asegurar la accesibilidad de los componentes digitales a lo largo del tiempo (p 109-110). Para ello es necesario la implementación de un Plan Estratégico de Preservación donde se establezcan las metas y objetivos, tanto a corto como a largo plazo, para alcanzar la misión del Archivo Digital concerniente a la preservación digital.

Los objetos digitales no son comprensibles o representables por sí mismos y se necesitan otros métodos para asegurar el acceso a largo plazo, por eso es importante el mantenimiento de los objetos digitales y de toda la información contenida. Entre los principales métodos de estrategias de preservación digital se encuentran:

I. **Conversión:**

La conversión es un proceso que debe aplicarse para gestionar la preservación digital, la norma UNE-ISO 13008: 2013 sobre procesos de migración y conversión de documentos electrónicos, define la conversión como el "proceso de transformación de los documentos de un formato a otro, manteniendo las características del documento" (p. 7). De esta manera, la conversión se diferencia del proceso de migración, pues se puede realizar la transferencia de los documentos de un sistema de almacenamiento o componente programático de acceso a otro sin modificar su contenido, pero alternando la estructura lógica o formato.

Lo que resulta clave en la conversión es el reconocimiento apropiado del formato y de la versión de este, para así aplicar el proceso de la manera más conveniente. Entre las razones para aplicar el proceso de conversión, según UNE-ISO 13008: 2013, se encuentra la descontinuación del formato original, es decir, la obsolescencia de

formatos, cuando un formato propietario debe convertirse a un formato abierto. Se debe tener en cuenta que los factores tecnológicos en los procesos de preservación de documentos digitales no son los únicos factores determinantes, por ello es necesario considerar factores de carácter legal, económico y de personal especializado.

En el caso de la conversión digital de documentos analógicos, se puede definir como el proceso que busca facilitar la difusión y proteger las copias originales evitando su uso. Como resultado de este proceso, surge la necesidad de custodiar y conservar la copia digital generada. Es así como, la conversión masiva de documentos analógicos a formatos digitales, junto con la fuerte expansión de los documentos nacidos digitales, provoca que diversas organizaciones comiencen a estudiar la problemática asociada a la preservación de esos recursos digitales desde mediados de la década de 1990 (Keefer y Gallart, 2003).

II. **Emulación:**

De acuerdo con Andrew Waugh y otros (2000) se puede definir la emulación como la acción que permite utilizar el software de aplicación original sin necesidad de mantener el sistema original, para explicar este proceso de mejor manera toma el ejemplo del error Y2K, en el año 2000, el cual permitió observar que las propias aplicaciones pueden contener errores que pueden causar la pérdida de información con el tiempo. De igual manera, señala que se deben contemplarse los siguientes aspectos:

- La aplicación original puede no capturar o preservar el conocimiento necesario para la preservación, por ejemplo, puede que no sea posible probar que la información no ha sido alterada.
- La emulación depende de preservar una cantidad significativa de información. Por ejemplo, una solución de emulación de hardware supone la preservación del emulador, el sistema operativo, la aplicación y los datos.
- El emulador es una aplicación de software en sí misma y deberá preservarse, ya sea emulando el sistema en el que se ejecuta o mediante una implementación periódica. La renovación precisa puede volverse difícil una vez que se pierde la familiaridad con el sistema que se emula.

Finalmente, aunque la emulación es una de las estrategias de conservación que se menciona en la literatura de la ciencia de la información, existe una crítica sobre este tipo de estrategia, ya que como menciona Serra (2001):

> (...) presenta un importante inconveniente: tanto la versión reducida del software original como el emulador también están sujetos a una progresiva obsolescencia, y su mantenimiento y actualización pueden ser muy difíciles, especialmente cuando dependan de una firma comercial que actúe exclusivamente en función de los intereses del mercado (p. 10).

Por lo tanto, este tipo de estrategia es fuente de discusión en el ámbito archivístico.

III. Migración

Siguiendo lo señalado por el modelo OAIS, plasmado posteriormente en la norma ISO 14721, se define la migración digital como el traspaso de información digital con el objetivo de conservarla en el tiempo. A su vez, se determinaron las motivaciones para el uso de la migración digital como estrategia de preservación:

- Mejorar la rentabilidad, pues con la constante evolución tanto del hardware como del software es común que su oferta en cuanto a capacidad de almacenamiento y anchos de banda de traspaso de información sea cada vez mayor, por lo que la migración a herramientas significa, por lo general, una mayor eficiencia y ahorro para los clientes y usuarios.
- Deterioro de los soportes, debido a la reducción progresiva de la fiabilidad de los soportes al momento de conservar bits de manera segura, lo cual conlleva a la necesidad de migrar a soportes modernos y actualizados de manera paulatina.

Por otra parte, en el ámbito nacional, el término de migración es definido jurídicamente por la norma técnica del documento electrónico en el Sistema Nacional de Archivos (2018), en su apartado II lo establece como:

> Proceso de transferir documentos electrónicos de un entorno de software/hardware o soporte de almacenamiento a otro entorno o soporte de almacenamiento con poca o ninguna alteración de su

estructura, y sin alteración del contenido y contexto.

Ambas definiciones, tanto la brindada por la ISO 14721 como la emitida por la norma técnica, coinciden en que la migración consiste en transferir información de un componente programático de acceso a otro o de un dispositivo de almacenamiento a otro, siempre y cuando se garantice que no existirá pérdida de datos y la continuidad de la información transferida.

La migración también se debe combinar con la estrategia de conversión de formatos, esta estrategia contempla la designación de formatos seguros, es decir, que sean fiables y auténticos, ya que la migración tiene como función principal:

> (…) la conversión del documento creado en un determinado entorno y codificado en un determinado formato, a otro formato para que funcione en una nueva plataforma informática más actual o estandarizada.
>
> Se parte de la idea de que los documentos deben ser accesibles a partir de los sistemas informáticos existentes en cada momento, lo que exige su migración periódica a formatos inteligibles por los sistemas actuales (Sastre, 2015 p. 15).

1.12 Propiedades Significativas

Uno de los aspectos esenciales para tener en cuenta, en materia de preservación digital es el poder garantizar la autenticidad, integridad, fidelidad y acceso de la información que se encuentra resguardada a largo plazo. Una forma de gestionar este aspecto es mediante la identificación y resguardo de las propiedades significativas que presentan los documentos electrónicos.

Según el proyecto de Investigación de las Propiedades Significativas del Contenido Electrónico a lo Largo del Tiempo (INSPECT, por sus siglas en inglés), las propiedades significativas “son aquellos aspectos del objeto digital que deben preservarse a lo largo del tiempo para que el objeto digital permanezca accesible y significativo” (2018).

Las propiedades significativas son las características que identifican y definen al documento electrónico, independientemente de las transformaciones que sufra durante su gestión, debido a que si se logra preservar se mantendrá la fijeza e integridad de la información que contiene y por tanto su valor como evidencia.

Dada la importancia que posee la identificación y la permanencia de las propiedades significativas, es de suma trascendencia identificarlas, en este sentido Castillo-Solano, M.G y Umaña-Alpízar, R (2018) citando a Serra mencionan que los tipos de propiedades significativas son:

- **Contenido**: Expresión de la información, no necesariamente en una forma humanamente legible (texto, imágenes, entre otros).
- **Contexto**: Información que permite la comprensión del entorno tecnológico y administrativo con el que se relaciona, así como su procedencia.
- **Estructura**: La organización de las partes que componen el objeto, y cómo se relacionan unas con otras (cabeceras, paginación, componentes criptográficos, entre otros).
- **Comportamiento**: Funcionalidades intrínsecas al objeto (enlaces hipertextuales, fechas actualizables, entre otros).
- **Apariencia**: La forma en que el contenido del objeto se visualiza ante un agente o usuario (fuentes de letra, colores, entre otros).

Como se evidencia de la cita anterior, las propiedades significativas abordan elementos esenciales a preservar en el tiempo con la intención de poder comprobar las características propias de los documentos de archivo como lo son la autenticidad, fiabilidad e integridad.

1.13 Formatos de preservación

De acuerdo con el Glosario de Preservación Archivística Digital Versión 4.0 (2014) la definición de un formato de archivo en el contexto informático es “la organización de los datos dentro de los objetos digitales, usualmente diseñada para facilitar el almacenamiento, recuperación, procesamiento, presentación y/o transmisión de esos datos por medio de algún programa”, por eso la elección de un formato en el tema de

preservación digital es un elemento esencial.

El Observatorio Vasco de la Cultura (2011) recomienda que, a la hora de seleccionar el formato más adecuado para un documento, se deben tener presentes dos factores:

I. **Factores de sostenibilidad**, que los formatos cuenten con:

Divulgación/Transparencia: que las especificaciones técnicas de los formatos sean accesibles (es decir son de código abierto).

Apertura: utilizar formatos abiertos, es decir formatos de archivo que no se hallan sujetos a patentes o derechos de autor.

Dependencia/Interoperabilidad: grado de dependencia de un formato determinado respecto a un hardware, a un dispositivo, programa o sistema operativo específico.

Estabilidad/Compatibilidad: grado en el que un formato mantiene su funcionalidad e integridad con versiones anteriores o posteriores.

Aceptación: hace referencia al grado de utilización de los formatos por parte de los creadores, distribuidores y usuarios de los recursos.

Estandarización: adecuación formal a los procesos o especificaciones establecidos por un organismo de normalización con el objetivo de garantizar la calidad de los archivos y su interoperabilidad.

Mecanismos de protección técnica: los mecanismos de protección técnica como por ejemplo el cifrado, utilizados habitualmente para proteger la propiedad intelectual, no deben dificultar la recuperación de datos, migración de los contenidos o su adaptación a nuevas necesidades derivadas de la evolución tecnológica.

II. **Factores de calidad y funcionalidad:** La elección del formato se fundamenta básicamente en su adecuación a las características del contenido y a las expectativas del usuario (p.13).

1. 14 Cadena de preservación

La custodia jurídica del documento de archivo es un concepto establecido por Hilary Jenkinson en el contexto de los Archivos desde 1922, en este sentido O'toole, J. (1994) describe que para Jenkinson era fundamental mantener una cadena ininterrumpida de custodia sobre los documentos para asegurar su autenticidad, pues consideraba que si las personas responsables de crearlos tienen la capacidad de mantenerlos a salvo de otras influencias que pudiesen romper con su carácter de autenticidad, estos podrían ser posteriormente utilizados como elementos de evidencia y prueba en procesos legales (p. 634).

Con la incursión en la producción de documentos en soportes digitales la idea inicial propuesta por Jenkinson tuvo que evolucionar y adaptarse a la especificidad de los documentos digitales, de tal manera que se garanticen las propiedades que aseguran la fiabilidad de la información digital, para que sirva como evidencia y prueba de las gestiones y acciones realizadas por la sociedad. Por lo tanto, para Flores, D (2020) es necesaria una nueva propuesta para la definición de la cadena de custodia de Archivo Digital, ya sea por la redefinición de la cadena de custodia o por la implementación operativa de la cadena de preservación.

Teniendo en cuenta la premisa anterior, el proyecto InterPARES 2 propone el modelo de cadena de preservación o COP, por sus siglas en inglés, por medio de la cual describe y documenta las fases que comprenden la gestión de los documentos de archivo digitales, así como los procesos que deben contemplar para garantizar la autenticidad de estos, dichas acciones se deben realizar en el transcurso de la gestión de los documentos, además, de ser aplicadas de forma interdependiente entre la figura del productor de documentos y el preservador, por lo que la omisión de cualquiera de los procesos en alguna de sus etapas pone en riesgo la fiabilidad y autenticidad de los documentos de archivo a lo largo del tiempo y de los cambios tecnológicos (Barnard, A. Delgado, A y Voutssas, J. 2017. p. 24).

1.15 Modelo de Referencia OAIS

Este modelo de referencia define los procesos para preservar y acceder, a largo plazo, a los objetos de información de forma efectiva. OAIS se trata de un modelo de referencia, por lo tanto, proporciona un marco estándar que va describiendo las funcionalidades básicas y los tipos de información requeridos para el entorno de preservación.

En la norma se identifican las responsabilidades obligatorias, así como las interacciones de las diversas partes interesadas de una organización, en el caso de la norma serían: productor, custodio y usuario, ya que son el entorno en el que opera e interactúa el modelo OAIS. Asimismo, aporta un método normalizado para la operatividad de los repositorios considerando las funciones archivísticas. Este modelo ha encontrado una gran aceptación entre las comunidades profesionales en ciencias de la información.

El modelo de referencia proporciona como objetivos principales, los siguientes:

- Proporcionar un marco para la comprensión y la creciente consciencia de los conceptos archivísticos necesarios para la preservación y acceso de información digital a largo plazo.
- Proporcionar los conceptos necesarios a las organizaciones no archivísticas para convertirse en participantes efectivos en el proceso de conservación.
- Proporcionar un marco para describir y comparar diferentes estrategias y técnicas de preservación a largo plazo.
- Proporcionar las bases para comparar los modelos de datos de información digital conservada por los archivos y para discutir cómo los modelos de datos y la información de base pueden cambiar en el tiempo.
- Proporcionar un marco que puede ser ampliado por otros esfuerzos para cubrir la preservación a largo plazo de información que no está en formato digital (UNE-ISO 14721, 2015).

De acuerdo con su base conceptual, la norma tiene como principio:

Conservar la información del contenido (*Content Information*), y hacerlo de

> forma comprensible para la comunidad designada, por lo que la información ha de ser representada de acuerdo con la base de conocimiento (*Knowledge Base*) de dicha comunidad; es decir, armonizar las herramientas de acceso con el conocimiento de los usuarios, sin perder de vista que dicho conocimiento evoluciona (Cruz-Mundet y Díez-Carrera, 2016, p. 228).

La información de contenido o *Content Information* está compuesta por la información contenida en el objeto (en nuestro caso un documento) y su Información de Representación asociada, necesaria para que la comunidad específica pueda entenderlo.

En cuanto al proceso de la preservación en el modelo OAIS, este se ejecuta en lo que se denomina como paquete de información (*Information Package*), el cual se conforma por 3 procedimientos: el Paquete de Transferencia de Información (*Submission Information Package*, SIP), que es el paquete o envoltorio que transmite el documento en cumplimiento del protocolo de transferencia definido; el Paquete de Información de Archivo (*ArchivalInformationPackage*, AIP) siendo este paquete el objeto de custodia almacenado para preservación en los repositorios. Por último, está el Paquete de Difusión de Información (*Dissemination Information Package*, DIP), el cual es el objeto retornado del contenido en custodia (tomado del AIP) proporcionado en respuesta a una solicitud por parte del usuario en cumplimiento de los protocolos de consulta establecidos.

La norma OAIS define tres tipos de componentes, los cuales son:

- **Modelo funcional**: está compuesto por seis entidades funcionales e interfaces relacionadas, las cuales son: Ingreso, Almacenamiento de Archivo, Gestión de Datos, Administración, Planificación de la Conservación y Acceso. Asimismo, incluye "servicios comunes" como Servicios del Sistema Operativo, Servicios de Red, Servicios de Seguridad.

- **Modelo de información**: describe en mayor profundidad la arquitectura funcional de un OAIS y una arquitectura de información para representar los Paquetes de Información y las Descripciones del Paquete e Información del

Empaquetado. Además, está pensado para ayudar a todo arquitecto o diseñador de sistemas de un futuro OAIS, si bien son conceptos no aplicables directamente en la práctica. De manera esquemática se estructura en tres partes (Cruz-Mundet y Díez-Carrera, 2016, p. 232): modelo lógico para la información de archivo, modelo lógico de información en un OAIS e Información sobre gestión de datos.

El modelo informático, expresa la existencia de los Paquetes de Información, definiéndolo como un contenedor que incluye dos tipos de objetos de información, la información de contenido y la información de descripción (IDC) (UNE-ISO 14721, 2015).

- **Transformaciones del empaquetado de información**: describe las "transformaciones, lógicas y físicas, de los Paquetes de Información y sus objetos asociados a medida que siguen un ciclo de vida desde el Productor hasta el OAIS, y del OAIS al Usuario" (UNE-ISO 14721, 2015, p. 81).

1.16 Metadatos

El uso de los metadatos en la preservación digital permite recopilar datos importantes de los documentos que se ingresan tanto a gestores como repositorios de la información, según Raventós-Pajares, P (2013), los metadatos pueden ser entendidos como:

Los datos que se utilizan para describir otros datos. Así como el conjunto de propiedades descriptivas sirven a una o más de las siguientes funciones:

1. Caracteriza de manera única un objeto: los valores asociados con las propiedades descriptivas permiten a un usuario, sea humano o sea una máquina, discriminar entre un objeto u otro. Certifica la autenticidad. Establece y documenta su contexto. Identifica y explota las relaciones estructurales que existen dentro y entre los objetos digitales.
2. Describe cómo se puede acceder al objeto y a su contenido: certifica el grado de integridad de ese contenido.

3. Contiene referencias de información que en un momento dado no forman parte explícitamente de un determinado conjunto de metadatos, pero que pueden ser puntos de control y procesamiento para otras aplicaciones o servicios (p. 3).

Como se puede ver en la definición anterior los metadatos juegan un papel muy importante en la misión de preservar la información, deben ser un elemento indispensable para la descripción de los objetos a conservar, y es aún más indispensable realizar una parametrización sobre el uso de estos elementos en los sistemas de información y su preservación.

Dada esta necesidad, se contemplan tanto el esquema de metadatos EAD (para los metadatos relacionados con ISAD-G) y el diccionario de metadatos de preservación PREMIS, dentro de una estructura METS, como una forma normalizada de coleccionar y organizar los metadatos.

Entiéndase esquema de metadatos como:

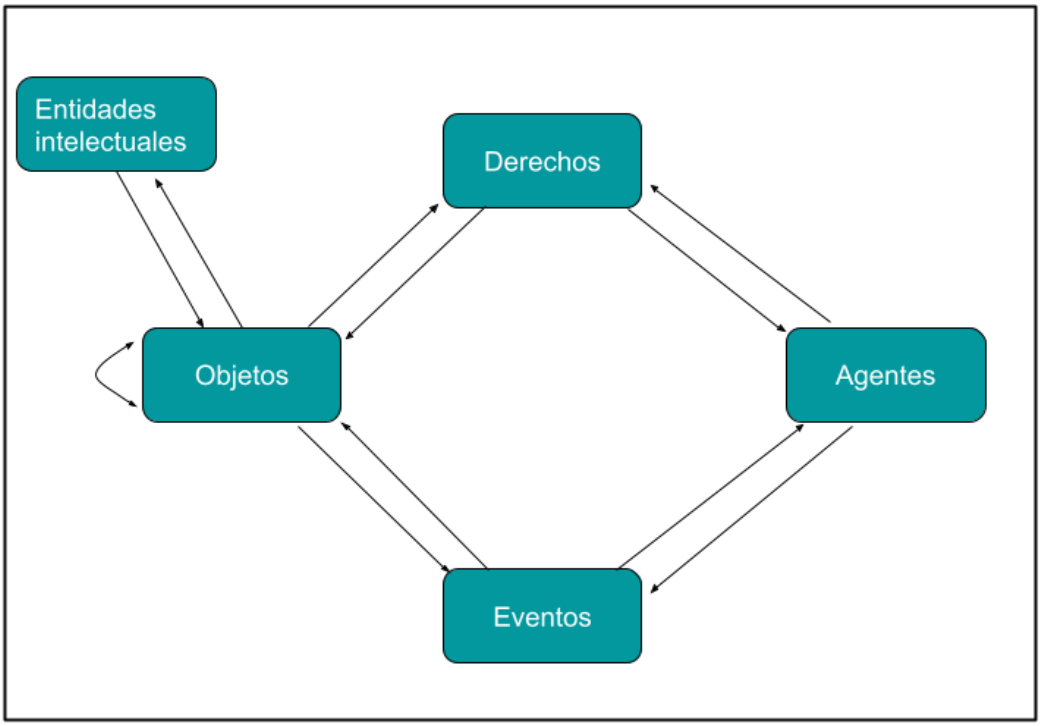
> Los esquemas de metadatos o simplemente esquema, son un conjunto de elementos diseñados para un fin específico, como puede ser la descripción de un objeto digital. La definición o el sentido de los propios elementos es conocida como la semántica del esquema. Los valores dados a los elementos de metadatos son el contenido. Esto quiere decir que los esquemas de metadatos en general especifican los nombres de los elementos que incorporan y su significado, es lo que se conoce como el modelo de datos o listado de datos (Raventós, P. 2013. p. 2).

1.17 PREMIS

El Diccionario de Metadatos PREMIS (*Preservation Metadata: Implementation Strategies*) define los metadatos de preservación como “la información que un repositorio utiliza para llevar a cabo el proceso de preservación digital. (...) metadatos destinados al mantenimiento de la viabilidad, la disponibilidad, la claridad, la autenticidad y la identidad en el contexto de la preservación” (2015, p. 9).

Este modelo de metadatos está conformado por cinco unidades semánticas, que tienen como fin específico describir los elementos que conforman el contexto de la preservación digital: Entidades Intelectuales, Objetos, Acontecimientos, Derechos y Agentes.

Figura 5. Unidades semánticas del modelo PREMIS



Fuente: Diccionario de datos PREMIS de metadatos de preservación (2015).

La imagen anterior se puede entender de la siguiente manera: "las entidades se representan mediante recuadros y las relaciones entre entidades mediante flechas. La dirección de la flecha indica el sentido de la conexión de la relación, tal y como se registra en los metadatos de preservación" (PREMIS, 2015, p. 11).

Las entidades anteriormente mencionadas son definidas, por el modelo de metadatos PREMIS (2015), de la siguiente manera:

- Entidad Intelectual: conjunto de contenidos que se considera una única unidad intelectual a efectos de gestión y descripción, por ejemplo, un libro, un mapa, una fotografía o una base de datos. Una Entidad Intelectual puede comprender

otras Entidades Intelectuales. Por ejemplo, un sitio web puede incluir una página web o una página web puede incluir una imagen. Una Entidad Intelectual puede tener una o más representaciones digitales.

- Objeto [digital]: unidad discreta de información en formato digital.
- Acontecimiento: acción que al menos afecta a un Objeto o Agente asociado o conocido por el repositorio de preservación.
- Agente: persona, organización o programa/sistema informático asociado a los Acontecimientos durante la vida de un Objeto, o a los Derechos ligados a un objeto.
- Derechos: declaración de uno o varios derechos o permisos pertenecientes a un Objeto o Agente (p. 12).

Cada una de estas entidades está conformada por una serie de unidades semánticas que se relacionan directamente con una o más entidades, el modelo define las unidades semánticas de la siguiente manera:

> Cada unidad semántica especificada en el Diccionario de Datos se mapea a una de las entidades del modelo de datos. En este sentido, una unidad semántica puede entenderse como una propiedad de una entidad. Por ejemplo, la unidad semántica size es una propiedad de la entidad Objeto. Las unidades semánticas poseen valores: para un objeto concreto el valor de size puede ser «843200004» (p. 12).

Existen determinados conceptos necesarios para el entendimiento y uso de este modelo, algunos de ellos son los siguientes:

- Contenedor: Una unidad semántica adquiere la forma de un contenedor que agrupa un conjunto de unidades semánticas relacionadas. Por ejemplo, la unidad semántica identifier (identificador) agrupa las unidades semánticas identifierType (tipo de identificador) e identifierValue (valor del identificador).
- Componentes semánticos del contenedor: las subunidades agrupadas en el contenedor.
- Contenedores de extensión: son aquellos que permiten el uso de

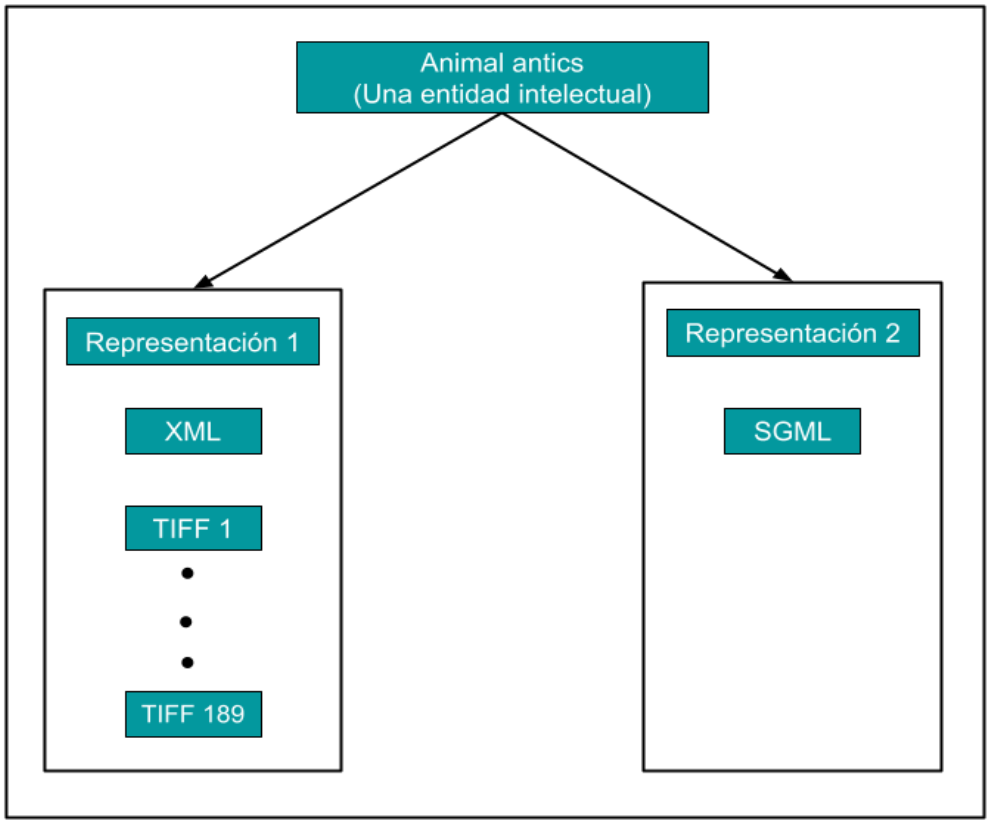
metadatos codificados según un esquema externo.

- Relación: es una declaración de asociación entre casos individuales de entidades. El término relación puede interpretarse en sentido lato o estricto, y expresarse de maneras muy diferentes. Por ejemplo, la afirmación «el Objeto A tiene un formato B» puede considerarse una relación entre A y B. El modelo PREMIS, sin embargo, trata el formato B como una propiedad del Objeto A. PREMIS reserva el concepto de relación para asociaciones entre dos o más entidades Objeto o entre entidades de distintos tipos, tales como un Objeto y un Agente (p. 13).

Uno de los elementos más importante de este esquema es el uso de representaciones de información, PREMIS define representaciones como: “El conjunto de ficheros necesarios para permitir la utilización de las entidades intelectuales a largo plazo” (2015, p. 14). Se pueden conservar más de una representación sobre un mismo objeto, puede ser una imagen con un fichero TIFF y el SGML, mediante el elemento fileGrp de METS; la única desventaja es que requiere más espacio para su almacenamiento.

Con la siguiente imagen se puede comprender de mejor forma en qué consiste una representación, se incluye un objeto o entidad intelectual y de ahí se desprenden todos los ficheros necesarios para conservar la información y datos necesarios.

Figura 6. Modelo de datos PREMIS



Fuente: Diccionario de datos PREMIS de metadatos de preservación (2015)

1.18 METS

Metadata Encoding & Transmission Standard (METS), es un esquema de codificación de metadatos que ofrece un formato basado en XML, que busca precisamente codificar los metadatos necesarios para la gestión de objetos digitales y su intercambio entre repositorios. Además, de acuerdo con la página web de la Biblioteca del Congreso de Estados Unidos, mencionan que "dependiendo de cómo se aplique, un documento METS podría usarse como un SIP, AIP o DIP, la elección de este último dependerá de las necesidades del cliente, dentro del modelo de referencia OAIS.

Un documento METS consta de siete secciones:

I. **Cabecera METS**: **<mets:metsHdr>**

Contiene metadatos que describen el propio documento METS, e incluye datos como

su productor, custodio, etc.

II. **Metadatos Descriptivos**: **<mets:dmdSec ID="ID">**

Esta sección puede: a) apuntar a metadatos descriptivos externos al documento METS (por ejemplo, un registro MARC en un OPAC o un documento EAD disponible en un servidor web); b) contener internamente los metadatos descriptivos, o c) combinar ambas aproximaciones. En la sección Metadatos Descriptivos se pueden incluir múltiples nodos que contienen distintos esquemas de metadatos descriptivos, tanto internos como externos.

III. **Metadatos Administrativos**: **<mets:amdSec ID="ID">**

Ofrece información sobre cómo se crearon y almacenaron los archivos que conforman el objeto digital, derechos de propiedad intelectual, metadatos sobre el objeto original a partir del cual se obtuvo la representación digital, e información sobre la procedencia de los archivos que conforman el objeto digital (es decir, relaciones entre copias maestras y derivadas, migraciones y transformaciones). Al igual que sucede con los metadatos descriptivos, los metadatos administrativos pueden ser externos o codificarse dentro del propio documento METS.

IV. **SecciónArchivo: <mets:fileSec>**

Lista todos los archivos con contenidos que forman parte del objeto digital. Los archivos pueden agruparse en elementos **<fileGrp>**, uno para cada una de las distintas versiones del objeto.

V. **MapaEstructural**: **<mets:structMap>**

Es la parte principal de un documento METS. Recoge la estructura jerárquica del objeto digital, y enlaza sus secciones con los archivos de contenido y los metadatos correspondientes a cada una de ellas.

VI. **Enlaces Estructurales**: **<mets:structLink>**

Permite registrar la existencia de hiperenlaces entre las secciones del mapa estructural. Tiene gran valor cuando se usa METS para guardar sitios web.

VII. Comportamientos: <mets:behaviorSec>

Se puede usar para vincular comportamientos ejecutables con los contenidos del documento METS. Cada comportamiento tiene una definición de interfaz y un "mecanismo" que identifica un módulo de código ejecutable que implementa y ejecuta el comportamiento definido de forma abstracta por la interfaz.

1.19 Continuidad del negocio

Debido a los avances tecnológicos y el cambio que esto representa, las organizaciones deben prepararse cada vez más para hacer frente a los eventos inesperados que ponen en peligro la información que considera como importante para cumplir con sus funciones, por lo que resulta de relevancia, desde el punto de vista de la preservación digital, tener herramientas que posibiliten la protección de la información digital ante los riesgos que trae consigo la virtualización de los procesos de trabajo.

De acuerdo con la norma UNE-ISO 22300 (2020), la continuidad de negocio se puede entender como la capacidad de la organización para continuar la entrega/prestación de productos o servicios a niveles predefinidos aceptables después de una disrupción, de esta manera, su gestión se constituye como un proceso integral que identifica las amenazas potenciales para la organización y el impacto que estas pueden tener, en caso de llegar a materializarse sobre las operaciones de negocio, además de suministrar un marco de referencia que le permita a la organización dar una respuesta eficaz (p. 10).

Por su parte Gaspar-Martínez, J. (2010), identificó una serie de objetivos específicos que deben buscarse alcanzar por medio de un plan de continuidad de negocio, los cuales son:

- Aumentar la probabilidad de continuidad de las funciones críticas de la organización en caso de que un incidente interrumpa las operaciones informáticas en las que se apoyan.
- Proporcionar un enfoque organizado y consolidado para dirigir actividades de

respuesta y recuperación ante cualquier incidente o interrupción de trabajo imprevista, evitando confusión y reduciendo la situación de tensión.

- Proporcionar una respuesta rápida y apropiada a cualquier incidente imprevisto.
- Recuperar las funciones críticas de negocio de manera oportuna.
- Reducir el tiempo de recuperación, y como consecuencia, las pérdidas económicas, directas e inducidas, como resultado de un desastre.
- Evitar la duplicidad de esfuerzos en la atención de imprevistos (p. 6).

Diversos organizaciones se han interesado en definir las pautas necesarias para la aplicación de un Sistema de Gestión de la Continuidad de Negocio (SGCN) a nivel institucional, en particular, la norma UNE-ISO 22300 (2020) ha definido a un SGCN como una parte del sistema de gestión que establece, implementa, opera, revisa, mantiene y mejora la continuidad de negocio, por lo tanto, por medio del sistema de gestión se definirán los recursos, servicios y actividades de planificación, las responsabilidades, los procedimientos y los recursos de una organización garantizar la continuidad de funciones críticas de negocio (p. 10). Por medio del siguiente cuadro se detallan algunas de las propuestas de modelos diseñados para la gestión de continuidad de negocio:

Cuadro 2. Modelos para la Gestión de la Continuidad de Negocio

Nombre	Descripción	Fases
Modelo NFPA 1600 Gestión de Emergencias y Desastres y Programas de Continuidad del Negocio.	Proporciona una serie de criterios con el objetivo de que las organizaciones logren desarrollar, implementar, evaluar y mantener un programa para la preparación, mitigación, reparación y continuidad de los procesos de negocio ante una situación adversa.	1. Gestión del Programa. 2. Planificación. 3. Implementación. 4. Pruebas y Ejercicios. 5. Mejoramiento del programa.
Modelo NIST Publicación Especial 800-34 Planeamiento de Contingencia para Sistemas de Información Federales.	Constituye una guía de planes de contingencia para que sean aplicados en sistemas de información.	1. Desarrollar la política del plan de contingencia. 2. Llevar a cabo el BIA (Business ImpactAnalysis). 3. Identificarcontrolespreventivos. 4. Crearestrategias de contingencia. 5. Pruebas, entrenamiento y ejercicios del plan. 6. Mantenerel plan.
Modelo para la implementación de prácticas globales de Gestión de Continuidad del Negocio.	Guía elaborada por el Business ContinuityInstitute (BCI) para gestión de la continuidad del negocio, por medio de la cual propone que sea abordado tomando en cuenta dos prácticas profesionales, como lo son: las prácticas de gestión y las prácticas técnicas.	1. Prácticas de Gestión. 1.a. Políticas y Gestión del Programa. 1.b. Integración de la gestión de continuidad del negocio en la cultura de la organización. 2. PrácticasTécnicas. 2.a. Entendimiento de la organización. 2.b. Determinación de estrategias de continuidad del negocio. 2.c. Desarrollar e implementar las respuestas. 2.d. Probar, Mantener y Revisar.
Modelo de buenas prácticas para la implementación de los requerimientos de la ISO 22301.	Actualización del Modelo Británico BS-25999 Sistema de Gestión de Continuidad del Negocio creado en el 2007, por medio del cual se	1. Contexto de la organización. 2. Liderazgo. 3. Planificación. 4. Apoyo.

Nombre	Descripción	Fases
	establece una serie de requisitos para implementar, mantener y mejorar un sistema de gestión de la continuidad de negocio.	5. Operación. 6. Estrategias de continuidad del negocio. 7. Establecer e implementar procedimientos de continuidad del negocio. 8. Respuesta a incidentes y planes de continuidad del negocio.

Fuente: Elaboración propia a partir de la información de Quevedo, J. (2012). Revisión de modelos de gestión de continuidad del negocio. Disponible en: https://revistasinvestigacion.unmsm.edu.pe/index.php/sistem/article/download/5620/4877/

Como se muestra en el cuadro 2, cada uno de los modelos proponen diferentes formas de abarcar la gestión de la continuidad del negocio, sin embargo, todos coinciden en que el proceso de continuidad de negocio debe partir teniendo en consideración el contexto organizacional, pues consideran que cada empresa o institución se pueden enfrentar a diferentes riesgos.

Por lo cual, resulta fundamental abarcar la gestión de riesgos como parte de la continuidad del negocio, ya que por medio de la evaluación de riesgo se permite aumentar la probabilidad y el impacto de las contingencias positivas, así como disminuir la probabilidad y el impacto de las negativas, para ello es necesario implementar un plan de gestión de riesgo. Según la norma UNE-ISO 31000 (2018), un plan para la gestión de riesgo consiste en un esquema de referencia para la gestión de riesgo que especifica los componentes y los recursos de la gestión que se van a aplicar.

De acuerdo con las normas internacionales, al planificar un sistema de gestión de seguridad de la información, es necesario que se tomen en cuenta el contexto de la organización, asimismo asegurar las responsabilidades y los roles pertinentes a la seguridad de la información y contemplar los lineamientos y políticas que se deben seguir para evaluar y mitigar los peligros.

Además, se deben planificar las acciones para tratar los riesgos y oportunidades, el cual es necesario para prevenir o reducir efectos indeseados, lograr la mejora

continua y finalmente integrar las acciones en los procesos del sistema de gestión de seguridad de la información.

2. Metodología

2.1 Tipo de Investigación

El tipo de investigación desarrollada es de carácter descriptivo, dado que establece un marco de referencia para la evaluación de soluciones de preservación digital en el país, mediante los requisitos mínimos necesarios que debe contemplar o establecer un producto o servicio de preservación digital en Costa Rica, por medio del análisis y descripción de referentes internacionales como normas, modelos y diversos proyectos del área en estudio.

Siguiendo lo establecido por Tamayo Tamayo (2003) se entiende que la investigación descriptiva: "comprende la descripción, registro, análisis e interpretación de la naturaleza actual, y la composición o procesos de los fenómenos. El enfoque se hace sobre conclusiones dominantes o sobre cómo una persona, grupo o cosa se conduce o funciona en el presente" (p. 46). Por lo cual, este tipo de investigación se enfoca en el establecimiento de requisitos para evaluar las características y singularidades de una solución de preservación digital.

Asimismo, el trabajo también integra la investigación exploratoria, ya que el tema desarrollado pertenece a un área poco estudiada en el país. De esta manera, se desarrolló una herramienta de evaluación integral disponible en línea, que sirve como una guía para que las instituciones adquieran soluciones de preservación digital confiables, con la cual se pretenden aclarar muchas dudas sobre el tema.

2.2 Enfoque de la Investigación

La presente investigación posee un enfoque mixto, es decir; incorpora tanto la parte cualitativa como la cuantitativa.

La investigación posee un enfoque cualitativo, debido a que se analizan referentes internacionales, mediante el cual se propone un marco de referencia para la

evaluación de soluciones de preservación digital basándose en la teoría y principios archivísticos, aplicados en el país.

Conjuntamente, se implementa el enfoque cuantitativo, puesto que, como parte del diagnóstico de la situación actual de la preservación digital de documentos en Costa Rica, se requirió aplicar una encuesta entre las instituciones del Sistema Nacional de Archivos que afirmaron disponer de repositorios documentales para documentos en soporte digital.

2.3 Modalidad de Graduación

Esta investigación se enmarca en la modalidad de seminario de graduación, y constituye un aporte original basado en los requisitos necesarios para poder evaluar soluciones de preservación digital en Costa Rica, siguiendo lo establecido en el marco jurídico nacional, normas y proyectos internacionales vinculados a la preservación digital sistémica.

2.4 Población

La población en estudio abarca a las instituciones que presentaron el Informe de Desarrollo Archivístico durante el período 2018-2019, ante la Dirección General del Archivo Nacional de Costa Rica, quien publicó mediante la Circular DSAE-02-2019 el Índice de Desarrollo Archivístico.

Específicamente, la población seleccionada corresponde a las instituciones que respondieron afirmativamente a la pregunta No.68 del Índice de Desarrollo Archivístico 2018-2019: ¿Existen repositorios documentales para los documentos en soporte digital? Un total de 91 instituciones respondieron afirmativamente.

2.4.1 Muestra

El tipo de muestreo aplicado en la presente investigación corresponde al muestreo probabilístico, ya que el conjunto de unidades estadísticas que componen la población en estudio tuvo una probabilidad conocida y no nula de ser incluida en la muestra.

Dentro del muestreo probabilístico se encuentran diversos métodos que permiten la elección de los elementos que compondrán la muestra, no obstante, el procedimiento elegido para la presente investigación es mayormente conocido como muestreo sistemático, dicho proceso consiste en la elección de un número al azar y agregar una cantidad fija para encontrar el total de los elementos que completan la muestra.

Por medio es este proceso se logra asegurar la representatividad de la población analizada en la investigación, ya que se garantiza la aleatoriedad en la elección de los elementos, eliminando la probabilidad de una muestra sesgada debido a la subjetividad de los investigadores, además de permitir inferir en algunas propiedades de la población abarcada.

El procedimiento para determinar el tamaño de la muestra se toma en cuenta la siguiente fórmula sobre el cálculo del tamaño de la muestra:

$$n = \frac{Z^2 x N x p x (1-9)}{e^2 x (N-1) + Z^2 x\ p\ x (1-p)}$$

A partir de la aplicación de la fórmula se determinó una muestra de 74 Archivos del Sistema Nacional de Archivos que respondieron afirmativamente a la pregunta No.68 del Índice de Desarrollo Archivístico 2018-2019.

$$n = \frac{1.96^2 x 91 x 0.5 x (1-0.5)}{0.05^2 x (91-1) + 1.96^2\ x\ 0.5\ x\ (1-0.5)}$$

En donde:

n= muestra

N= 91 (es el tamaño de la población o universo (número total de posibles encuestados))

z= 1.96 (nivel de confianza) que equivale a un 95%

e= 0.05 (variable de error muestral) que equivale a un 5%

p = 0.5 (proporción aproximada del fenómeno en estudio en la población de referencia)

q = 0.5 (proporción de la población de referencia que no presenta el fenómeno en estudio, es decir (1 -p)

En el caso de p y q la suma siempre debe dar 1.

2.5 Técnicas de recolección de datos

Para el desarrollo del trabajo se emplearon diversas técnicas de recolección de datos entre las cuales se pueden mencionar:

- La entrevista: mediante esta técnica de recolección de datos se reunió el criterio y el testimonio de funcionarios implicados en proyectos de preservación, con el fin de obtener información sobre la aplicación de medidas empleadas hacia la preservación digital a nivel nacional, la cual se desarrolló a través de una entrevista semiestructurada.
- El análisis documental: permite recolectar datos de fuentes secundarias comolibros, leyes, revistas y periódicos que se utilizan como fuentes para recolección de datos sobre las variables de interés.
- La encuesta: por medio de esta técnica se recopiló datos que permitieron mostrar el estado actual de las instituciones del sector público en relación con el establecimiento y aplicación de medidas orientadas para garantizar la preservación digital, y se aplicó a una muestra representativa de la población en estudio, por medio de un cuestionario con preguntas abiertas y cerradas.
- Tormenta de ideas: mediante esta técnica se logra la identificación de los riesgos asociados a la preservación digital, así como las causas y consecuencias asociadas, los eventos que pueden ocasionar el riesgo, y las opciones para su tratamiento.
- Nudo de corbata de pajarita (en adelante corbatín): por medio de esta técnica de apreciación del riesgo, se logra diagramar de forma sencilla y clara desde las causas hasta las consecuencias de un riesgo, representado por el nudo de un corbatín.

2.6 Fuentes de información

Para el desarrollo de la presente investigación se consultaron diversas fuentes de información, tanto primarias como secundarias.

- Fuentes primarias: legislación nacional sobre documento electrónico, normas internacionales, trabajos finales de graduación en temas relacionados a preservación digital.
- Fuentes secundarias: artículos científicos de bases de datos a texto completo como Dialnet, ibersid, entre otros.
- Obras de referencia: Diccionario de Terminología Archivística.

CAPÍTULO III.
DIAGNÓSTICO DE LA SITUACIÓN ACTUAL DEL SISTEMA NACIONAL DE ARCHIVOS EN MATERIA DE PRESERVACIÓN DIGITAL.

CAPÍTULO III. DIAGNÓSTICO DE LA SITUACIÓN ACTUAL

El presente apartado pretende obtener información que permita reflejar el estado actual de la preservación digital de documentos en Costa Rica, para ello, se analizó el contexto normativo actual que cubre a las instituciones del sector público costarricense, con el fin de determinar las herramientas jurídicas con las que disponen, además, se detallan los resultados arrojados por la encuesta aplicada a las instituciones del Sistema Nacional de Archivos (SNA), por medio de la cual se logró conocer las condiciones imperantes en el proceso de preservación de la información digital, evidenciando tanto las fortalezas como las debilidades.

Por último, se expone una comparación de soluciones de preservación digital, así como de proveedores disponibles en el mercado que prestan el servicio de almacenamiento digital, lo cual, por ningún motivo debe confundirse como una alternativa para la preservación de la información digital.

1. Análisis normativo nacional

La preservación de la información contenida en documentos digitales es pieza clave dentro de las instituciones y debe estar asegurada a través de requerimientos técnicos, físicos y lógicos. Cada país debe proveer instrucciones de seguridad, para garantizar que la autenticidad, integridad y fiabilidad de la información registrada en los documentos y por tanto en los archivos, es oportuna y completa para su accesibilidad en el tiempo.

La Junta Administrativa del Archivo Nacional es la máxima autoridad del SNA, actúa como órgano rector y es el encargado de establecer las políticas archivísticas para las instituciones pertenecientes al sistema, además de recomendar estrategias para el desarrollo del SNA. Como parte de la estrategia de transformación digital, el Archivo Nacional anunció proyectos en materia de preservación digital, los cuales no han sido concretados. Tampoco se han reglamentado estándares o modelos de preservación normalizados.

Por lo tanto, las instituciones pertenecientes al SNA, actúan como encargadas de definir y aplicar las estrategias para la estructuración de su sistema de preservación de documentos digitales, basándose en legislación archivística nacional vigente o en el criterio de profesionales de Tecnologías de Información.

Las causas de la situación antes descrita pueden deberse a distintos factores. Por una parte, la inoperancia del Archivo Nacional, en la modernización y adquisición de conocimiento en preservación de la información digital; así como en emitir recomendaciones y procedimientos técnicos para la adquisición o desarrollo de sistemas de preservación digital para las instituciones del SNA.

Por otra parte, la necesidad de legislar aspectos relevantes sobre la autenticidad, integridad, fiabilidad, usabilidad y seguridad del documento electrónico, así como su conservación a largo plazo, ha derivado la generación de normativa específica que se encuentra dispersa en diferentes cuerpos normativos, tal como se detalla en el cuadro 3:

Cuadro 3. Normas relacionadas con preservación digital en Costa Rica

Tipo de norma	Número	Año	Objeto
Ley de Certificados, Firmas Digitales y Documentos Electrónicos.	8454	2005	Reconocimiento de la equivalencia funcional del documento electrónico con firma digital.
Reglamento a la Ley del Sistema Nacional de Archivos.	40554 -C	2017	Regula el funcionamiento de los órganos del Sistema Nacional de Archivos.
Norma técnica para la gestión de documentos electrónicos en el Sistema Nacional de Archivos.	Acuerdo 7	2018	Por medio de la cual se regula lo relativo al documento electrónico, su gestión, y conservación a largo plazo, dirigida a todas las instituciones que conforman el Sistema Nacional de Archivos.
Normas técnicas para la gestión y el control de las Tecnologías de Información.	R-DC-17-2020	2020	Establece los criterios básicos de control que deben observarse en la gestión de tecnologías de información, como instrumento esencial en la prestación de los servicios públicos.
Código Nacional de Tecnologías Digitales.	CNTD	2020	Por el cual se establecen los mínimos deseables para la adquisición, desarrollo y gestión de las tecnologías y los servicios digitales en el sector público costarricense.

Fuente: elaboración propia.

Ahondando más en esta normativa, en materia de preservación digital, se destaca lo siguiente:

1.1 Ley del Sistema Nacional de Archivos y su Reglamento

La Ley N.º 7202 del Sistema Nacional de Archivos y su reglamento, disponen que todas las instituciones públicas de Costa Rica deberán tener archivos organizados para conservar documentos en cualquier soporte. Por un lado, la Ley 7202, marca los lineamientos a seguir y puede interpretarse a la luz de la nueva técnica y recursos virtualizados; un ejemplo de ello es cuando especifica la obligatoriedad de la existencia de un depósito en condiciones para el acervo documental, así también se

requiere entonces la existencia de un repositorio en condiciones para el acervo digital, ya que cumplen con el mismo propósito.

Mientras tanto, el Reglamento a la Ley 7202, en lasección III Conservación de documentos, señala la responsabilidad de los archivos en establecer los mecanismos y procedimientos necesarios para asegurar la autenticidad, integridad, inalterabilidad y disponibilidad de los documentos electrónicos de archivo, en el largo plazo. Para ello, reglamenta con el artículo 87, una serie de medidas básicas de preservación de documentos en soporte electrónico.

Sin embargo, los "mecanismos y procedimientos" señalados anteriormente, no están normados en un estándar técnico específico para la preservación de la información digital. Por tanto, queda bajo el criterio de las instituciones y sus funcionarios, la elección de los procedimientos que crean convenientes en apego al cumplimiento de la normativa vigente.

1.2 Ley de Certificados, Firmas Digitales y Documentos Electrónicos

La Ley N.º 8454 establece la equivalencia jurídica de un documento electrónico con firma digital certificada con un documento en soporte en papel y con firma rúbrica. Además, en el artículo 6 establece en materia de conservación de documentos electrónicos que si opta por conservar en ese soporte se debe aplicar las medidas de seguridad necesarias para garantizar la inalterabilidad, el acceso o consulta posterior y su preservación a largo plazo.

En cuanto a la migración, en el mismo artículo se indica que cuando se trate de registros, archivos o respaldos que por ley deban ser conservados, deberá tener, previamente, la autorización de la autoridad competente.

1.3 Norma Técnica para la Gestión de Documentos Electrónicos

La norma publicada en Alcance Digital N.º 105 de La Gaceta N.º 105 de la fecha 21-05-2018, señala que en el SNA son las propias instituciones quienes deben coordinar todos los aspectos técnicos relativos a la preservación de sus documentos digitales.

El apartado número 2 de la norma, indica condiciones mínimas para la conservación de documentos electrónicos, en donde establece en su medida número 10, la necesidad de disponer de la infraestructura digital requerida para la preservación, por lo que insta a las instituciones a:

> a) Disponer de un repositorio digital que permita de manera segura almacenar a través del tiempo los documentos y control de los flujos de almacenamiento y consulta.
>
> e) Investigar y aplicar las buenas prácticas reflejadas en las normas nacionales e internacionales, con el objeto de preservar a lo largo del tiempo los documentos digitales.

Por consiguiente, como se muestra en los apartados mencionados, la norma dicta acciones generales para hacerle frente a la necesidad de preservar los documentos electrónicos, sin embargo, no profundiza en problemáticas como la obsolescencia tecnológica y la limitada capacidad del almacenamiento para enfrentar el cambio hacia una producción documental en soporte digital, esto pese a tratarse de una norma que busca abarcar la gestión de documentos electrónicos de una manera integral.

1.4 Normas Técnicas para la Gestión y el Control de las Tecnologías de Información

Es una normativa de acatamiento obligatorio para la Contraloría General de la República y las instituciones y órganos sujetos a su fiscalización. La norma establece diversos criterios de control, entre ellos, el de seguridad de la información, para garantizar la confidencialidad, integridad y disponibilidad de la información.

Es una norma que obliga a las instituciones a implementar una política de seguridad de la información, así como, tener los procedimientos correspondientes y asignar los recursos necesarios para lograr los niveles de seguridad requeridos. Sin embargo, no hace referencia a preservación digital y, por ende, tampoco a los repositorios de preservación digital; en consecuencia, pueden adquirirse sistemas electrónicos sin los

requisitos técnicos para preservación y que rápidamente se convierten en obsoletos, eventualmente generando pérdida de tiempo, recursos e información vital para las organizaciones y los ciudadanos.

Es importante señalar que de acuerdo con la resolución R-DC-17-2020 de la Contraloría General de la República del diecisiete de marzo del dos mil veinte, deroga las normas técnicas para la gestión y el control de las tecnologías de información (N-2-2007-CO-DFOE), resolución N.º R-CO-26-2007, y modifica las normas de control interno para el sector público.

1.5 Código Nacional de Tecnologías Digitales (CNTD)

Por su parte, el CNTD, publicado en el año 2020 es bastante extenso y exhaustivo, ya que se basa en un compendio de políticas públicas que establecen mínimos deseables para la adquisición, uso y desarrollo de las tecnologías de información y la comunicación en el Sector Público Costarricense. Sin embargo, a pesar de su amplitud y su estrecha relación con el ámbito tecnológico es una de las escasas normas que existen en el país que considera la importancia de la preservación digital.

Contempla como una de sus líneas de estandarización el acceso universal de todas las personas, independientemente de su condición, a la información generada o adquirida por medios digitales. Para ello, el CNTD pretende brindar un marco de referencia de seguridad tecnológica, interoperabilidad y neutralidad tecnológica en sistemas de información orientados a la presentación de servicios digitales, y hacia un esquema de trabajo de carga distribuida y con capacidad de interoperar.

El CNTD recomienda que, para la gestión de interoperabilidad de archivos digitales abiertos, la transferencia de documentos digitales entre sistemas sea por medio de paquetes de información de transferencia (SIP), y para su preservación por medio de paquetes de información de archivo (AIP), según se establece en la normativa OAIS (ISO 14721:2015).

Por último, otro aspecto importante que desarrolla esta normativa es la gestión de metadatos para intercambio de documentos digitales, entre los metadatos existentes

que se deben considerar están los metadatos para descripción y preservación. Disponer de metadatos de codificación o estructura como el estándar METS y el diccionario de datos PREMIS juega un papel vital, pues ofrecen la viabilidad para que un objeto digital continúe existiendo y permanezca accesible y usable, y por tanto, se puede interpretar su significado e intención a lo largo del tiempo; además permite identificar la versión original, duplicados, ediciones o modificaciones de la versión original.

2. Proyectos de preservación digital de documentos en Costa Rica

Mediante el presente apartado se examinarán los proyectos orientados a la implementación de soluciones de preservación digital de documentos en Costa Rica; por lo cual se expondrán los objetivos, el alcance en su aplicación, las estrategias establecidas y las funcionalidades de las soluciones, así como el estado actual en el que se encuentran.

2.1 Archivo Universitario Rafael Obregón Loría (AUROL)

El proyecto de Archivo Digital de la Universidad de Costa Rica (ADUCR) fue la primera iniciativa sobre preservación digital en Costa Rica, aunque no se llegó a formalizar e implementar, se adquirió conocimiento que fue utilizado posteriormente en los cursos de la Sección de Archivística de la Escuela de Historia, además, de poner en la palestra la problemática y proponer una metodología para que sea abordada.

A. Contexto del proyecto

La propuesta para establecer un Archivo Digital para la Universidad de Costa Rica se comenzó a gestar conforme los sistemas de información institucionales empezaron a generar documentos electrónicos originales que debían ser conservados, de tal forma que se mantuvieran sus propiedades, a mediano y largo plazo; identificando así la ausencia de herramientas y pautas necesarias para cumplir con esta premisa.

Por consiguiente, durante el 2013 se creó un equipo interdisciplinario conformado por funcionarios del Archivo Universitario Rafael Obregón Loría (AUROL), el Centro de Informática, la Unidad de Gestión de Proyectos, la Sección de Archivística de la Escuela de Historia y un colaborador externo, el Máster Jordi Serra Serra experto en preservación digital, dicho grupo de trabajo se planteó evaluar y presentar una respuesta metodológica a las necesidades encontradas.

B. **Alcance**

Con la implementación de este proyecto se buscó conservar y permitir el acceso a los documentos, datos y cualquier tipo de evidencia de información en formato digital producto de las funciones de la Universidad de Costa Rica, por lo que abarcaría a cada una de las unidades que componen a la institución.

Para obtener un resultado que se adecuara a las necesidades institucionales presentes en ese entonces, el equipo de trabajo elaboró una política institucional de preservación digital, la definición de requisitos funcionales del Archivo Digital y el establecimiento de un modelo de protocolo de ingreso y custodia para los paquetes archivísticos que se generarían.

C. **Servicios, funcionalidades y estrategias**

Como punto de partida se llevó a cabo la evaluación de riesgos que afectaba la conservación de los documentos electrónicos producidos en la Universidad de Costa Rica como parte del cumplimiento de sus funciones, este análisis se basó en la aplicación de un cuestionario específico autoevaluable (Digital continuityself-assessmenttool), desarrollado por los Archivos Nacionales del Reino Unido en el marco del Digital Continuity Project en el 2011, yfue completado por las unidades que a su vez formaban parte del equipo interdisciplinario a cargo del proyecto.

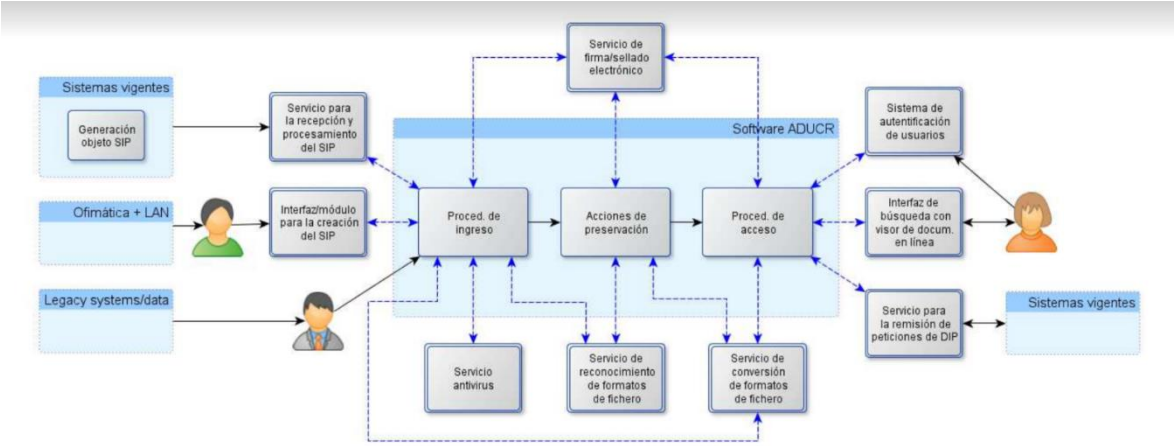
Por medio del cual se identificaron las situaciones que afectaban a la institución en materia de preservación y que debían ser subsanados, como por ejemplo: el almacenamiento de documentos y datos en sistemas obsoletos, la no vinculación de los sistemas con el valor de la información ni la normativa que los afecta o el almacenamiento de información en discos externos, discos duros locales, servidores

de correo electrónico, sistemas de gestión documental y servicios en la nube que funcionaban sin ningún tipo de normalización basada en la teoría archivística.

De acuerdo con las limitaciones detectadas, plantearon establecer una política que posicionara la importancia de la preservación digital a nivel institucional, donde se asignaban las responsabilidades y se fijaban los parámetros funcionales y técnicos del ADUCR.

El modelo funcional buscaba seguir lo propuesto por el modelo OAIS, por medio de la aplicación de sus entidades funcionales, por lo que el escenario planteado se centraba en una solución de archivo digital basada en un software de *Open Source*, no obstante, debía ser complementada por servicios externos que cumplieran a cabalidad lo requerido por un sistema de preservación digital basado en OAIS, por lo que se previó, que el funcionamiento de la solución debía actuar de la siguiente manera:

Figura 7. Escenario tecnológico inicial de ADUCR



Fuente: AUROL. (2013). Proyecto de preservación digital para la Universidad de Costa Rica. Modelo funcional y técnico del archivo digital.

Paralelamente con el escenario tecnológico inicial, la estrategia de preservación presentaba seis planes de trabajo en concordancia con el funcionamiento del ADUCR, los mismos fueron divididos de la siguiente forma:

- Plan de datos: define el uso de contenedores de información (paquetes de información) descritos por el modelo OAIS como los SIP, AIP y DIP para la

transferencia, almacenamiento y acceso a la información ingresada en el ADUCR.

- Plan de ingresos: se detallan cuáles serán los elementos que podrán ingresar al archivo digital, quienes serán los encargados de elaborar los protocolos correspondientes y de qué manera se realizará la transferencia de los paquetes de información.
- Plan de conservación: como parte de la estrategia de conservación de los objetos digitales, se propuso la normalización de los formatos admitidos por el sistema con base en lo establecido por PRONOM, por otra parte, para contrarrestar la obsolescencia tecnológica se formuló la exploración de formatos a través de registros y fuentes de información fiable, además, de la suscripción a servicios de alerta junto con el testeo de lectura y/o ejecución de una muestra significativa de todos los formatos conservados; por último, se sugirió la ejecución del proceso de migración de los AIP con representaciones afectadas por el formato obsoleto.
- Plan de acceso: se definen las comunidades designadas de usuarios del archivo digital, por lo que se identifica la base de conocimientos de estos grupos y el tipo de servicio que adquieren, además, se establecieron los mecanismos para la obtención de documentos por parte de los usuarios, de esta manera los documentos se lograrían visualizar tanto en línea como por medio de la descarga, de tal manera que obtendrían copias auténticas que se facilitan en forma de paquete de información de acceso. No obstante, el acceso no puede ser anónimo, por consiguiente, todos los usuarios tendrían que acceder por medio de autentificación previa y quedaría sujeto a la protección de datos confidenciales y personales definida en la normativa relacionada a los documentos.
- Plan de tecnología: los requisitos planteados buscan garantizar la integridad y la disponibilidad de todos los objetos digitales almacenados, a través del cumplimiento normativo y procedimental de seguridad de servicios de información de la institución en lo que respecta al control de accesos, verificación de integridad, protección contra ataques internos, y protección contra ataques externos y desastres. De la misma manera, se incorpora la necesidad de tener medidas que permitan el monitoreo de la continuidad en la

vigencia del software y hardware usados, cantidad de usuarios concurrentes por forma de acceso, continuidad de la prestación de servicio por parte del proveedor, el volumen de ingresos y la cantidad de migraciones y operaciones de preservación.

- Plan de continuidad: se estructuró desde diversas perspectivas como en la capacidad financiera para garantizar el funcionamiento del archivo digital, continuidad en caso de cambio de personal encargado del proyecto, en caso de cierre o desaparición de la institución y en caso de desastres (AUROL, 2013).

Por ese motivo, el proyecto para establecer un Archivo Digital en la Universidad de Costa Rica representó uno de los primeros esfuerzos en el país destinados a abarcar la preservación digital de los objetos digitales generados por una organización en el ejercicio de sus funciones, pese a no llegar a implementarse a los niveles que se tenían previstos sirvió como modelo para que otras instituciones públicas fijarán su atención en dicha problemática y sumarán esfuerzos para aportar al respecto, y que sirvió de base para el proyecto ADN del Archivo Nacional.

2.2 Proyecto Archivo Nacional Digital (ADN)

La información suministrada a continuación se recopiló por medio de una entrevista realizada a Natalia Cantillano Mora, Coordinadora del Departamento de Servicios Archivísticos Externos junto con Luis Carlo Rojas Mora, profesional de la Unidad de Servicios Técnicos Archivísticos, ambos formaron parte del equipo de trabajo responsable de diseñar y ejecutar el proyecto denominado ADN, por medio de esta se pretende identificar y comprender el proyecto ADN y sus implicaciones sobre el estado actual de la preservación digital en Costa Rica.

A. Contexto del proyecto

Este proyecto nace debido a la influencia de la promulgación del documento titulado como “Estrategia de Transformación Digital hacia la Costa Rica del Bicentenario, 2018-2022” impulsada desde el Gobierno de la República y por la Directriz N°019-MP-MICITT, en donde se propone que a partir del 1ero de diciembre del 2020, la administración central deberá producir al menos un 75% de sus documentos en soporte electrónico con firma digital, lo anterior representa un incremento escalonado

a corto y mediano plazo de la producción documental en soporte digital, lo cual ha coincidido con el Plan de Acción de Estado Abierto y el objetivo de carbono neutralidad, lo que ha incentivado, aún más, el uso de herramientas tecnológicas y la disminución gradual del uso del papel para la producción de documentos.

Al contemplar este contexto, el Archivo Nacional se vio en la obligación de tomar medidas que le permitiera estar preparado, pues como lo estipula el artículo 53 de la Ley 7202 del Sistema Nacional de Archivos: el Presidente de la República y sus respectivos Ministerios deben transferir a la Dirección General del Archivo Nacional todos los documentos generados y recibidos por sus despachos, que hayan concluido su trámite de gestión, al terminar el periodo presidencial de cuatro años; de tal manera que la capacidad del Archivo Nacional para la recepción, gestión y custodia de estos documentos debe verse ampliada en los próximos meses.

Por consiguiente, se definió la necesidad de disponer de un repositorio digital que almacene y preserve los fondos documentales que van a ser transferidos en este soporte. Ante esta situación, a partir del 18 de febrero del 2019, comenzó el trabajo de un equipo interdisciplinario conformado por personal especializado del Archivo Nacional, el cual tenía la misión de implementar una solución que cumpliera con los requerimientos legales y funcionales para gestionar y preservar documentos.

De esta manera, por medio del ADN se pretende implementar un servicio de preservación digital de documentos a todas las instituciones que conforman el SNA, dicho servicio incluiría el acompañamiento archivístico y tecnológico para la puesta en marcha de la solución digital, el software de preservación, almacenamiento y soporte técnico.

B. **Alcance**

Durante el año 2019 e inicios del 2020, la Unidad de Servicios Técnicos Archivísticos del Departamento de Servicios Archivísticos Externos trabajó en el diseño de un proyecto para la implementación de una solución de preservación de documentos digitales, la cual se pretende aplicar de manera incremental, lo que significa que la solución recoge los elementos mínimos necesarios, pasando por lo

deseable hasta alcanzar una solución ideal, para ello se aplicó, en primera instancia, un plan piloto que cubrió al Archivo Nacional y al Ministerio de Cultura y Juventud, por medio del cual se lograron identificar oportunidades de mejora en la gestión del cambio que esto representa, lo anterior con miras a cubrir a las instituciones del SNA que deseen adquirir el servicio.

C. **Servicio**

Al adentrarse en las funcionalidades de la solución ADN, se reconoce la intención del equipo de trabajo de implementar un servicio integral, que no solo se encargue de la preservación de los documentos, sino que también suministre una serie de herramientas básicas que incentiven la normalización de la producción de documentos y su respectiva gestión, para ello se establecieron cinco servicios que se describen a continuación:

Implementación, normativa y capacitación: esta fase proporciona una serie de servicios que incluye:

- Un diagnóstico de la producción de documentos electrónicos en la institución.
- Un análisis de los instrumentos archivísticos existentes.
- La capacitación del encargado del Archivo Central y personal de Tecnologías de Información para la administración de la PT y solución ADN.
- La capacitación a las personas usuarias de las unidades administrativas.
- La evaluación de los resultados del uso del servicio.

No obstante, esta fase también requiere de la aplicación de las siguientes acciones adicionales que deben ser cumplidas por los clientes que deseen adquirir el servicio, como lo son:

- La definición deun cronograma de implementación del servicio en las demás unidades administrativas.
- La obtención e instalación del sello electrónico (firma digital de persona jurídica).
- La interconexión de la institución con el servicio del ADN.

- La elaboración y/o actualización de normativa archivística institucional, en caso de ser necesario.

Mantenimiento y soporte: este servicio incluye la actualización continua de la solución informática, además de brindar soporte técnico tanto en materia archivística como tecnológica, todos los manuales y documentación necesaria para el uso y manipulación de la solución.

Herramienta de preservación digital: la licencia de uso de la solución tecnológica de preservación digital, denominada ARCA, pretendía ser comprada a la empresa Business IntegratorsSystems Limitada (BIS) con la finalidad de desarrollar el plan piloto en el Ministerio de Cultura y Juventud, como se logra constatar en el Sistema Integrado de Compras Públicas (N.º de solicitud de contratación 0062019000400044), no obstante, este plan piloto no se logró implementar por falta de presupuesto.

Al igual que otras soluciones, el funcionamiento de ARCA se basa en el modelo OAIS o su equivalente ISO 14721, por lo tanto, su operación se encuentra basado en la conservación de Paquete de Información (PI), en donde el contenido de la información y su descripción respectiva es protegido por medio del encapsulado en formato XML con Base64, dicha estructura se representa de mejor manera en la siguiente figura:

Figura 8. Composición del Paquete de Información en el ADN

Fuente: Congreso Archivístico (2019). Archivo Nacional.

Como se muestra, el PI presenta tres variantes, la primera, es el Paquete de Información de Transferencia (SIP), en esta fase el objeto de origen es transferido por el productor hacia el Archivo en las condiciones previamente acordadas, el segundo estado del contenido, se refiere al Paquete de Información Archivística (AIP) en donde el AIP se convierte en el contenido que será preservado por el Archivo para su preservación, por último, la información se puede convertir en un Paquete de Información de Consulta (DIP), y ser utilizado para brindarle acceso a los usuarios cuando estos así lo soliciten. De esta manera convergen bajo el modelo OAIS tres entidades funcionales, conformadas por el productor del contenido del documento, la dirección y los usuarios, las personas o sistemas que acceden a la información resguardada.

Complementariamente, se incorpora la descripción multinivel por medio de la Norma Nacional de Descripción Archivística y por consiguiente las respectivas aplicaciones de lenguaje marcado XML en el área de los archivos como Encoded Archival

Description (EAD), Encoded Archival Context (EAC) y Encoded Archival Guide (EAG). De igual forma, se instauraron las siguientes medidas:

- Utilización de esquemas y diccionarios de metadatos de preservación, como el esquema METS y el diccionario PREMIS.
- Bitácoras de trazabilidad y pistas de auditoría.
- Protección de los Paquetes de Información Archivística mediante cifrado.
- Foliación de expedientes por medio de la creación de índices electrónicos.
- Uso de certificados de sello electrónico institucional como un elemento de confianza para la validez de los documentos.
- Al igual que la información de los documentos, los metadatos que describen el contexto, la estructura y el contenido serán conservados por el tiempo que sea requerido.

Enlaces y continuidad del negocio: el servicio se compromete a brindar un plan de continuidad del negocio, entendiendo que la información es un activo que debe estar disponible las 24 horas del día, los siete días de la semana, por tal razón, se brinda redundancia en los enlaces de conectividad con enlaces de punto a punto, una plataforma con sistemas distribuidos que permiten la escalabilidad de la solución, además de un webservice, un TLL y manuales técnicos para la integración y conexión de los sistemas existentes en las instituciones con el repositorio y sistema de gestión del ADN.

Almacenamiento y seguridad: se abarca por medio de la redundancia en respaldos de información, la creación de planes de contingencia ante la interrupción del servicio, el cifrado de las bases de datos y la comunicación de las aplicaciones.

Otra característica importante de la solución se encuentra en el acompañamiento y orientación de los profesionales del Archivo Nacional a los encargados de los archivos centrales y al personal de Tecnologías de Información de las instituciones que opten por contraer el servicio, de esta manera, se afronta parte de la problemática que representa la continuidad digital, buscando controlar aspectos relevantes como la normalización del uso de formatos digitales y la identificación de infraestructura tecnológica destinada para el almacenamiento.

D. **Estado actual del proyecto**

En la actualidad, el proyecto se encuentra paralizado por la afectación que ha tenido la institución desde el punto de vista presupuestario por la pandemia, Covid-19, la cual alteró la metodología de trabajo establecida anteriormente, sin embargo, esto no impidió que el equipo de trabajo efectuará los diagnósticos y la revisión de las herramientas archivísticas.

Asimismo, se está trabajando en la creación de una Norma Técnica Nacional que vendría a reunir los requisitos mínimos necesarios que deben cumplir las instituciones para formar parte de la solución. También se están identificando los elementos que deben cumplir los repositorios digitales para el almacenamiento de documentos teniendo en cuenta la normativa nacional existente y las buenas prácticas internacionales. De momento, se hanidentificado los siguientes requisitos:

- Certificado de firma digital para los funcionarios encargados de producir y firmar documentos.
- Certificado institucional de sello electrónico.
- Instrumentos archivísticos actualizados, validados y normalizados a nivel institucional.
- Plantillas normalizadas, diseñadas por tipo documental para la normalización de producción de documentos.
- Mapeo de flujos de trabajo e identificación de los documentos que se producen.
- Mapeo de la normativa institucional existente relacionada con la gestión y preservación de documentos electrónicos.
- Identificación de infraestructura tecnológica para el almacenamiento de los documentos.
- Cultura y capacitación del personal de la institución.

Como se logró observar, el proyecto impulsado por Archivo Nacional, ADN, representaría un avance significativo en relación a la preservación digital en el sector público costarricense, pues de aplicarse se convertiría en una opción de bajo costo en relación con otras posibilidades en el mercado actual, además de tener acceso al

acompañamiento y asesoría del personal del Archivo Nacional destinado al proyecto, esto permitiría que aquellas instituciones adheridas al proyecto desarrollen los procesos de preservación digital de una forma estandarizada por medio de una herramienta que pretende brindar una solución en cumplimiento con normas internacionales de buenas prácticas y la normativa nacional.

3. Principales resultados de la encuesta aplicada al SNA

Para una mejor comprensión del estado actual de la preservación digital en Costa Rica, se desarrolló el presente análisis con base en los resultados obtenidos mediante la aplicación de una encuesta a los encargados de los archivos centrales de las instituciones pertenecientes al SNA, los mismos fueron elegidos de acuerdo a la información proporcionada en el Informe de Desarrollo Archivístico durante el período 2018-2019, y que según la Circular DSAE-02-2019, Índice de Desarrollo Archivístico, indicaron tener repositorios documentales para los documentos en soporte digital.

El cuestionario se orientó a una población de 91 archivos del Sistema Nacional de Archivos, de la cual se terminó por constituir una muestra representativa de 74 archivos que reflejaban la diversidad institucional existente en el Sector Público Costarricense, tales como: ministerios, instituciones adscritas, autónomas y gobiernos locales; sin embargo, pese a múltiples esfuerzos destinados para conseguir el total de las respuestas, solamente se recibieron 51 respuestas del total de la muestra. La encuesta abarcó los siguientes aspectos relacionados con la preservación digital y arrojó los siguientes resultados:

3.1 Gestión de documentos

La gestión de documentos es un área que cruza la organización de manera transversal, esta dispone de diversos objetivos, entre ellos, implantar normas y políticas en la materia, promulgar directrices y procedimientos, normalizar productos y servicios, diseñar, implantar y administrar sistemas de gestión de documentos y además, integrar la gestión de documentos al resto de los sistemas y procesos de la

organización, esto con la finalidad de controlar y gestionar los documentos de una manera eficaz y eficiente, tanto en su recepción como en su creación, mantenimiento, uso y disposición.

De acuerdo con Barnard, Delgado y Voutssas (2017), se puede establecer que las actividades que conforman el proceso de preservación digital comienzan con la sensibilización de lo que se requiere para elaborar o producir documentos de archivo fidedignos a través del tiempo (p. 23). Es por esta razón, que resulta de trascendental interés que las organizaciones establezcan de manera previa o paralela a la implementación del repositorio para preservación digital, las medidas que le permitan garantizar que la producción e ingreso de documentos al sistema de preservación digital corresponde a objetos digitales con todas las propiedades significativas que aseguren el valor probatorio de la información durante su gestión.

Al respecto, de acuerdo con los resultados arrojados a través de la aplicación del cuestionario, el 68,6% de las instituciones afirmaron poseer una política de gestión de documentos, es decir, la mayoría de las organizaciones han definido orientaciones, normas y directrices para promover una creación y gestión de documentos íntegros, auténticos, fiables y disponibles a lo largo del tiempo, independientemente de su forma o estructura y acorde con la normativa nacional que regula la materia.

Siguiendo esta premisa, es importante mencionar que el 100% de las instituciones encuestadas señalaron que en la actualidad producen y reciben documentos en soporte digital, como bien es sabido el país dispone de normativa que regula tanto el documento electrónico como la firma digital desde el año 2005, sin embargo, el uso y gestión de estos ha sido lento y con un alcance reducido. Según el Banco Central de Costa Rica a octubre de 2020 se ha emitido 461.004 certificados digitales, es decir, menos de un 10% de la población mayor de 18 años tiene firma digital certificada.

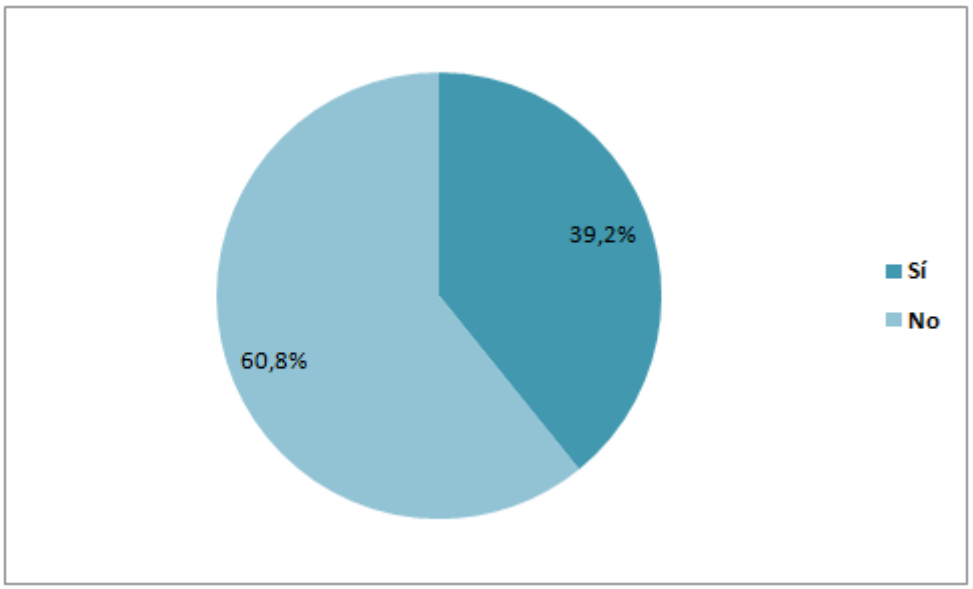
A pesar de lo anterior, la directriz 019-MP-MICITT (2018), ordena a los jerarcas de la Administración Central, y a los jerarcas de la Administración Descentralizada que “al menos un 75% de todos los documentos que se gestionan y conservan en la institución sean documentos electrónicos firmados digitalmente, antes del 1ero de

diciembre de 2020” (artículo 3), por lo que la producción y gestión de documentos digitales ha ido en aumento.

Además, la situación generada por la pandemia de Covid-19, disparó de manera exponencial el teletrabajo y por consiguiente los servicios electrónicos y el uso de firma digital, el 94,1% de las organizaciones señalan que los documentos que están produciendo cumplen con las especificaciones técnicas definidas en la Política de Formatos Oficiales de los Documentos Electrónicos Firmados Digitalmente.

En cuanto a la implementación de SGDE, solamente el 39.2% de las instituciones del SNA ha implementado uno, como se muestra en el siguiente gráfico:

Gráfico 1. Porcentaje de instituciones del SNA que tienen un Sistema de Gestión de Documentos Electrónicos, durante 2020



Fuente: elaboración propia a partir de los cuestionarios aplicados.

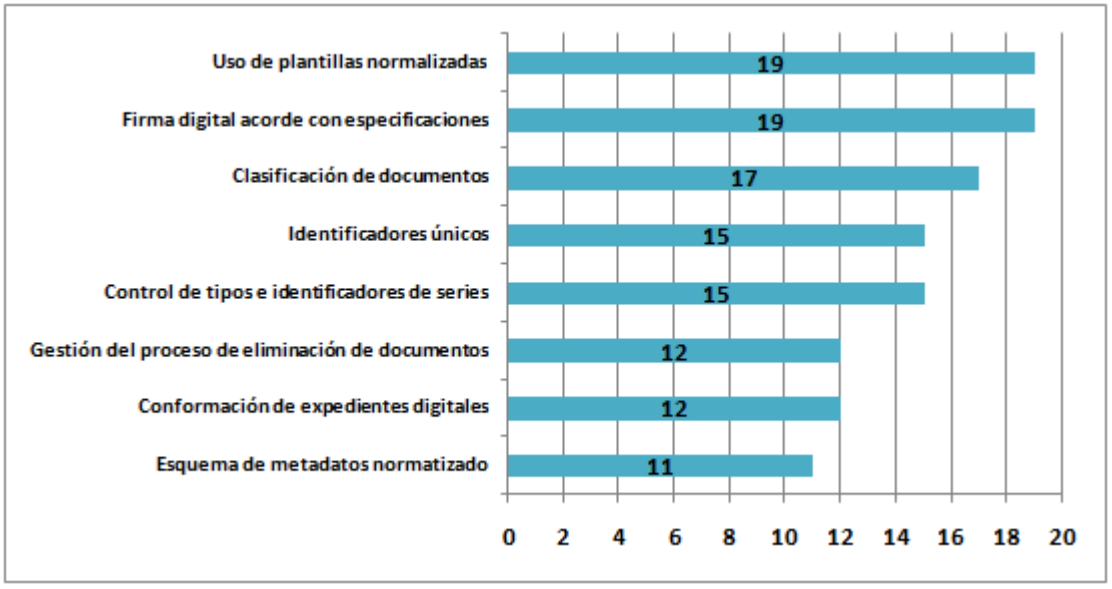
Al analizar las funcionalidades de dichos SGDE, se evidencia que, de las 20 instituciones que afirman disponer de un SGDE:

- Nueve de los SGDE no disponende esquemas de metadatos normalizados en cumplimiento con la Norma Nacional de Descripción.
- Ocho de los SGDE no gestionan la disposición final de los documentos, de acuerdo con tablas de plazos de conservación documental.

- Ocho de los SGDE no realizan la conformación de expedientes digitales de una manera normalizada, siguiendo la Norma Técnica Nacional de Expedientes Administrativos.
- Cinco de los SGDE no utilizan identificadores únicos en sus documentos electrónicos.
- Tres de los SGDE no han vinculado el cuadro de clasificación de documentos y por tanto no reflejan la identificación y estructuración sistemática de las actividades de su institución.
- Uno de los SGDE no utiliza plantillas normalizadas para la producción de documentos.

En el siguiente gráfico se muestra la implementación de las funcionalidades anteriormente descritas:

Gráfico 2. Cantidad de Archivos del SNA que implementan las funcionalidades requeridas en un SGDE, durante 2020



Fuente: elaboración propia a partir de los cuestionarios aplicados.

De lo anterior se determina que, los sistemas informáticos utilizados por las instituciones del SNA, no pueden considerarse como SGDE, por una parte, porque no están cumpliendo con los aspectos mínimos mencionados anteriormente; y por otra parte, porque la producción, captura y gestión de los procesos archivísticos de los

documentos debe ser sistemática, en concordancia con las políticas y procedimientos autorizados.

Además, el 47.8% de las organizaciones que dicen poseer “SGDE”, mencionan que los documentos que producen no incluyen información de autenticidad y descripción como parte de los datos estructurados (metadatos del fichero). Lo cual resulta preocupante por dos motivos, el primero porque los archivistas están confundiendo un sistema de producción documental con un SGDE; el segundo, porque se está perdiendo la información contextual, lo que provoca que los objetos digitales resulten incomprensibles y poco fiables, aunque sean accesibles.

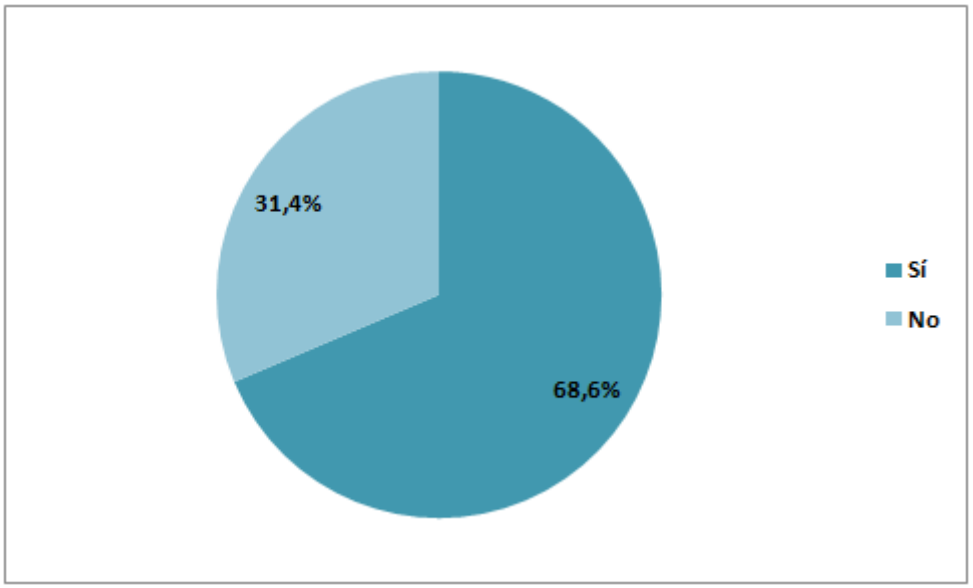
Aunque todas las instituciones encuestadas producen y reciben documentos en soporte digital, queda demostrado que, en la actualidad, en un contexto de gobierno electrónico, gestionar y almacenar documentos electrónicos de manera automatizada pero indiscriminada sigue siendo una práctica común y generalizada dentro del SNA, lo cual pone en riesgo la integridad, seguridad, trazabilidad y viabilidad de la preservación de la información contenida en los documentos electrónicos.

3.2 Almacenamiento

Gestionar el almacenamiento de documentos electrónicos es indispensable para garantizar las necesidades de seguridad y acceso a la información, así como la continuidad operacional de los servicios. Por tanto, disponer de repositorios digitales para la preservación, como archivos digitales centralizados, es una necesidad para asegurar la perdurabilidad de los documentos y sus metadatos, así como su recuperación a través del tiempo.

Como resultado de la encuesta se obtiene que un 68,6% de las instituciones del SNA, indicaron que poseen repositorios para el almacenamiento de los documentos electrónicos acorde con el CNTD, tal como se presenta en el siguiente gráfico:

Gráfico 3. Porcentaje de archivos del SNA que tienen repositorios para preservación digital, durante 2020



Fuente: elaboración propia a partir de los cuestionarios aplicados.

De lo anterior se desprende que:

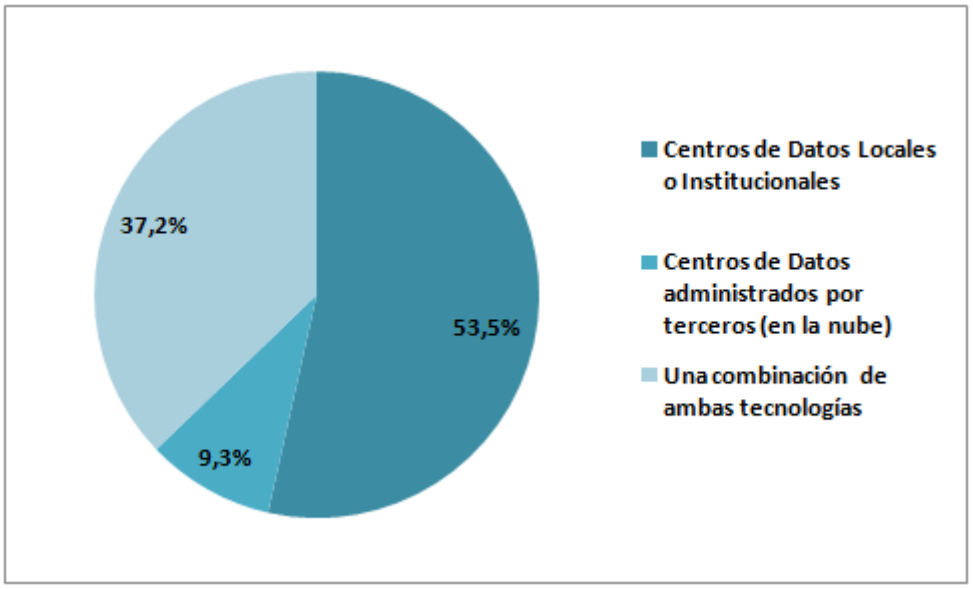
- Considerando que tan solo un 39,2% (Gráfico 1) de las instituciones afirman tener un SGDE, resulta imposible y contradictorio que un 68.6% (Gráfico 3) afirma tener con un repositorio digital para la preservación de documentos digitales acorde con el CNTD, debido a que el CNTD establece como necesario la integración funcional y lógica del SGDE con el repositorio digital por medio de la aplicación del Modelo OAIS.

- Se puede inferir que existe una confusión conceptual entre repositorio digital para preservación de documentos con soluciones de almacenamiento. El 68,6% de los encuestados consideran que cumplen con el CNTD debido a que almacenan sus documentos electrónicos. Sin embargo, el almacenamiento digital no considera los procedimientos para la preservación digital a largo plazo.

Las soluciones de almacenamiento, utilizadas por los archivos del SNA, para brindar persistencia a los activos de información se basan mayoritariamente (53.5%) en

centros de datos locales o institucionales, seguidos por soluciones que representan un híbrido entre infraestructura local y la tercerización de la misma en la nube (37.2%) y tan sólo un 9.3% han optado por el almacenamiento total en la nube, tal como se muestra a continuación:

Gráfico 4. Porcentaje de tipos de soluciones de almacenamientos utilizadas por los archivos del SNA, durante 2020



Fuente: elaboración propia a partir de los cuestionarios aplicados.

No obstante, al ser consultados sobre la aplicación de medidas de control de acceso, seguridad, interoperabilidad y conservación establecidas en CNTD, la mitad de las organizaciones aseguran que cumplen de manera satisfactoria con dichas medidas, sin embargo, se logra evidenciar que es un cumplimiento parcial ya que al consultar las medidas que aplican, los elementos que cuentan con un mayor nivel de cumplimiento son los siguientes:

- Asignación de roles y perfiles para el ingreso al sistema.
- Generación de copias de seguridad.
- Elaboración de directrices y lineamientos de seguridad de la información.
- Uso de estándares tecnológicos como ISO 27001 y 27002, COBIT e ITILL.
- Uso de certificados y firmas digitales vigentes.

- Protecciones contra software malicioso, protecciones de correo electrónico y navegadores web.
- Registro de eventos, respuesta y gestión de incidentes.

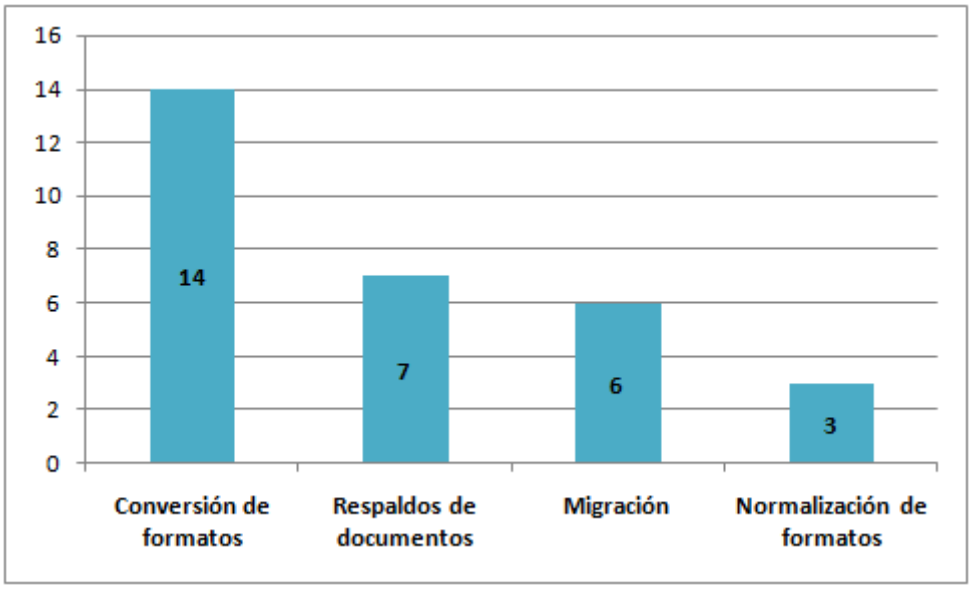
Es decir, que la otra mitad de las instituciones que señalan no aplicar las medidas expuestas en el CNTD tienen una mayor exposición a ataques, amenazas, abusos, sustracciones y accesos no autorizados a la información almacenada, evidenciando de esta manera que no existe una identificación y una administración coherente entre los riesgos a los que se expone la información y el acceso a la información almacenada, poniendo en peligro la confidencialidad, autenticidad, integridad, disponibilidad y seguridad de la información, evidenciado además que los servicios de almacenamiento que están utilizandolas instituciones encuestadas posiblemente no sean inclusivos, integrados ni seguros, ya que no cumplen con las medidas mínimos de interoperabilidad, seguridad y control de acceso.

3.3 Preservación digital

Partiendo de la premisa establecida por Barnard, A; Delgado, A y Voutssás, J (2014) en donde señalan que los encargados de preservar documentos tienen la responsabilidad de establecer sistemas de preservación de documentos de archivo al momento de adoptar una estrategia de preservación, este sistema debe recoger un conjunto de principios, políticas, reglas y estrategias, así como las herramientas y mecanismos destinadas para ser implementados en una institución u organización para tratar de garantizar la preservación de la información a largo plazo (p. 204).

Al analizar el funcionamiento de las instituciones encuestadas en este aspecto se encontró, en primera instancia, que un 35,3% señalaron tener una estrategia de preservación digital; al consultar sobre las estrategias implementadas se obtuvieron diversas respuestas, sin embargo, se logró determinar que la más utilizada es la conversión de formatos, acompañadas por otras como la generación de respaldos, la migración y normalización de formatos, lo anterior se detalla en el siguiente gráfico:

Gráfico 5. Aplicación de estrategias de preservación en las instituciones del SNA, durante 2020



Fuente: elaboración propia a partir de los cuestionarios aplicados.

La estandarización en el uso de formatos digitales es una estrategia válida que incrementa la estabilidad de los documentos que se pretenden preservar a largo plazo, no obstante, dicho proceso se debe hacer con base en estándares ampliamente aceptados y soportados, para ello TheNational Archives del Reino Unido dispuso el proyecto PRONOM, con el cual se brinda información imparcial respecto a los formatos de archivo y productos de software con el fin de asegurar la preservación a largo plazo (PRONOM, 2020).

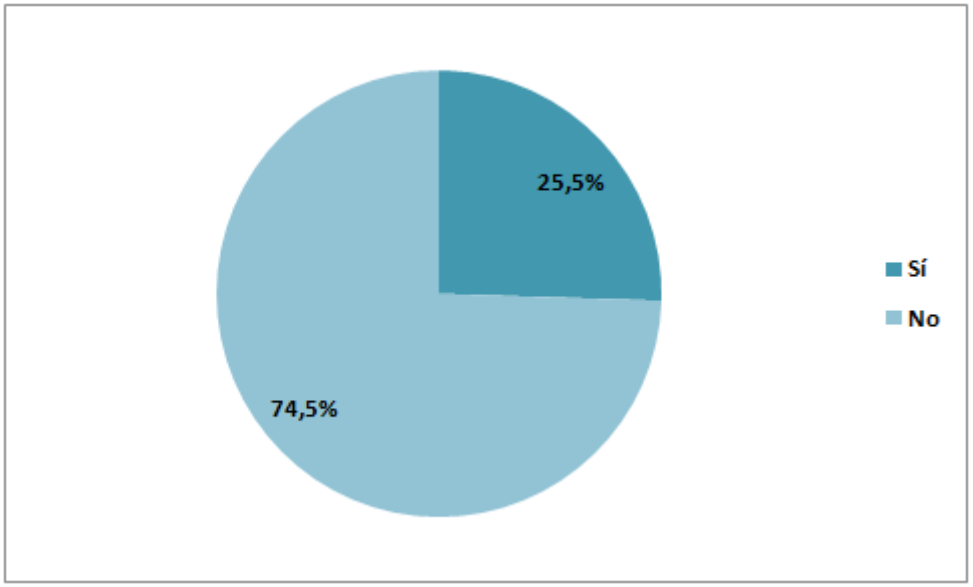
Al respecto, solamente una de las instituciones encuestadas informó utilizar PRONOM como herramienta para limitar los formatos digitales permitidos. El resto de las instituciones mencionaron que no se basan en ninguna herramienta o norma interna para la normalización de los formatos digitales permitidos. Por lo tanto, los archivos están realizando conversión de formatos, sin antes reconocerlos e identificarlos, y generalmente, los formatos utilizados para almacenar la informacióndigital son inestables y se deterioran al cabo de pocos años.

De igual forma, resulta importante aclarar que la realización de migraciones y respaldos de documentos por sí solas no constituyen estrategias viables a largo plazo

para garantizar la preservación de los documentos digitales, en el caso de la migración se debe aplicar en casos específicos en donde el software o el hardware se vuelvan obsoletos o por una cuestión de conveniencia organizacional, en tanto con la generación de respaldos de documentos, si bien constituye una buena práctica, resulta inviable pretender asegurar la preservación aplicando exclusivamente este procedimiento, puesto que no cubre aspectos relevantes como la obsolescencia de formatos de fichero.

Las circunstancias mencionadas anteriormente en cuanto a la confusión de los formatos de fichero se pueden deber a la nula preparación institucional para la preservación digital, tal como se evidencia en el siguiente gráfico, el 74,5% de las instituciones del SNA no tienen una política institucional para la preservación digital:

Gráfico 6. Porcentaje de instituciones del SNA que han implementado una política institucional de preservación digital, durante 2020



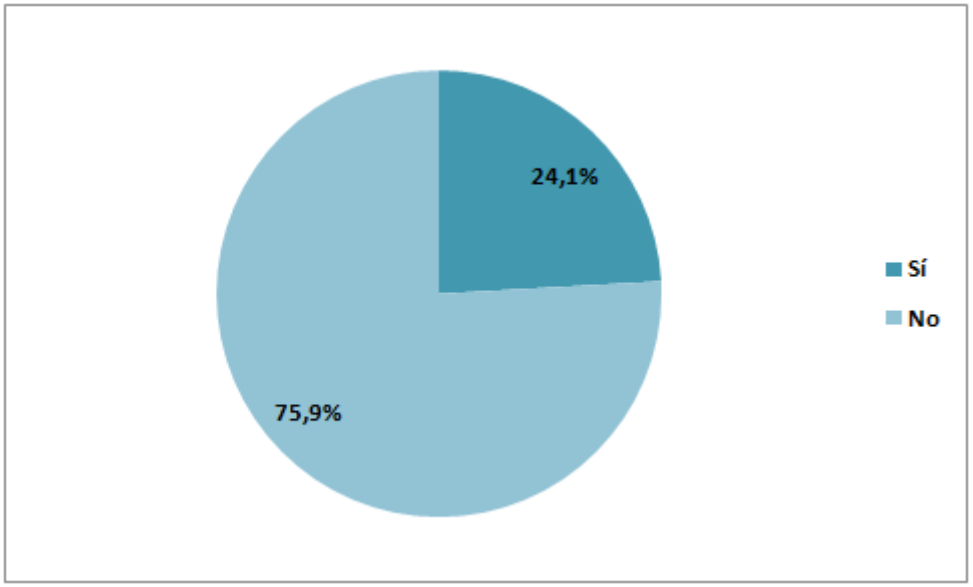
Fuente: elaboración propia a partir de los cuestionarios aplicados.

Se evidencia que la mayoría de instituciones del SNA han constituido sus "repositorios digitales" al margen de un proceso planificado y en ausencia del apoyo de las autoridades institucionales, lo cual perjudica inevitablemente la sostenibilidad y la continuidad del proyecto, pues los recursos necesarios para su funcionamiento no pueden ser garantizados a lo largo del tiempo, además, carecen de la definición de

medidas que posibiliten brindar un seguimiento oportuno al cumplimiento de objetivos y metas que se pretenden alcanzar con el proceso de preservación.

Asimismo, cuando se les consultó sobre el uso del modelo OAIS, se reflejaron resultados similares, ya que el 75,9% de las instituciones que aseguraron tener un repositorio para preservación digital mencionaron no haberlo tomado en consideración para la adquisición o diseño de sus repositorios digitales, como se muestra en el gráfico 7, lo anterior aleja aún más a las instituciones del SNA de incorporar una visión de preservación digital que sea sistémica, en donde se ofrezca una custodia ininterrumpida del documento en sistemas que cumplan con los requisitos funcionales para garantizar que sean fidedignos a largo plazo.

Gráfico 7. Porcentaje de archivos del SNA que han aplicado el modelo OAIS en sus repositorios digitales de preservación, durante 2020



Fuente: elaboración propia a partir de los cuestionarios aplicados.

Además, el gráfico anterior y el gráfico 3, muestran una clara contradicción entre los archivistas, puesto que cuando se les cuestionó si sus repositorios para preservación digital cumplían con el CNTD, el 68,6% (gráfico 3) respondió afirmativamente; sin embargo, cuando se les cuestionó sobre la aplicación del Modelo OAIS en sus repositorios digitales solo un 24,1% (gráfico 7) dijo cumplirlo. Entonces, es evidente que en la mayoría de los archivos:

- No se conoce el contenido ni alcance del Código Nacional de Tecnologías Digitales.
- No se está tomando en consideración el Código Nacional para la adquisición de sistemas de preservación digital.
- No se está aplicando el Modelo OAIS.

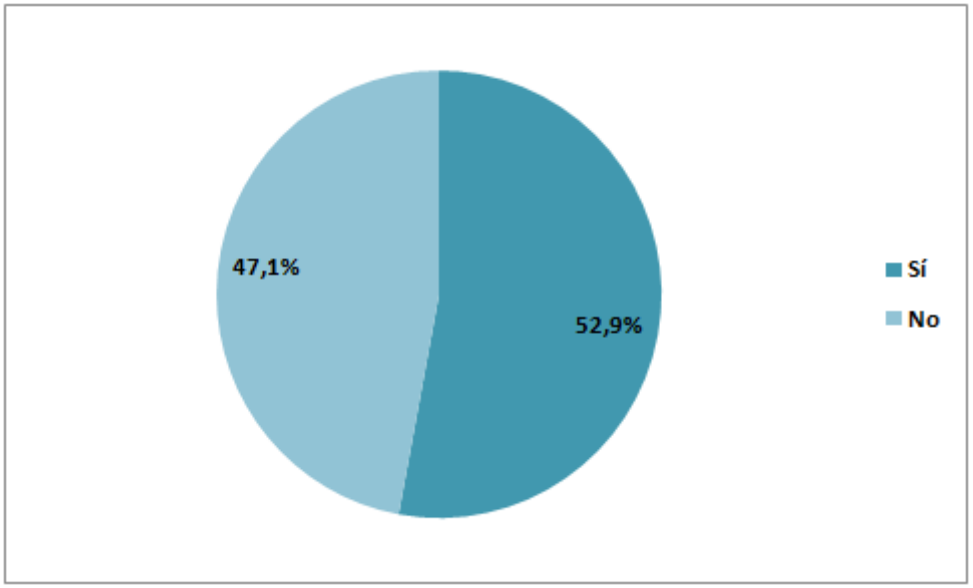
A pesar de los datos anteriores, el 71,4 % de los encuestados consideran que sus repositorios institucionales se encuentran preparados para la preservación de documentos digitales, esto evidencia una de las causas del problema, puesto que muestra la falta de concientización y sensibilización de los responsables al momento de afrontar la problemática, además, prueba que no se dispone de los conocimientos necesarios para mitigar los riesgos asociados a la inexistencia de políticas, estrategias y procesos destinados a la preservación digital en sus instituciones.

Por último, como reflejo de la indolencia mostrada por las instituciones en la aplicación de procedimientos de preservación digital, se encuentran las respuestas proporcionadas en relación a la aplicación de buenas prácticas archivísticas para la preservación de documentos digitales, pues se han limitado, en su mayoría, a la aplicación de algunas de normas técnicas emitidas por el Archivo Nacional, lo cual resulta insuficiente para asegurar una adecuada administración de los repositorios digitales.

3.4 Seguridad de la información

La seguridad de la información conlleva la preservación de la autenticidad, la confidencialidad, la integridad, el acceso, la disponibilidad de la información y la continuidad del servicio. Con el fin de corroborar si los archivos del SNA, mantienen segura su información, se les consultó, acerca de la protección de sus datos.

Gráfico 8. Porcentaje de instituciones del SNA que tienen un plan de protección de datos acorde con el Código Nacional de Tecnologías Digitales, durante 2020



Fuente: elaboración propia a partir de los cuestionarios aplicados.

El 52.9% de los encuestados aseguraron tener un plan de protección de datos acorde con lo estipulado en el Código Nacional de Tecnologías Digitales, por lo cual contemplan el respaldo operativo de datos, la recuperación ante desastres para la continuidad del negocio, la protección de los activos de información ante errores de aplicación, errores de usuario y ataques de un programa malicioso o código maligno (malware), así como fallos de la máquina o cortes de energía en las instalaciones.

La protección de datos es el proceso de resguardar la información de la corrupción y pérdida, y de acuerdo con el CNTD, para ello se debe cumplir con tres principios básicos:

- La integridad de los datos: la modificación de cualquier tipo de información debe ser conocida y autorizada por el autor o entidad.

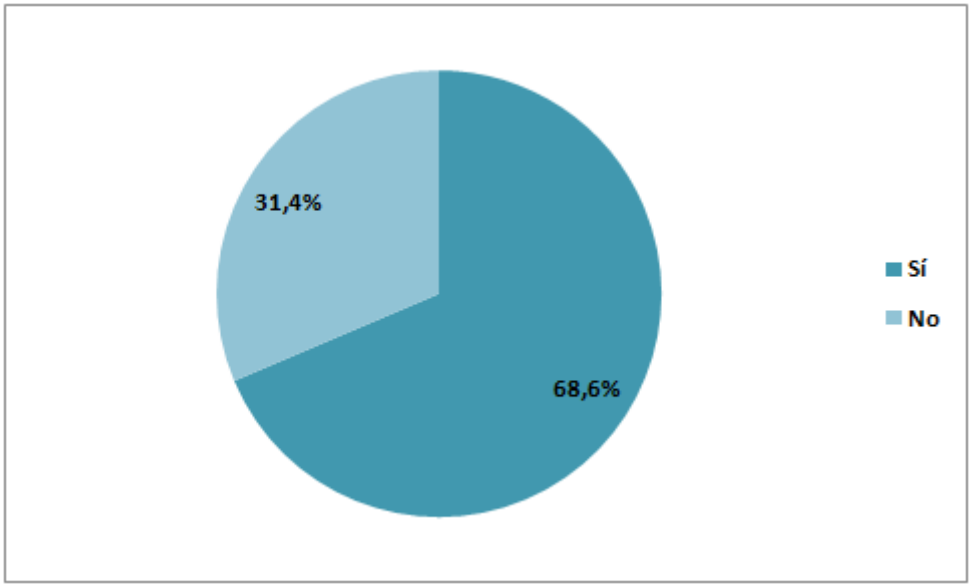
- La disponibilidad del sistema: la operación continúa para mantener la productividad y la credibilidad de la empresa.
- La confidencialidad: la divulgación de datos debe ser autorizada y protegida contra ataques que violen este principio.

Sin embargo, de acuerdo con el análisis realizado anteriormente, es imposible asegurar que el 52,9% de las instituciones está incumpliendo con el plan de protección de datos, debido a que no tienen los sistemas de preservación necesarios para asegurar la integridad, disponibilidad y confidencialidad de la información que están custodiando.

La ausencia de un plan de protección de datos permite que las amenazas a la seguridad de la información incrementen, por lo tanto, garantizar la protección total de los documentos electrónicos es imposible. El propósito del plan de protección de datos y un sistema de seguridad de la información consiste en que los riesgos a la seguridad de la información sean reconocidos y, puedan ser gestionados y minimizados.

Disponer de una copia de los activos de información en una localización geográfica alterna a la institución puede contribuir a la seguridad de la información, en caso de amenazas o desastres naturales, y consecuentemente la continuidad de los servicios.

Gráfico 9. Porcentaje de instituciones del SNA que tienen una copia de los activos de información en una localización geográfica alterna a la institución, durante 2020



Fuente: elaboración propia a partir de los cuestionarios aplicados.

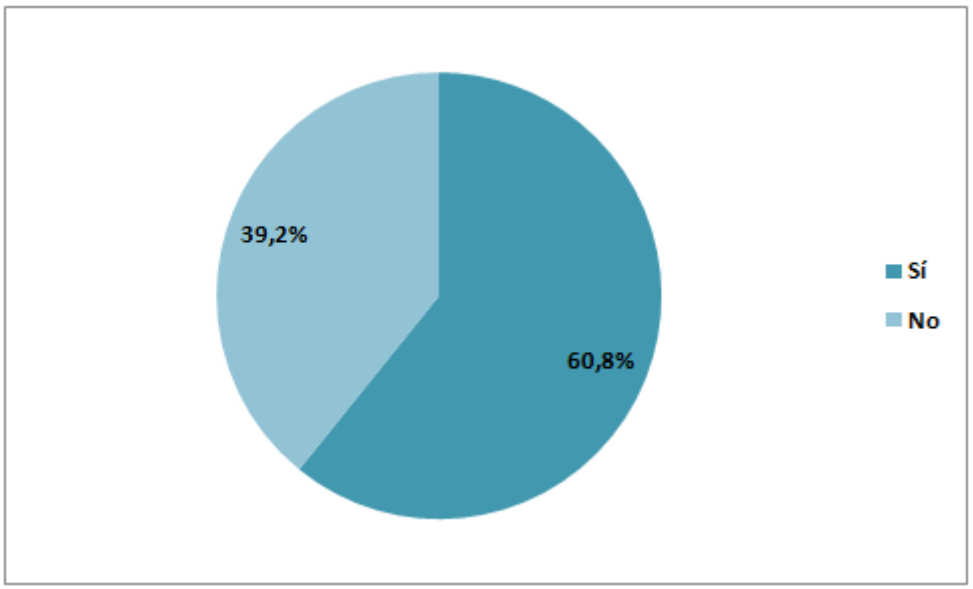
El 68.6% de los archivos del SNA, respondió que tienen una copia de los activos de información en una localización geográfica alterna, con el fin de recuperar la información por cualquier amenaza o accidente ocurrido en la localización principal donde se encuentra la información. Mientras que el 31,4%, no está adoptando los controles mínimos de seguridad para proteger sus activos de información, por lo tanto, un porcentaje considerable de instituciones se encuentran en posición de desventaja y vulnerabilidad para soportar los riesgos en caso de amenazas, desastres o accidentes.

No obstante, a pesar de que las copias de seguridad traen consigo una serie de beneficios para la organización estas son únicamente uno de los distintos medios de seguridad que pueden o deben implementarse, ya que la seguridad toma en cuenta también aspectos como la identificación y recuperación de información esencial en tiempos oportunos, los niveles de seguridad, registros de trazabilidad y las pistas de auditoría.

Como se mencionó anteriormente, son diversos los mecanismos que participan en la seguridad de la información, entre ellos los registros de la trazabilidad y las auditorías. El 60.8% de las organizaciones mencionan que mantienen los registros de

la trazabilidad de todas las acciones realizadas sobre los ficheros, lo que a su vez garantiza que dichos registros o bitácoras están disponibles para futuras inspecciones con el fin de evidenciar cualquier tipo de evento o irregularidad, en cuanto a integridad y autenticidad de la información, lo anterior se evidencia en el siguiente gráfico:

Gráfico 10. Porcentaje de instituciones del SNA que tienen registros de trazabilidad en su repositorio digital, durante 2020



Fuente: elaboración propia a partir de los cuestionarios aplicados.

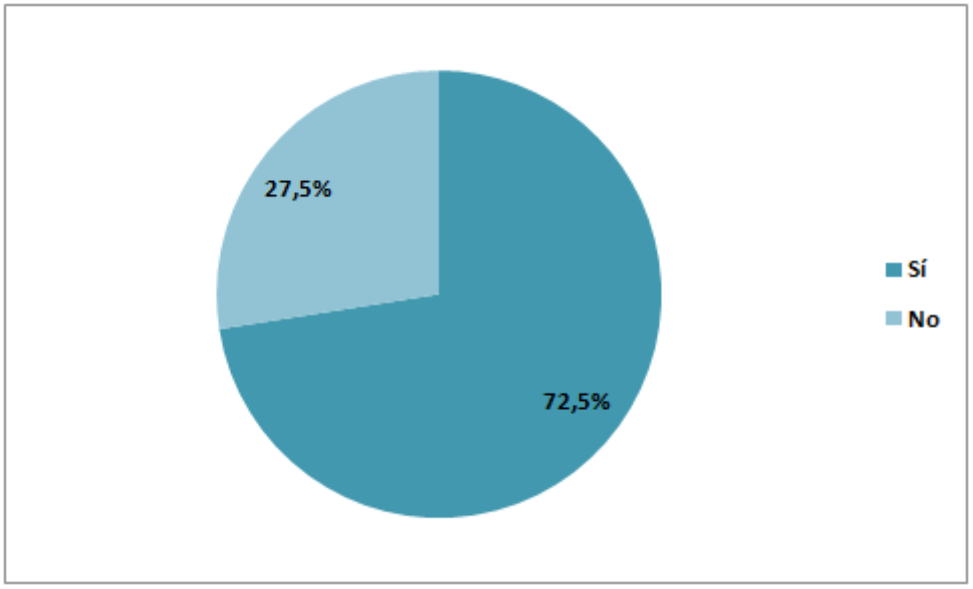
A pesar de que la mayoría de las instituciones tienen registros de trazabilidad, únicamente el 51% audita dichos registros, es decir, un 49% desconoce los eventos relevantes ocurridos en el sistema y por consiguiente invisibiliza de cierta manera las posibilidades de mejora o minimización de riesgos a los que se encuentra expuesta la información custodiada.

3.5 Acceso

Si bien es cierto, la perspectiva de archivo digital abierto persigue el acceso libre y sin obstáculos a la información digital, es importante que exista la verificación de los derechos o permisos necesarios para poder acceder a los documentos digitales, según la tabla de control de acceso.

La mayoría de las organizaciones encuestadas, 72,5%, señalan que sus repositorios digitales disponen de permisos y roles específicos de acceso, lo que garantiza que la información custodiada es accedida únicamente por los usuarios autorizados.

Gráfico 11. Porcentaje de instituciones del SNA que tienen permisos y roles específicos en su repositorio digital, durante 2020



Fuente: elaboración propia a partir de los cuestionarios aplicados.

Sin embargo, para el 27,5% de organizaciones restantes, existe el riesgo constante de comprometer información confidencial, como datos personales, sensibles o información restringida que no puede divulgarse sin el consentimiento expreso, y que resguardan el derecho fundamental a la intimidad de los ciudadanos, tal como se indica en la Ley 8968 de Protección de la Persona frente al tratamiento de sus datos personales vigente desde el año 2011.

3.6 Continuidad digital

La continuidad digital, ofrece la posibilidad de que la información de una institución permanezca consultable e interpretable, en cualquier momento, independientemente del momento en el que fue producida originalmente, manteniendo sus propiedades de autenticidad, integridad, fiabilidad y accesibilidad.

Respecto a continuidad digital, aproximadamente el 70% de los encuestados, aseguran que en su institución:

- No tienen un Plan de Acción de Continuidad Digital.
- No han identificado dónde están los riesgos en su información y, por lo tanto, no han tomado las medidas activas para administrar esos riesgos.
- No se incorpora la continuidad digital en los procesos y estrategias de la organización, de manera que, no es posible asegurar el acceso a la información a través del tiempo.
- No disponen de un protocolo para el ingreso o transferencia de objetos digitales, que permita garantizar que la información recibida o transferida pueda ser utilizada a través del tiempo.

Con base en la información anterior, se deduce que la mayoría de las instituciones encuestadas, no gestionan la continuidad digital, debido a que no comprenden el valor de la información que administran. Por tanto, su tecnología y los procesos que gestionan su información, no resguardan sus activos de información y corren el riesgo de perder su capacidad para encontrar, abrir, comprender, confiar y trabajar con su información; lo que podría tener un impacto considerable en la continuidad de su negocio.

3.7 Gestión del riesgo

Identificar los riesgos, permite dar respuesta a la incertidumbre y a los factores de cambio del futuro, por lo que anticiparse a ello, permite diseñar estrategias para la gestión exitosa de la información a lo largo del tiempo. Por tanto, el análisis del riesgo respecto a la obsolescencia tecnológica y la preservación de la información digital es indispensable para la identificación de amenazas y peligros respecto a la seguridad de la información.

Respecto a gestión de riesgo, aproximadamente el 70% de los encuestados, aseguran que en su institución:

- No se ha establecido un marco de referencia para gestionar los riesgos producidos por la continuidad digital.
- No se han realizado informes de evaluación de riesgos de continuidad digital para la toma de decisiones dentro de la organización.
- No se han establecido los roles y responsabilidades para gestionar los riesgos para la continuidad digital.
- Tampoco se han definido los objetivos y criterios de éxito para la evaluación del riesgo en la continuidad digital.
- No se ha establecido un proceso para identificar, analizar, controlar, registrar, monitorear y revisar los riesgos.

Lo anterior, refleja que las instituciones costarricenses, no están resolviendo sus necesidades inmediatas de riesgo, ni tampoco están diseñando estrategias a largo plazo para la gestión de sus activos de información. Sin lugar a duda, no se han cuestionado que los sistemas en los que se mantiene la información no suelen ser adecuados para la gestión a largo plazo, debido a que la necesidad de la información perdurará más que la vida útil de sus sistemas de información.

4. Soluciones para la preservación digital

Existen diversas soluciones para la preservación digital de documentos, algunas de ellas se han ido gestando gracias a la función investigativa de distintas universidades, que han visualizado la necesidad de conservar el acervo documental en soportes digitales, principalmente, para fines culturales, históricos o investigativos, mientras que otras organizaciones privadas y públicas también han creado soluciones para subsanar una necesidad que se acerca más a un contexto administrativo y jurídico, no obstante, ambas propuestas han ido evolucionando con el tiempo y adaptándose a las necesidades de los usuarios, gracias en parte a que muchas de ellas fueron constituidas como código abierto.

En este orden de ideas, se debe contemplar que existen diversas adaptaciones del Modelo de Referencia OAIS para constituir modelos de trabajo más específicos y que

respondan a necesidades organizacionales, por lo que aún no existen modelos exitosos que sustituyan al modelo OAIS con una propuesta que sirva como punto de referencia a nivel conceptual. Por lo tanto, para el análisis de los repositorios de preservación digital se toma en consideración, como indicadores generales, las entidades del modelo funcional OAIS: la ingesta, el almacenamiento, la gestión de datos, el mantenimiento o preservación y el acceso.

Las soluciones a analizar y posterior comparación son: FEDORA, ERA, Archivematica, RODA y ARCA, al respecto se procedió a consultar los sitios web oficiales de las soluciones que disponen de uno, así como la documentación técnica disponible y material orientativo tales como manuales de uso generados por los proyectos y recursos audiovisuales desarrollados por la comunidad de usuarios, de igual manera, se probaron las demostraciones de producto de aquellas herramientas que disponían de una, como fue el caso de RODA y Archivematica.

Lo anterior permitió identificar de qué manera surgió el proyecto, quiénes son sus propietarios, qué entidades funcionales del modelo OAIS aplican, qué metadatos utilizan, qué estrategias de preservación emplean y qué estándares o normas de descripción archivística fueron adoptados.

4.1 Flexible and Extensible Digital Object and Repository Architecture (FEDORA)

Desde 1997 se ha llevado a cabo un proyecto de investigación en la Universidad de Cornell que se denominó Arquitectura de Repositorio de Objetos Digitales Extensible Flexible (FEDORA). FEDORA es un sistema de repositorio de código abierto, robusto y modular para la gestión y difusión de contenido digital, así como para la preservación de dichos objetos digitales.

Utiliza el método personalizado Fedora Object XML (FOXML) para empaquetar contenido, aunque puede ingerir y difundir paquetes en formatos METS y MPEG-21 DIDL. Sin embargo, la implementación de OAIS en esta herramienta se centra en sus funciones de ingesta y difusión.

El proyecto FEDORA está dirigido por *FedoraLeadershipGroup* y está bajo la dirección de la División de Programas Apoyados por la Comunidad DuraSpace de LYRASIS.

4.2 Electronic Records Archives (ERA)

La primera etapa del programa comenzó en 1998 y se ha convertido en un sistema de administración de información que proporciona capacidades para la transferencia, ingesta, almacenamiento y conservación de registros electrónicos, así como funcionalidad de flujo de trabajo para respaldar las transacciones entre los Archivos Nacionales y las Agencias Federales de los Estados Unidos relacionadas con la programación de registros y la transferencia de custodia física y legal de los documentos.

Archivos de Registros Electrónicos (ERA) ha adoptado el diseño modular en general de OAIS, las principales funcionalidades del sistema ERA son *Submission*, que permite la transferencia e ingesta de la información con sus metadatos. Permite la conservación y el almacenamiento de los paquetes de información en el Repositorio (*Repository*), permite la inclusión de Metadatos (*Metadata*) y, por último, permite el Acceso (*Access*) a los documentos.

ERA incorpora un catálogo de metadatos XML basado en estándares con elementos PREMIS para la conservación de metadatos. La política actual de ERA es mantener los registros en el formato en el que fueron transferidos, además de las nuevas versiones creadas a partir de acciones de transformación de formato.

4.3 Repository of Authentic Digital Objects (RODA)

Consiste en una iniciativa desarrollada por los Archivos Nacionales de Portugal en alianza con la Universidad de Minho, que surgió con el objetivo de garantizar el almacenamiento y preservación de los documentos electrónicos gestionados por el gobierno portugués.

En cuanto a su funcionamiento, el sistema RODA busca implementar las entidades funcionales establecidas dentro del modelo OAIS, de tal manera que cumple con:

1. Ingesta: los SIP pueden ser entregados por medio de transferencia electrónica o cargas en bloque, por ejemplo, utilizando el protocolo de transferencia FTP, de igual manera, pueden cargarse desde medios adjuntos al sistema.
2. Almacenamiento: por medio del módulo de ejecución de trabajo le permite al administrador del repositorio la conversión de formatos, la verificación de suma de comprobación, la generación de informes respecto al estado de los SIP recibidos y el control de virus, igualmente, permite la evaluación de los objetos digitales almacenados o proyectados a ser transferidos.
3. Gestión de datos: el sistema registra y administra cada uno de los datos generados como parte de la gestión de los objetos digitales custodiados, mediante lafecha, componente involucrado, método o función del sistema, objetos de destino, usuario que ejecutó la acción, la duración de la acción y la dirección IP del usuario que ejecutó la acción.
4. Mantenimiento: permite el registro de formatos, además de tener un sistema de notificaciones que permite notificar a los usuarios sobre eventos específicos en el sistema, permitiendo el monitoreo constante sobre el mismo.
5. Acceso: cuenta con servicios y funciones de apoyo a los usuarios para la búsqueda y localización de los objetos digitales, para ello incorpora herramientas como el inventario, buscadores avanzados y una red representación que presenta de la información de manera estructurada y ordenada de manera semántica (RODA, 2018).

RODA también incluye diversos estándares que complementan su operación, principalmente en relación con la descripción y la gestión de metadatos en general dentro del sistema. De esta manera, incorpora el uso del diccionario de datos PREMIS para los metadatos de preservación, la codificación de los objetos digitales se realiza con base en la estructura propuesta por el estándar METS, además, del uso de Dublin Core yEncodedArchivalDescription (EAD) para los metadatos descriptivos, partiendo de la norma ISAD-G (RODA, 2018).

Finalmente, en cuanto a la seguridad y confiabilidad de los objetos digitales, el sistema procura cumplir con las métricas y requisitos propuestos en las herramientas de evaluación TRAC (TrustworthyRepositories Audit &Certification) e ISO 16363.

4.4 Archivematica

Archivematica es un sistema de preservación digital gratuito y de código abierto que inició en el 2009 y está diseñado para mantener el acceso a largo plazo a la memoria digital. El sistema ejecuta diversos procedimientos que permiten a los usuarios procesar objetos digitales desde la ingesta hasta el acceso de dichos objetos. La metodología del sistema está centrada en ciclos de lanzamiento rápidos e iterativos, cada uno de los cuales mejora la arquitectura, los requisitos, las herramientas, la documentación y los recursos de desarrollo del sistema.

Las funcionalidades del sistema están basadas de acuerdo con el modelo funcional establecido en el modelo OAIS para proporcionar Paquetes de Información de Archivo (AIP) confiables, auténticos, e interoperables para el almacenamiento en el repositorio. Los usuarios monitorean y controlan los microservicios a través de un panel de control basado en la web.

Archivematica utiliza, en materia de metadatos, PREMIS (eventos, agentes, derechos y restricciones), METS para codificación, Dublin Core, la especificación BagIt de la Biblioteca del Congreso y otros estándares y prácticas. Además, contiene un Registro de Políticas de Formato (FPR) basadas en un análisis de las características significativas de los formatos de archivo, en el cual también se puede agregar políticas locales.

Este proyecto está gestionado por Artefactual Systems y con financiación de la UNESCO Memoria del Mundo, Subcomité de Tecnología, la ciudad de Vancouver Archives, Harvard Business School Baker Library, el Museo de Arte Moderno (MOMA), la Universidad de Alberta Bibliotecas, la Biblioteca de la Universidad de Columbia Británica, el Rockefeller Archive Centre, Simon Fraser University Archives and Records Management, Yale University Library, Zuse-InstituteBerlin, Council of Prairie and PacificUniversityLibraries (COPPUL), Biblioteca Histórica de Bentley, Universidad de Michigan, Duraspace, Bibliotecas del MIT, Consejo de Bibliotecas Universitarias de Ontario, Biblioteca Nacional de Gales y el Consejo Canadiense de Archivos.

4.5 ARCA

ARCA es una solución de repositorio digital basada en el funcionamiento del modelo OAIS, su objetivo principal es asegurar la custodia, acceso, difusión, interoperabilidad y preservación de información y objetos digitales en un entorno seguro.

Este sistema pertenece a la empresa Business IntegratorsSystems (BIS), quienes iniciaron con su desarrollo desde el año 2011. En el año 2017, fue implementado por el Archivo Central del Teatro Nacional de Costa Rica, de igual manera, ha sido utilizado por el Archivo Central del Archivo Nacional, gracias a la donación de una licencia de uso y posteriormente, se pretendió su adquisición de manera comercial con miras a ser implementado en el ADN, en el año 2019, sin embargo, como se mencionó anteriormente el proyecto se encuentra detenido.

En relación con su funcionamiento, el sistema lleva a cabo la ingesta por medio de la aplicación de diversos procesos como descripciones obligatorias, administración de formatos, revisiones antivirus y de firmas digitales, además, de la comprobación y autenticación de las propiedades significativas de los objetos digitales que se pretenden ingresar.

La descripción de la información contenida en los Paquetes de Información Archivística (AIP) se realiza de acuerdo con lo establecido en cuatro normas de descripción, como lo son: la ISAD-G, la ISAAR (CPF), la ISDF y la ISDIAH. De igual forma, cada documento está registrado como un nodo de tipo <fContent>, ubicado en la estructura METS, el cual a su vez se encuentra protegido por un contenedor XML, asegurado por medio de una firma digital de tipo XAdESA.

Como estrategia de preservación, además de cumplir con las entidades funcionales establecidas por el modelo OAIS, también incorpora el reconocimiento y registro de formatos basados en la iniciativa PRONOM, la extracción y colección automática de propiedades significativas, así como los mecanismos de autenticidad e integridad dentro de la cadena de custodia, junto con la conversión de formatos de ficheros, lo

anterior, se realiza por medio de la aplicación de diversos estándares como METS, PREMIS, EAD, EAC-CPF, EAG y MIX, en el caso de imágenes.

Por último, la seguridad de los activos de información se realiza por medio de tres ejes:

1. Aseguramiento de autenticidad: se realiza a través de la extracción automática de las propiedades significativas de autenticidad del documento electrónico y su custodia en el valor PREMIS correspondiente, además, los AIP son asegurados por medio de una firma digital de alta longevidad.
2. Control de integridad: en este eje se implementa nuevamente la firma digital de los AIP, con el fin de identificar cualquier variación o alteración en el mismo, además, se incorporan índices electrónicos con firma digital avanzada para el resguardo de los expedientes digitales.
3. Control de acceso: la verificación de credenciales de los usuarios para acceder a los documentos es contrastada con las condiciones de acceso asignados a cada documento, esto por medio de su motor de seguridad.

4.6 Comparativa entre soluciones para la preservación digital

De acuerdo con la información recopilada de las cinco soluciones, en el siguiente cuadro se comparan y se analizan si las soluciones desarrolladas anteriormente, cumplen con las entidades funcionales establecidas en la norma OAIS.

Cuadro 4. Cuadro comparativo de soluciones de preservación digital

Herramientas / Funcionalidades y características	archivematica	ERA	Fedora	RODA	Arca
INGESTA	☑	☑	☑	☑	☑
ALMACENAMIENTO	☑	☑	☒	☑	☑
GESTIÓN DE DATOS	☑	☑	☒	☑	☑
MANTENIMIENTO	☑	☑	☒	☑	☑
ACCESO	☑	☑	☑	☑	☑
ESTRUCTURA DE CODIFICACIÓN	METS	METS	METS	METS	METS
DESCRIPCIÓN NORMALIZADA	PREMIS Dublin Core	PREMIS	PREMIS	PREMIS MIX EAD EAC	PREMIS MIX EAD EAC EAG
CONVERSIÓN DE FORMATOS	☑	☒	☒	☑	☑
LICENCIAMIENTO	código abierto	exclusivo para NARA	código abierto	código abierto	PROPIETARIO

Fuente: elaboración propia.

Una vez analizadas las diferentes iniciativas de soluciones de preservación digital y su comparación, se desprende que los diferentes proyectos de preservación digital han adoptado el modelo de referencia OAIS como punto de partida para el desarrollo metodológico y funcional de la solución.

Lo anterior no significa que todas las herramientas trabajan y responden a las necesidades de preservación de la misma forma, precisamente, en la descripción normalizada de los Paquetes de Información, se refleja parte de la desavenencia existente entre los sistemas analizados, pues tanto ERA como FEDORA se limitan a incorporar los metadatos PREMIS, mientras que RODA y ARCA incluyen metadatos administrativos y descriptivos como los EAD y los EAC, en el caso de Archivematica hacen uso del estándar Dublin Core para la descripción de los objetos digitales.

Otra diferencia funcional se refleja en la capacidad de aplicar conversiones de formatos en los paquetes AIP, tanto la ERA como FEDORA no realizan esta función, mientras que soluciones como Archivematica, RODA y ARCA brindan a sus

usuarios mayor libertad en la gestión de formatos de archivo, posibilitando la configuración y establecer los formatos pertinentes para preservación.

5. Servicios de almacenamiento en la nube

De acuerdo con Vázquez-Moctezuma (2015) el almacenamiento en la nube o también conocido como *cloudcomputing* se da gracias al uso de equipos virtualizados compuestos por una infraestructura informática que es indivisible para el usuario, pero que su funcionamiento sustituye la infraestructura local física tradicionalmente utilizada, de igual manera, el Instituto Nacional de Estándares y Tecnologías de los Estados Unidos (NIST) considera que se trata de un modelo que permite el acceso bajo demanda a través de la red a un conjunto compartido de recursos de computación configurables que pueden ser rápidamente provisionados con el mínimo esfuerzo de gestión o interacción del proveedor del servicio.

Las ofertas de las diferentes empresas que brindan servicios de almacenamiento en la nube en relación con los procesos de preservación digital, va desde un servicio de ordenador virtual, servicios de almacenamiento simple y servicios de almacenamiento en bloque, siendo esta última la que brinda una solución aproximada a un modelo de preservación digital pues por medio de una red de área de almacenamiento, conocida como SAN, encargada de garantizar el acceso continuo de los objetos depositados, otorgando cierta fiabilidad ante cualquier incidente tecnológico (Lejía-Roman, 2017, p. 61).

Existen diversas modalidades de servicios en la nube, según De la Vega (2013) pueden ser divididos principalmente en tres, que corresponden a:

- Infraestructura como servicio (IaaS): los proveedores de IaaS ofrecen máquinas virtuales preconfiguradas que se pueden usar como si se tuviera un servidor físico, los usuarios alquilan o subcontratan una infraestructura de hardware a un tercero.
- Plataformas como servicio (PaaS): incluye una plataforma completa que permite compilar código, almacenar información en una base de datos y entregar la aplicación desde una sola plataforma.

- Software como servicio (SaaS): proporciona diversos softwares a los usuarios, por ejemplo, aplicaciones de correo electrónico y procesadores de texto en línea, en este tipo las opciones de software a las que el usuario puede acceder son amplias y van cambiando conforme a las necesidades de las organizaciones.

Un Archivo Digital en la nube puede ser hospedado en un servicio bajo la modalidad SAAS y nunca podría ser tan sólo un servicio IaaS o PaaS, debido a que ofrece una tecnología robusta que no solamente tenga la posibilidad de almacenar en la nube, sino también la opción de hospedar una herramienta que ejecute las funciones de preservación, en ese sentido, las plataformas de nube mencionadas a continuación pueden hospedar un servicio de Archivo Digital, pero ninguna, por sí misma constituye uno.

5.1 Google Cloud Storage

Google Cloud Storage consiste en una solución de almacenamiento de objetos digitales diseñada para complementar el *cloudcomputing* perteneciente a la compañía Google, conocido como Google Cloud PlatForm, la misma se suele utilizar para el almacenamiento de datos no estructurados, sin embargo, también permite el almacenamiento y acceso de datos estructurados, estos datos pueden ser desde documentos individuales hasta copias de seguridad de grandes bases de datos (Documentación de Google Cloud, 2019).

Características y funcionalidades

Google Cloud Storage ha categorizado su servicio en cuatro tipos de almacenamiento: Standard Storage, Nearline Storage, Coldline Storage y Archival Storage; estos varían en cuanto a costo, plazo de almacenamiento y tipos de datos que se desean almacenar en la nube. Sin embargo, la única categoría que debe tener presenta para el almacenamiento, por sus funcionalidades, es la siguiente:

- **Archival Storage:** esta categoría está destinada para datos que requieren un almacenamiento de largo plazo, por esta razón ofrece un plazo de al menos 365 días de custodia en los servidores interconectados de Google, a esta modalidad

se le denomina almacenamiento en "frío", debido a que pretende custodiar datos consultados con poca frecuencia, de igual manera, entre los acuerdos a nivel de servicio propone la creación de copias de seguridad en línea para la recuperación ante desastres. La disponibilidad de los objetos digitales en Archival Storage se muestra en el siguiente cuadro:

Cuadro 5. Porcentaje de disponibilidad de los datos en Archival Storage de acuerdo con la región donde se decida almacenar

Tipo de ubicación	ANS de disponibilidad	Disponibilidad mensualtípica
Multiregión	Ninguno	99,95%
Región doble	Ninguno	99,95%
Región	Ninguno	99,99%

Fuente: Google Cloud (2020), https://cloud.google.com/storage/sla

En cuanto a su costo, esta clase de almacenamiento varía de acuerdo con la ubicación geográfica donde el cliente decida mantener custodiado su información y la modalidad en que se prefiera generar las correspondientes copias de seguridad, tal como se presenta en el siguiente cuadro:

Cuadro 6. Costo por Giga Bytes en la modalidad Archive Storage por región

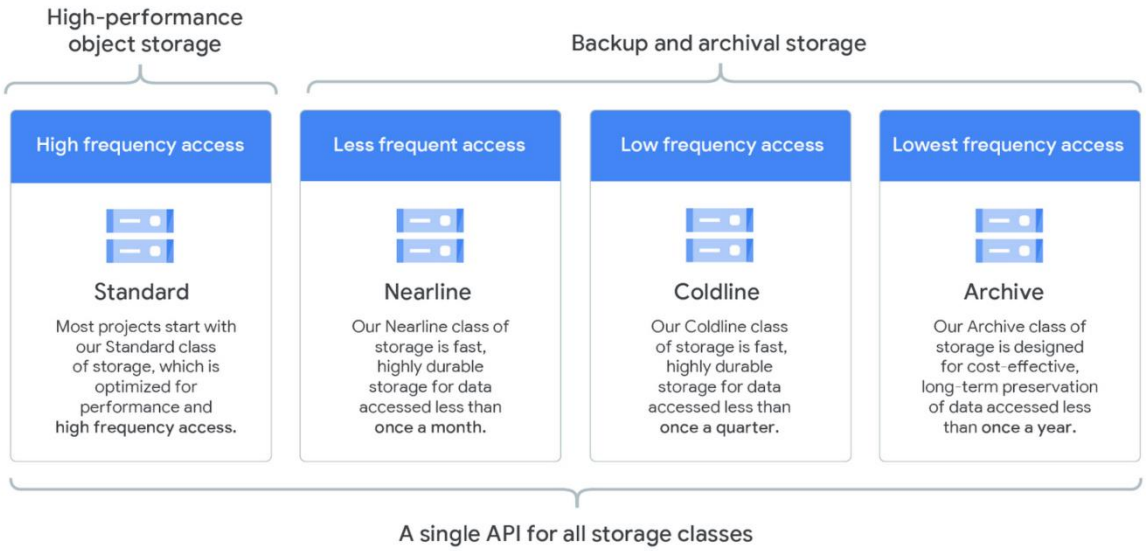
Región	Archive Storage (por GB al mes)
Unión Europea (multiregión)	0.004 USD
Asia (multiregión)	0.004 USD
Estados Unidos (multiregión)	0.004 USD
Iowa (US-Central)	0.012 USD
São Paulo (Este de Sudamerica 1)	0.030 USD

Fuente: Google Cloud (2020), https://cloud.google.com/storage/pricing#storage-pricing

Por lo tanto, después de conocer las clases de almacenamiento y sus principales características se puede establecer que Cloud Storage apunta a cubrir dos tipos de necesidades requeridas por sus clientes, la primera de ellas es de acuerdo con la

dinámica de trabajo que se tendrá con los objetos digitales que se pretenden custodiar, como se muestra en la siguiente figura:

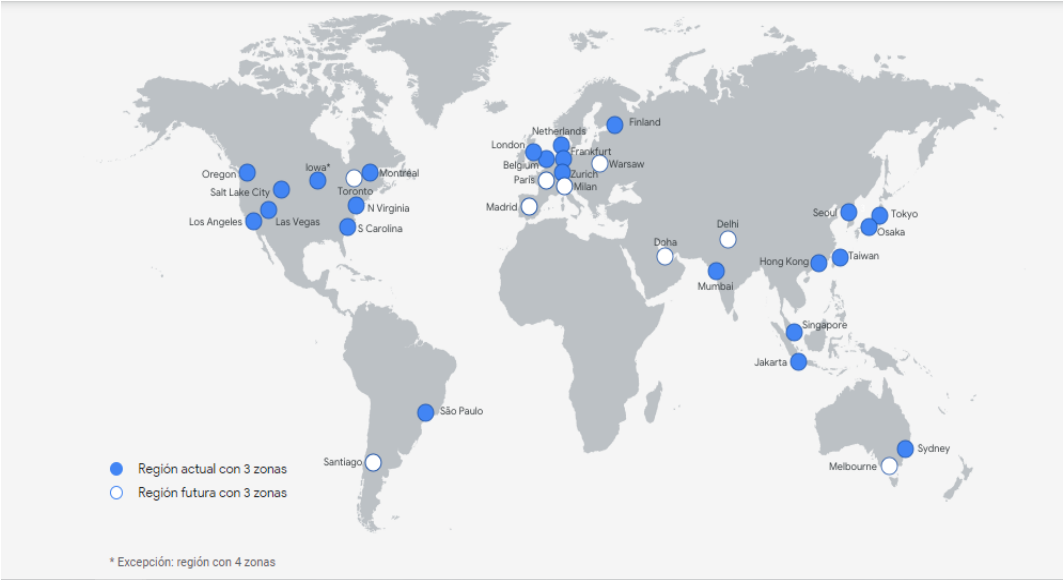
Figura 9. Principales características de las clases de almacenamiento en GCS



Fuente: Google Cloud PlatForm (2020), https://cloud.google.com/blog/products/storage-data-transfer/archive-storage-class-for-coldest-data-now-available

La segunda necesidad que pretende cubrir y por medio de la cual establece los precios de almacenamiento, corresponde a la disponibilidad de los objetos digitales, para ello Google ha dispuesto de recursos de almacenamiento en diversos zonas alrededor del mundo, a través de los cuales el cliente tiene la posibilidad de distribuir los respaldos de su información en diversas regiones, permitiendo acceder a la misma en caso de falla o con el fin de maximizar las posibilidades de supervivencia ante desastres naturales o provocados por una falla en el fluido eléctrico u otra perturbación que produzca la interrupción en el flujo de la información en alguno de sus servidores. Por medio de la siguiente figura se visualiza la ubicación de la infraestructura de Google alrededor del mundo:

Figura 10. Ubicaciones a nivel mundial de los recursos de almacenamiento de Google, durante el 2020



Fuente: página web de Google Cloud

5.2 Amazon

La empresa Amazon también se ha unido a la industria de almacenamiento de objetos digitales, al igual que Google Cloud PlatForm, ha creado todo un ecosistema de soluciones ofimáticas en la nube, en donde sus clientes pueden crear, editar, desarrollar, compartir y almacenar los productos de trabajo, de esta manera su *cloudcomputing*puede almacenar desde datos estructurados hasta la información generada desde la página web o aplicación de la organización que adquiere sus servicios.

Características y funcionalidades

Esta colección de servicios se denomina Amazon Web Service o también conocido como AWS por la abreviación de su nombre. AWS, ofrece a sus clientes diversas soluciones de almacenamiento:

I. **Almacenamiento de Archivos**

Amazon Elastic File System o Amazon EFS: basa su servicio en el Sistema de Archivos NFS que permite almacenar y distribuir archivos a través de la red de forma

centralizada, sin embargo, se debe contemplar que en este tipo de sistemas la configuración se facilita si se realiza por medio de un entorno Linux, de igual manera es compatible con los principales Sistemas Operativos (SO).

Es importante comprender este aspecto, pues bajo esta modalidad Amazon ofrece la opción de conectar las aplicaciones y sistemas locales de sus clientes con su nube, formando de esta manera una nube híbrida, con la cual se pretende mejorar la latencia y acceso de los datos, por lo tanto, el servicio EFS se relaciona de mejor manera con empresas o instituciones que utilizan el SO Linux (Amazon Web Services, 2020, p. 6). Los precios para acceder a esta tipología de servicio se detallan a continuación:

Cuadro 7. Precios por servicio en Amazon EFS

Amazon EFS	
Almacenamientoestándar (GB/mes)	0,30 USD
Almacenamiento de acceso poco frecuentes (GB/mes)	0,025 USD
Solicitudes de acceso poco frecuentes	0,001 USD
Rendimiento aprovisionado (MB/s-mes)	6,00 USD

Fuente: sitio web oficial de Amazon. (2020). https://aws.amazon.com/es/efs/pricing/

Amazon FSx para Windows File Server: esta modalidad se basa en Windows Services, con ello busca proporcionar un amplio conjunto de funciones administrativas que incluyen restauración de datos, cuotas de usuario y listas de control de acceso. Además, ofrece la creación de copias de seguridad diarias y el cifrado de los datos tanto en reposo como en tránsito, cuando se lleven a cabo transferencias (Amazon, 2020).

De igual manera, propone dos tipos de almacenamiento, dependiendo del hardware que sea utilizado para dicha función, ya que pueden utilizarse Solid State /Unidades de Estado Sólido (SSD) o Hard Drive/Disco Duro (HDD), la diferencia entre ambas radica en que los HDD se encuentran conformados por piezas móviles, específicamente un disco que gira y un brazo mecánico que lee y escribe la información, en cambio los SSD es una sola pieza compacta, por lo que existe un

menor riesgo a sufrir daños físicos en comparación con los HDD, sin embargo, es más costoso y esta diferencia se refleja en el siguiente cuadro de precios:

Cuadro 8. Precios por capacidad de almacenamiento en FSx Windows File Server

Amazon FSxpara Windows File Server	
Capacidad de almacenamiento SSD (GB/mes)	0,130 USD
Capacidad de almacenamiento HDD(GB/mes)	0,013 USD
Capacidad de rendimiento (MBps/mes)	2.200,00 USD
Almacenamiento de copias de seguridad (GB/mes)	0,050 USD

Fuente: sitio web oficial de Amazon. (2020). https://aws.amazon.com/es/fsx/windows/pricing/?nc=sn&loc=3

II. **Almacenamientoenbloque**

Amazon Elastic Block Store: consiste en un servicio de almacenamiento en bloque, es decir, los datos resguardados bajo esta modalidad se dividen y se almacenan en partes separadas, esto de acuerdo a criterios previamente establecidos por el cliente, por consiguiente, esto permite que sea utilizado en bases de datos relacionales y no relacionales, aplicaciones empresariales, aplicaciones en contenedores, motores de análisis de big data y flujos de trabajo de contenido multimedia (Amazon, 2020).

Como método de seguridad ofrecen la generación de instantáneas de los datos custodiados en cada uno de los bloques, esto quiere decir que se generan copias de seguridad de datos de manera periódica que pueden servir para la recuperación ante desastres y migrar a otros servicios de almacenamiento. En cuanto al costo, con Amazon EBS se paga de acuerdo con el consumo.

Cuadro 9. Precios de acuerdo con el volumen de uso en Amazon EBS

Cantidad	Precios
Volúmenes de SSD de uso general	0,10 USD por GB-mes de almacenamiento aprovisionado
Volúmenes de SSD de IOPS provisionadas	0,125 USD por GB-mes de almacenamiento aprovisionado Y 0,065 USD por mes de IOPS provisionadas
Volúmenes de SSD de IOPS provisionadas	0,125 USD por GB-mes de almacenamiento aprovisionado Y 0,065 USD por mes de IOPS provisionadas
Volúmenes de HDD optimizados para el desempeño	0,045 USD por GB-mes de almacenamiento aprovisionado
Volúmenes de HDD frío	0,015 USD por GB-mes de almacenamiento aprovisionado

Fuente: sitio web oficial de Amazon. (2020). https://aws.amazon.com/es/ebs/pricing/

5.3 Microsoft Azure

Microsoft Azure es una plataforma en la nube que cuenta con más de 200 productos y servicios en la nube, por medio de los cuales se posibilita la creación, ejecución y administración de aplicaciones en múltiples nubes, utilizando las herramientas y los marcos de acuerdo con la elección del usuario, con esto busca permitir la interoperabilidad entre sistemas y herramientas (Microsoft, 2020).

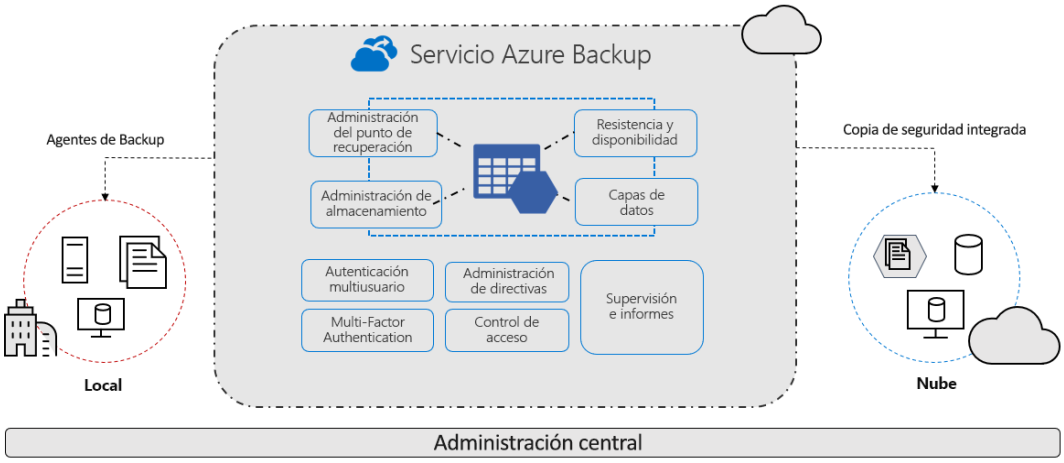
Azure trabaja bajo el paradigma de *Cloud Computing*, en donde se pueden encontrar los siguientes servicios: desarrollo de aplicaciones, inteligencia artificial, migración a la nube, análisis de datos, nube e infraestructuras híbridas, seguridad y gobernanza, además de presentar una serie de productos como migración de datos, seguridad de los datos, contenedores, *blockchain* y almacenamiento.

Características y funcionalidades

Por consiguiente, Azure ofrece diversos tipos de almacenamiento, teniendo en cuenta las necesidades de sus clientes, los mismos son divididos y caracterizados por Microsoft de la siguiente manera:

- **Azure Disk Storage o almacenamiento en disco:** herramientas diseñadas para las cargas de trabajo críticas, ofrece almacenamiento en bloque de alta durabilidad. Ofrece 3 opciones de almacenamiento de acuerdo con los recursos físicos destinados al resguardo de la información, pues tienen discos SSD premium, SSD estándar y HDD estándar. Esta modalidad dispone de una capacidad de almacenamiento de 32 TB para cada uno de los discos utilizados, además, se han dispuesto de recursos de almacenamiento en diversas zonas geográficas por todo Estados Unidos y Canadá.
- **Blob Storage:** es una solución de almacenamiento de objetos, específicamente se encuentra diseñada para administrar datos no estructurados, por lo que frecuentemente es destinada a procesos como el análisis de datos, de igual manera, ofrece asegurar la información suministrada por medio del cifrado de datos.
- **Azure Backup o solución de copia de seguridad integrada para todos sus recursos:** comprende una solución que se encarga de realizar las copias de seguridad de los recursos dispuestos en la nube de Azure, por lo tanto, puede generar y administrar copias de seguridad de datos, objetos digitales, carpetas, bases de datos, entre otros. El funcionamiento de Azure Backup se logra explicar de mejor manera por medio de la siguiente figura:

Figura 11. Administración de las copias de seguridad en Azure



Fuente: documentación de producto Microsoft Azure. (2019). https://docs.microsoft.com/es-es/azure/backup/backup-overview

- **File Storage Azure:** esta modalidad ofrece el uso de diversos protocolos de implementación de sistemas de archivos en la red como NFS, compatibles con el SO Linux y SMB, compatible con el SO Windows, ambas permiten compartir y administrar servicios de archivo de forma centralizada, de esta manera, Azure incorpora el concepto de nube híbrida como parte de sus servicios, por medio de la cual combina la información almacenada en una infraestructura local o nube privada con una nube pública.

Precios para la adquisición de almacenamiento en Azure

Azure ofrece un servicio de calculadora que permite realizar un análisis según las necesidades del cliente, permitiendo la elección del tipo de almacenamiento requerido, el tipo de redundancia, la región donde se va a encontrar el almacenamiento, por ejemplo: seleccionando el almacenamiento en Bloques o block blob storage, región principal el Este de los Estados Unidos, redundancia: GRS y con un nivel de rendimiento estándar. De acuerdo con las anteriores características el precio se estableció en: 1,485.61 USD; lo anterior se desglosa en el siguiente cuadro:

Cuadro 10. Precio según servicio y características en Azure

Servicio	Características	Precio
Almacenamiento	BloquesBlob 60TP	183.71 USD
Nivel de almacenamiento	Estándar	
Redundancia	Geo Replicación 60 TP	1,228.80 USD
Operaciones de escritura por mes	1000 operaciones	2.10 USD
Operaciones de listas y creación de contenedores	100000 operaciones	1.00 USD
Operaciones de lectura	100000 operaciones	500.00 USD
Recuperación de datos	1000 GM	20.00 USD
Operaciones de escritura	Sin límite	0.00 USD
Total		**1,485.61 USD**

Fuente: elaboración propia con información del sitio web oficial Microsoft Azure, 2020

Los precios pueden variar dependiendo de la zona en la que se decida mantener el almacenamiento, en el siguiente cuadro se puede apreciar el precio de sus servicios de almacenamiento con las mismas características que se muestran en el cuadro anterior, pero con una ubicación geográfica distinta:

Cuadro 11. Precio del servicio de almacenamiento según la ubicación geográfica

Región	Precio
Este de Estados Unidos	1,485.61 USD
Este de Asia	5,901.81 USD
Australia Central	7,998.75 USD
Sur de Brasil	10,277.06 USD
Canadá Central	1,690.13 USD
Francia Central	1,726.96 USD
Sur de Europa	1,480.52 USD

Fuente: elaboración propia con información tomada del sitio web oficial Azure, 2020

6. Servicios de preservación y almacenamiento nacionales

A nivel nacional existen diversas empresas que se dedican actualmente a ofrecer un servicio de preservación y almacenamiento, por lo que a través del presente apartado se busca conocer el servicio que actualmente ofrecen y cuáles son sus funcionalidades, lo anterior con el fin de determinar si pueden ser competentes para hospedar un Archivo Digital, sin embargo, no se logró obtener la información de todas las empresas públicas y privadas que anuncian este tipo de servicios, pese a los constantes intentos de establecer una comunicación directa por medio de oficios, correos y llamadas telefónicas.

Entre las empresas que se pudo recabar información sobre sus servicios se encuentran:

6.1 Radiográfica Costarricense S.A (RACSA)

La compañía Radiográfica Costarricense, también conocida como RACSA, es una empresa pública que brinda soluciones tecnológicas en el país, por lo tanto, también ha incluido dentro de su catálogo de productos y servicios los recursos tecnológicos relacionados con el almacenamiento y la producción documental.

De esta forma, RACSA dispone de un conjunto de servicios que posibilitan el almacenamiento de información y la virtualización de recursos digitales, de tal manera, que sus clientes tienen la posibilidad de tercerizar la administración de sus DataCenter, para ello ofrecen un equipo de trabajo certificado y en cumplimiento de normas y guías como ITIL, COBIT e ISO por medio de los cuales buscan garantizar la seguridad y la continuidad del servicio (RACSA, 2021).

Asimismo, ofrece la opción de suministrar infraestructura de hardware y software con administración propia, aplicando herramientas de virtualización para que los clientes tengan acceso remoto, es por ello que también incorpora la realización de respaldos, con el fin de alcanzar una alta disponibilidad (RACSA, 2021).

Por último, promociona una de sus productos que consideran como un Sistema de Gestión Documental, denominado como RACSA Doc´s, esta solución es promovida por el sitio web oficial de la empresa como un sistema que permite la integración con

otros sistemas tecnológicos y la organización de la información por medio de la conformación de expedientes digitales, de igual manera, aseguran que el sistema cumple con la norma ISAD-G, específicamente con los elementos obligatorios de la norma y con el estándar PDF/A-3, a su vez, se encuentra conformado por flujos de trabajo, mecanismos de autenticación y la validación de firmas digitales de los documentos recibidos (RACSA, 2021).

6.2 Empresa Servicios Públicos de Heredia

La Empresa Servicios Públicos de Heredia (ESPH) es una empresa pública no estatal que se dedica a brindar servicios comerciales e industriales, dentro de los cuales se encuentra la prestación de servicio relacionados con las telecomunicaciones, de esta forma, ha ido incursionando tanto en oferta de servicios de infraestructura tecnológica como en adecuación de software orientados a la preservación digital.

Por medio del proceso de licitación n°8111250292038894 para la adquisición de una "solución servicio como sistema (SaaS) de un gestor documental y repositorio digital" gestionada por la Dirección Nacional de Notariado (DNN), en el año 2020, se logró tener acceso y conocer la oferta de ESPH a través del Sistema Integrado de Compras Públicas (SICOP).

Como parte de las características de almacenamiento definidas por la DNN se encontraba el almacenamiento de la información digital por medio de bases de datos y no a través de carpetas contenidas en File Systems o Sistemas de Archivos, esto porque dentro de sus especificaciones se establece la utilización de Paquetes de Información en cumplimiento del Modelo de Referencia OAIS, por consiguiente, en este entendido dentro de los componentes de entrega se pueden encontrar elementos como: licencias de Microsoft SQL Server Standard Edition 2019 (base de datos relacional), alquiler mensual del software Arca para Plataforma de Gestión Documental y el servicio mensual de infraestructura de servidores Windows ADN.

Otro de los aspectos considerados en concordancia con la seguridad de la información fue la realización de copias de seguridad en línea en ubicaciones remotas, en cumplimiento del ítem 7 de la sección 2 de la Directriz 29-2007 de la

Junta Administrativa del Archivo Nacional, de igual forma, el centro de datos que hospeda la solución debe tener la certificación TIER de nivel 3.

El costo mensual del servicio, de acuerdo con el Formulario de Justificación de Solicitud de Contratación de Bienes y Servicios (2020), se fijó en un total de ¢3.610.000,00 durante un periodo de 12 meses, sin embargo, se debe considerar que este monto engloba tanto el software de preservación como la infraestructura tecnológica para el almacenamiento lógico de los materiales digitales.

7. Conclusiones del diagnóstico

De acuerdo con el diagnóstico de la situación actual de Costa Rica en materia de preservación digital, se llegaron a las siguientes conclusiones:

Del análisis normativo nacional:

- La normativa en materia de preservación digital es insuficiente, y se encuentra dispersa en diferentes directrices, normas o reglamentos, los cuales brindan escasos requisitos o condiciones mínimas e insuficientes con las que deben cumplir las organizaciones para asegurar la preservación digital de la información. El Código Nacional de Tecnologías Digitales es la norma actual que más profundiza en el tema de preservación digital y a su vez recomienda modelos de referencias, normas y estándares de buenas prácticas importantes a tomar en cuenta cuando se va a implementar cualquier proyecto de preservación digital.

De los proyectos de preservación digital:

- A nivel nacional únicamente el Archivo Universitario Rafael Obregón Loría y la Dirección General del Archivo Nacional han incursionado en soluciones de preservación digital. En el primero, ADUCR, surgió como una visión a futuro en el año 2013, sin embargo, no logró ejecutarse por decisiones administrativas de la UCR; el segundo, ADN, aún se encuentra en proceso y no surge como una visión, sino que fue reactivo al proceso de transferencia documental que debe realizar la Presidencia de la República y los ministros de Estado en febrero de 2022. En ese sentido, la escasez de iniciativas refleja un insuficiente y

preocupante desarrollo en preservación de la información digital a nivel país, puesto que se han estancado en la experimentación y no se han llegado a normalizar y ejecutar.

- Asimismo, cabe resaltar que si el proyecto ADN del Archivo Nacional, se logra ejecutar a cabalidad, traerá consigo una serie de beneficios para todas las organizaciones del SNA, pues pretende ser un proyecto integral, que no solo brindaría un repositorio de preservación digital sino también, capacitación, normalización, almacenamiento, mantenimiento y acompañamiento, por lo que representaría un avance significativo en la preservación de la información digital en Costa Rica.

De los resultados de la encuesta aplicada al SNA

- Todas las organizaciones del SNA están produciendo y recibiendo documentos digitales, sin embargo, muchas no tienen los conocimientos, apoyo y mecanismos adecuados para gestionarlos y almacenarlos de una manera segura y controlada, ya que la actual evolución tecnológica y la latente obsolescencia, obliga a que la custodia de la información digital sea un proceso en constante evolución, y tener un repositorio digital y aplicar respaldos o copias de seguridad, no necesariamente son sinónimo de preservación digital.
- Las prácticas más generalizadas a nivel nacional son implementar sistemas de gestión de documentos electrónicos y repositorios digitales, distantes de la teoría archivística y sin antes establecer políticas, estrategias o directrices en materia de preservación digital, protección de datos y continuidad digital, lo cual impide tener una estrategia y una visión integral de lo que implica preservar, del valor que tiene la información para la organización, de los roles y responsabilidades que se deben designar y asumir e impide además, una oportuna priorización y gestión de los riesgos a los que se expone la información digital.
- Existe una clara confusión entre almacenamiento y preservación digital, ya que una parte considerable de las organizaciones encuestadas señalan que cumplen con lo dispuesto en el Código Nacional de Tecnologías Digitales, que disponen de estrategias de preservación digital y que poseen repositorios de preservación digital, cuando en realidad lo que poseen son repositorios para almacenar la

información digital (centros de datos locales, en la nube o una combinación de ambas) pero no para preservarla.

- Se detectó que en algunas instituciones el departamento de archivo central tiene poca o nula injerencia, al considerar que la preservación digital es un tema que solamente atañe al campo tecnológico, lo cual resulta sumamente grave y alarmante, pues refleja que se está excluyendo el criterio archivístico de la toma de decisiones relativas a la preservación, por lo que no se puede garantizar que las acciones implementadas sean orientadas a garantizar la autenticidad, integridad y fiabilidad de los objetos digitales custodiados en las plataformas utilizadas.
- La insuficiencia de recursos económicos que actualmente experimenta las instituciones del sector público, ha provocado que lo destinado a la implementación de proyectos de preservación sea cada vez más limitado, lo cual ha empujado a las organizaciones a adoptar servicios en la nube como herramientas para el almacenamiento de los documentos producidos, si bien estas plataformas brindan una serie de beneficios a nivel de costos, también representan un riesgo para la preservación del contenido de los documentos, ya que no se basan en estrategias de preservación digital, se alejan de la teoría archivística, del modelo de referencia OAIS y de la cadena de custodia de la información digital.

De las Soluciones de Preservación Digital

- A nivel internacional se ha experimentado un proceso de concientización sobre la importancia de los procesos de preservación de la información digital, trayendo consigo avances significativos en la creación de solución espara la preservación digital, las cuales pueden ser adaptadas cada vez con mayor frecuencia al contexto nacional, no obstante, se requiere de la sensibilización de los tomadores de decisión y de unidades técnicas capacitadas y competentes para la generación del cambio requerido.

De los servicios de almacenamiento en la nube

- Los servicios de almacenamiento en la nube, como *Software as a Service* o SaaS, pueden convertirse en una opción para hospedar un servicio de Archivo Digital, pero ninguna, por sí misma constituye uno.

De los servicios de preservación y almacenamiento nacionales

- Pese a que no se pudo obtener información del total de la población de las empresas públicas y privadas que ofrecen actualmente un servicio de almacenamiento y preservación digital, se logró determinar que algunas de ellas brindan un servicio que se centra en el almacenamiento de datos, sin embargo, estos no consideran las funcionalidades que debe cumplir un Archivo Digital.
- A la inversa, también se identificó un ejemplo de alianza que permitió incorporar las funcionalidades de un Archivo Digital a los servicios de almacenamiento que habitualmente manejan las empresas, como lo fue la licitación gestionada por la Dirección Nacional de Notariado, de igual manera, este caso ratificó la necesidad de desarrollar previamente un proceso de culturización a nivel institucional que permitan establecer las bases que faciliten la incorporación de una solución de preservación de documentos digitales.

CAPÍTULO IV.
EVALUACIÓN DE RIESGOS ASOCIADOS A LA PRESERVACIÓN DIGITAL DE DOCUMENTOS EN EL SISTEMA NACIONAL DE ARCHIVOS.

CAPÍTULO IV. EVALUACIÓN DE RIESGOS ASOCIADOS

A través del presente apartado se pretende desarrollar la evaluación de los riesgos asociados a la preservación digital de documentos en el SNA, tomando como insumo el diagnóstico de la situación actual, desarrollado en el capítulo anterior, lo cual permitirá visualizar un escenario que sirva de punto de partida para el diseño del marco de evaluación para soluciones de preservación digital y la herramienta disponible en línea, por lo tanto se procederá a identificar los peligros y la valoración de los riesgos.

1. Gestión del riesgo

La gestión del riesgo forma parte esencial de todas las actividades asociadas con la organización, en Costa Rica el marco normativo básico que regula la gestión y valoración del riesgo está conformado por la Ley General de Control Interno N° 8292, los artículos 2 inciso f, 14, 18 y 19 contemplan la valoración del riesgo según lo que se indica a continuación:

- Es deber del jerarca y los titulares subordinados realizar la valoración del riesgo, donde se identifiquen y analicen los riesgos, y su posible efecto en la consecución de los objetivos de la institución; así como determinar su impacto y la probabilidad de que ocurran, y decidir sobre las acciones que se tomarán para administrarlos.

- Todo ente u órgano deberá disponer de un Sistema Específico de Valoración del Riesgo Institucional (SEVRI) por áreas, sectores, actividades o tareas que, de conformidad con sus particularidades, permita identificar el nivel de riesgo institucional y adoptar los métodos de uso continuo y sistemático, con el fin de analizarlos y administrarlos, y que se ubiquen en un nivel de riesgo organizacional aceptable.

- La Contraloría General de la República, emitió las Directrices Generales para el Establecimiento y Funcionamiento del Sistema Específico de Valoración del Riesgo Institucional (SEVRI), las cuales son de acatamiento obligatorio.

Pese a existir un marco regulatorio en materia de riesgos, las instituciones públicas parecen no considerar su Archivo Digital y por ende la continuidad de la información digital en sus SEVRI, lo cual se evidenció en el diagnóstico desarrollado en el capítulo anterior, cuando se les cuestionó a las instituciones del SNA sobre la gestión de los riesgos relacionados a su información, alrededor del 70% de las instituciones:

1. No establecen marcos de referencia para gestionar los riesgos producidos y dar continuidad a la información digital (67,3 %).

2. No desarrollan informes de evaluación de riesgos de continuidad digital y por tanto no están disponibles para la toma de decisiones dentro de la organización (69,2 %).

3. No se han establecido los roles y responsabilidades para gestionar los riesgos relacionados a la continuidad digital (67,3 %).

4. No se han definido los objetivos y criterios de éxito para la evaluación del riesgo para la continuidad digital (71,2 %).

5. No se ha establecido un proceso de cómo se identificarán, analizarán, controlarán, registrarán, monitorearán y revisarán los riesgos (67,3 %).

Con base en lo anterior, se evidencia que, aunque las instituciones están implementando medidas para mejorar los sistemas que gestionan y administran su información digital, están dejando de lado la gestión de riesgos asociados, lo cual es esencial para la continuidad digital de la información en el Archivo Digital. Todas las actividades realizadas en el Archivo Digital conllevan un riesgo asociado, por lo cual debe gestionarse su incertidumbre mediante la identificación, análisis y valoración de los riesgos, para aumentar la probabilidad de alcanzar los objetivos del Archivo Digital.

A continuación, se identifican los principales riesgos detectados en el diagnóstico sobre preservación digital aplicado al Sistema Nacional de Archivos.

2. Identificación del riesgo

Teniendo en consideración lo expuesto anteriormente, se utilizó como técnica de identificación de riesgos una lluvia de ideas mediante los resultados obtenidos como parte del diagnóstico del SNA realizado en el capítulo anterior, esta técnica "implica el estímulo y el fomento de conversaciones fluidas entre un grupo de personas competentes, con objeto de identificar los posibles modos de fallo y los peligros asociados, los riesgos, los criterios para la toma de decisiones, y/o las opciones de tratamiento" (UNE-ISO 31010, 2011, p.31). Con base en las técnicas mencionadas, se lograron identificar los siguientes riesgos relacionados con el proceso de preservación de documentos digitales en el SNA:

Cuadro 12. Riesgos identificados asociados a la preservación digital en el Sistema Nacional de Archivos, 2020

Código del riesgo	Riesgo identificado
R01	Pérdida de información digital.
R02	Vulnerabilidad de la información digital.
R03	Limitado acceso a la información digital.
R04	Pérdida de equivalencia funcional y valor probatorio de los documentos.
R05	Ataquesinformáticos.
R06	Accesos no autorizados a información / documentos.
R07	Obsolescencia del formato digital.
R08	Obsolescencia del software.
R09	Obsolescencia del hardware.
R10	Errores humanos que afectan la preservación de la información digital.
R11	Expiración de la criptografía del Paquete de Información Archivística.
R12	Ruptura de la cadena de custodia digital del documento.
R13	Falta de evidencia de registros de trazabilidad.
R14	Gestión insuficiente de la continuidad digital.
R15	Ineficiencia para el intercambio y utilización de información entre sistemas.

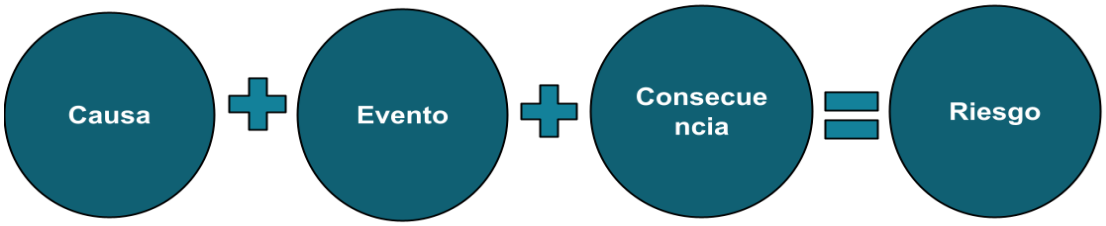
Fuente: Elaboración propia.

Con la finalidad de obtener una visión ampliada de los riesgos identificados, se utilizará la técnica del corbatín, el cual "se utiliza para presentar un riesgo mostrando una gama de causas y consecuencias" (UNE-ISO 31010, 2011, p. 72); para el cual se requiere una adecuada comprensión de la información de las causas y consecuencias de un riesgo, así como de las barreras y controles que pueden impedir o mitigar el riesgo.

Un riesgo, de acuerdo con la UNE-ISO 31000:2018 es el efecto de la incertidumbre sobre los objetivos de una organización y sus sistemas, los efectos pueden ser positivos, negativos o ambos, y puede abordar, crear o resultar en oportunidades y amenazas.

Por consiguiente, y de acuerdo con la técnica de identificación de riesgos, el riesgo es equivalente a la suma de una serie de elementos, tal como se muestra en la siguiente figura:

Figura 12. Composición del riesgo



Fuente: Elaboración propia.

Causa: son todos aquellos elementos que se pueden considerar como principio, motivo u origen de un evento que representa algún tipo de amenaza a la organización.

Evento: ocurrencia o cambio de un conjunto particular de circunstancias.

Consecuencia: resultado de la falta de mitigación de un riesgo.

Así las cosas, con base en el proceso que describe la norma UNE-ISO 31010, para elaborar el análisis de riesgos se realizaron los siguientes procedimientos:

- Mediante el análisis de los resultados del diagnóstico realizado en el SNA y además con base en una lluvia de ideas, se identificaron una serie de riesgos, los cuales estarán representados como el nudo central de una corbata.

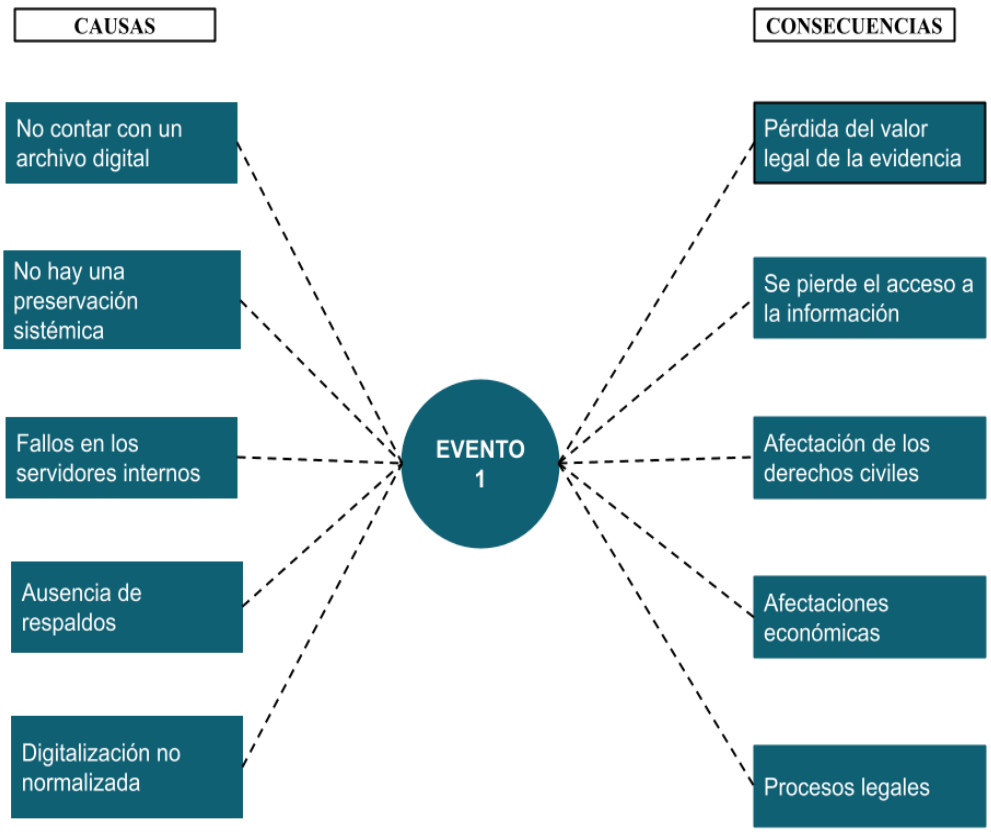
- Luego, se listan las causas del riesgo, considerando los orígenes del riesgo y se trazan las líneas entre cada causa y el evento formado, del lado izquierdo de la corbata.

- En el lado derecho de la corbata se listan las posibles consecuencias del riesgo y se trazan las líneas que unen el evento del riesgo con cada consecuencia posible.

El resultado de este proceso es un diagrama sencillo que se distingue por su fácil comprensión al mostrar de manera clara y precisa las principales causas y consecuencias, tal como se aprecia a continuación:

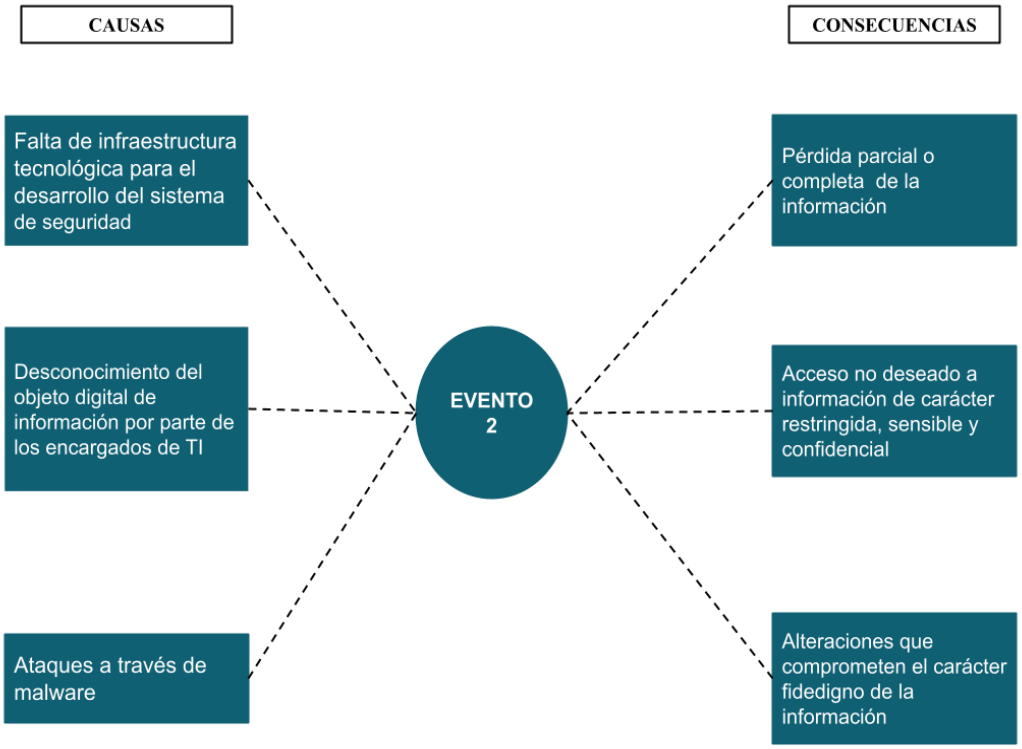
Riesgo 1: Pérdida de información digital

Descripción del evento: Un 60,8% de las instituciones encuestadas no tienen un SGDE, los SGDE existentes no aplican en su totalidad los procesos técnicos archivísticos necesarios para la gestión de documentos, además un 75,9% de las instituciones no conocen qué es un repositorio de preservación digital, y un 74,5% no han implementado una política institucional para el proceso de preservación digital; los eventos anteriormente mencionados posibilitan que se produzca pérdida de información digital.



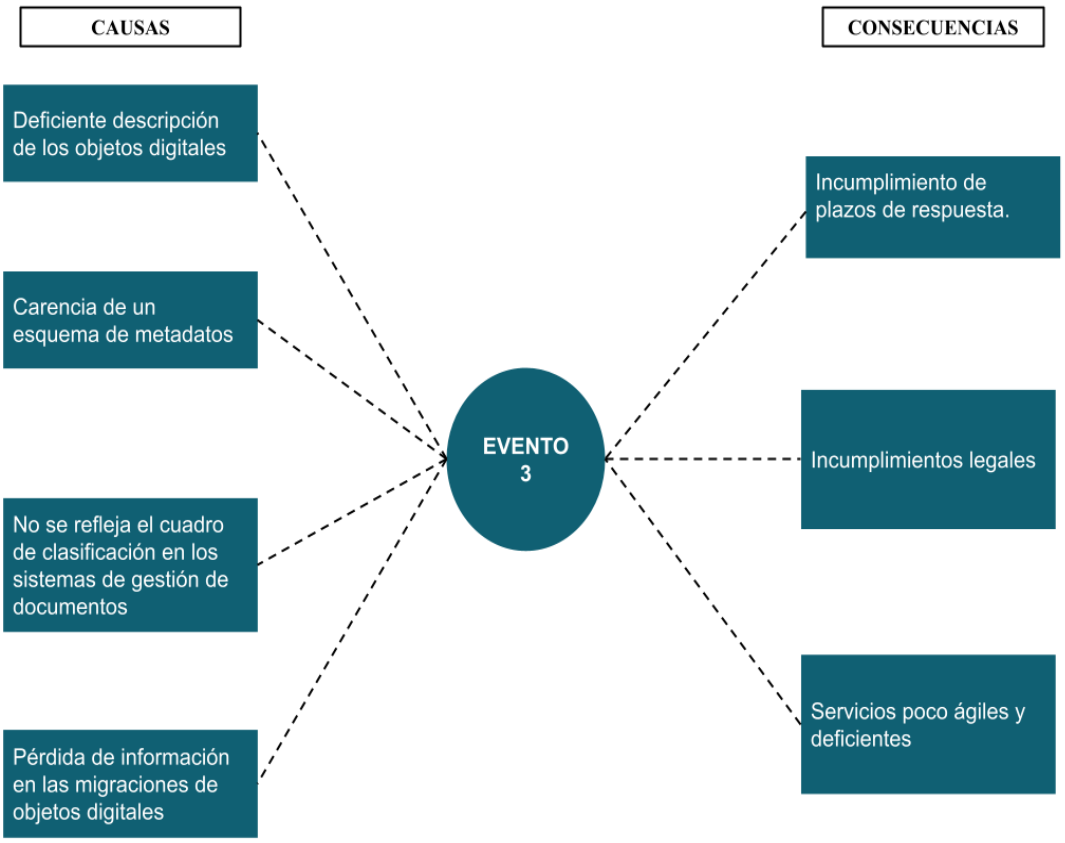
Riesgo 2: Vulnerabilidad de la información digital

Descripción del evento: La mitad de las instituciones encuestadas no aplican las medidas de seguridad establecidas en el CNTD, mientras que la mitad restante aplica solamente algunos de los elementos recomendados en la norma, por lo que la ausencia de medidas de seguridad expone a la información digital a ser vulnerada o dañada.



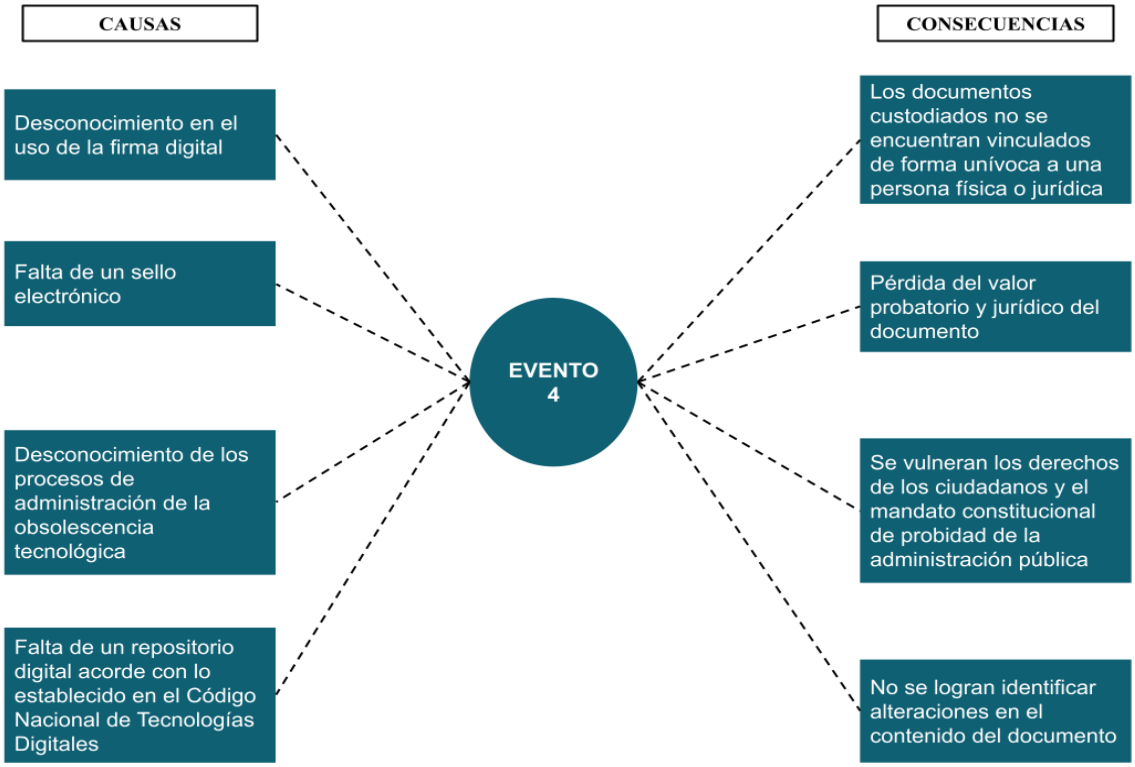
Riesgo 3: Limitado acceso a la información digital

Descripción del evento: Alrededor de un 80% de las instituciones encuestadas no tienenun esquema de metadatos normalizado, aunado a lo anterior, aproximadamente un 70% no han incorporado el cuadro de clasificación en las herramientas utilizadas para hospedar los documentos digitales. Por último, la mayoría de las descripciones realizadas a los documentos no se aplican acorde con lo estipulado en normas de descripción archivística, estos hechos dificultan el acceso a la información digital.



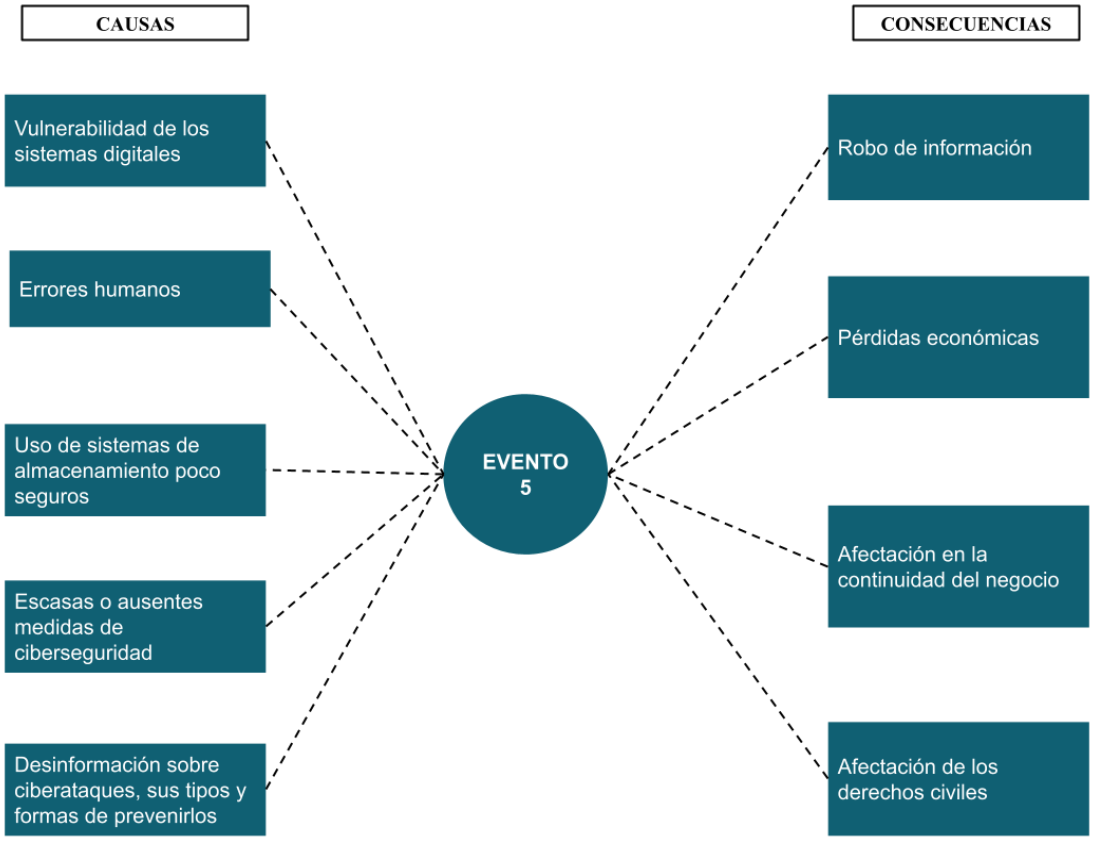
Riesgo 4: Pérdida de equivalencia funcional y valor probatorio de los documentos

Descripción del evento: Las instituciones encuestadas no tienen las condiciones adecuadas para garantizar la equivalencia funcional y probatoria de los documentos que actualmente custodian y producen, pues a mediano y largo plazo las credenciales con las que se firmaron los documentos van a expirar y no se disponen de ambientes digitales controlados, como repositorios digitales para la preservación digital, que apliquen mecanismos para monitorear activamente la integridad y autenticidad de las propiedades significativas.



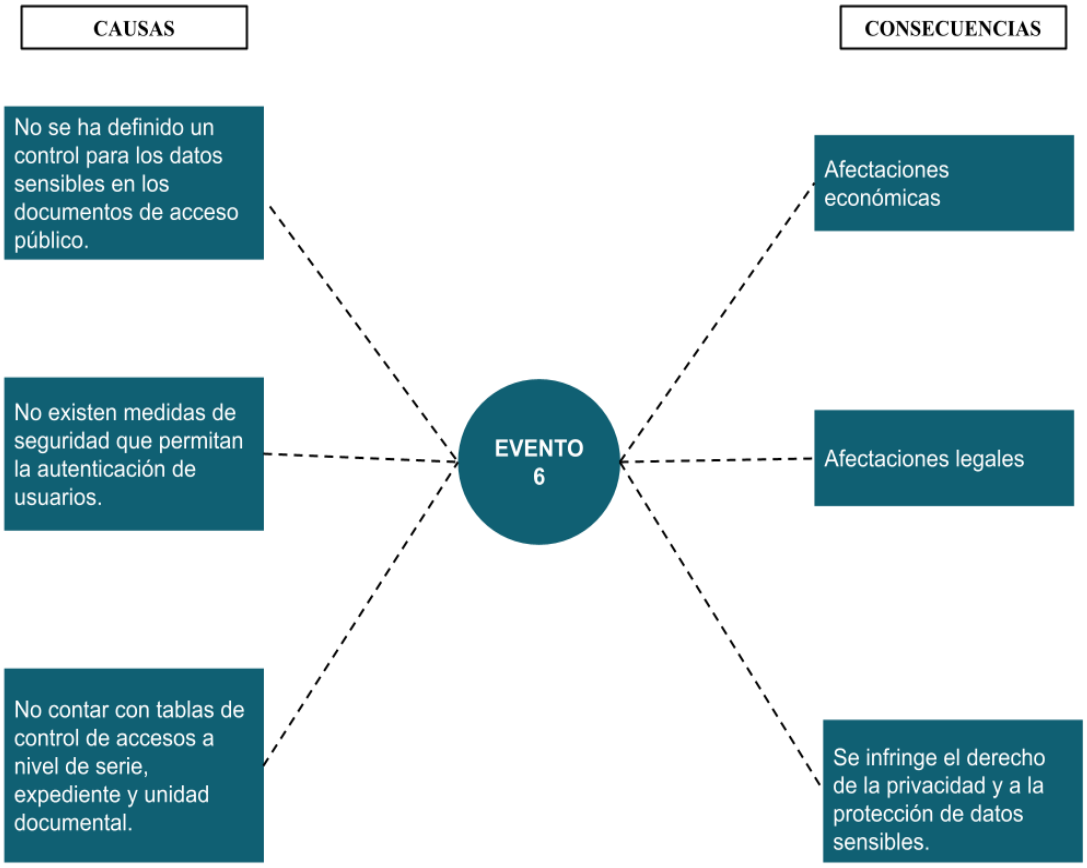
Riesgo 5: Ataques informáticos

Descripción del evento: El 47,1% de las instituciones no disponen de un plan de protección de datos acorde con las medidas establecidas por el CNTD, además, un 31% no realiza geo replicaciones de la información digital custodiada, aumentando así la posibilidad de sufrir ataques informáticos.



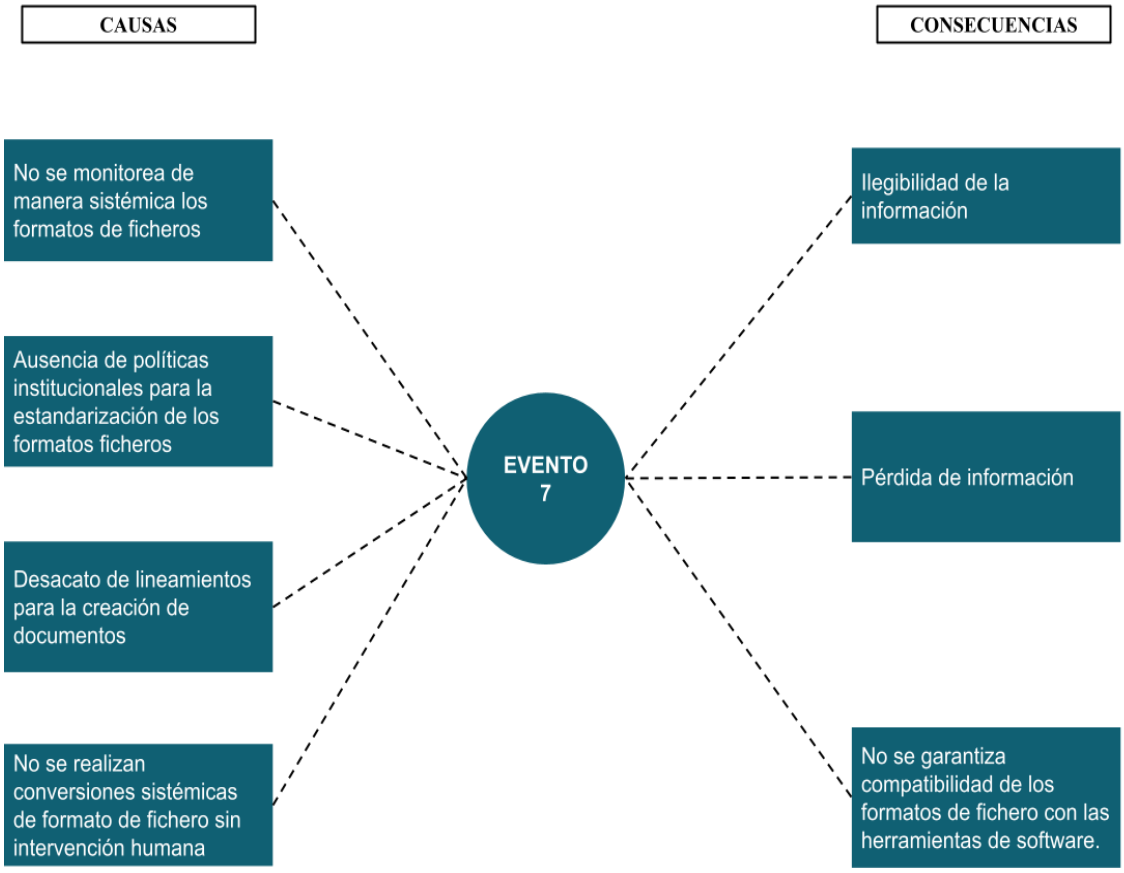
Riesgo 6: Accesos no autorizados a información / documentos

Descripción del evento: Un 27,5 % de las instituciones no han establecido tablas de controles de acceso a las series documentales, expedientes y documentos dentro de sus sistemas de información o esta actividad no es soportada por dichos sistemas de información, por lo que no tienen un control sobre los accesos a la información digital, posibilitando los ingresos no deseados sobre información con carácter restringido.



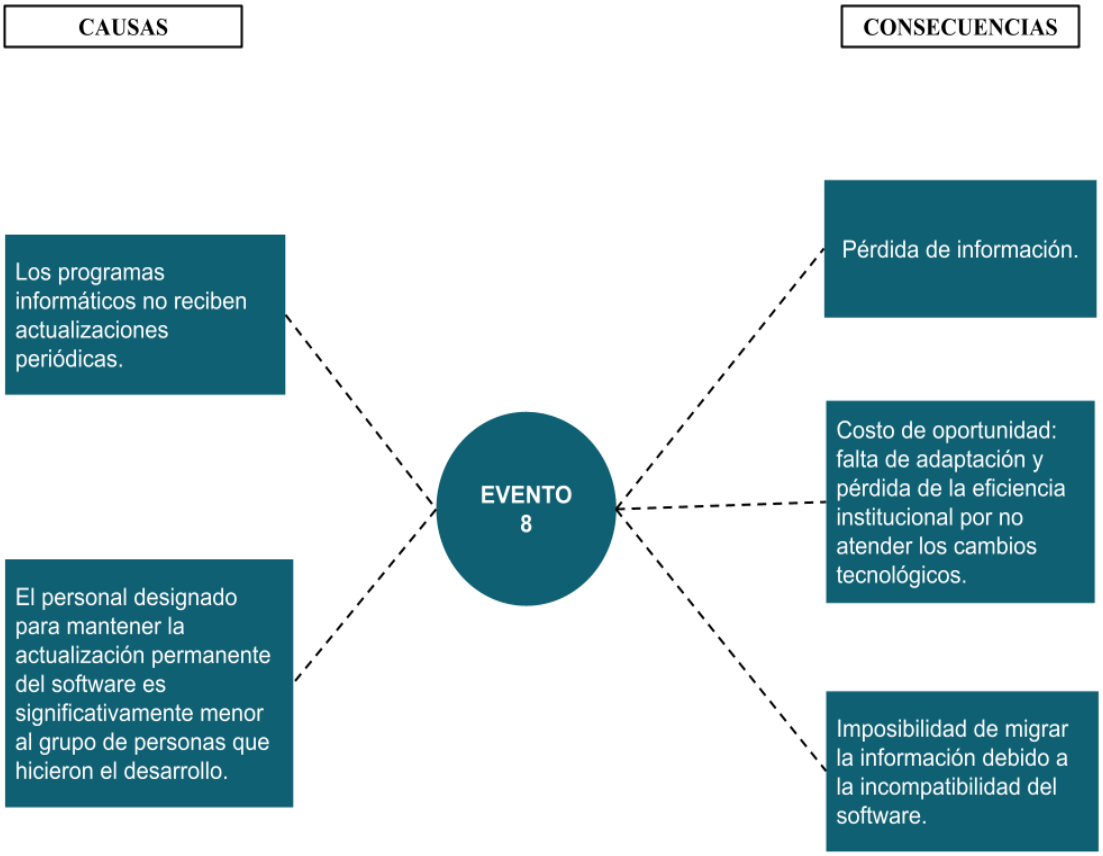
Riesgo 7: Obsolescencia del formato digital

Descripción del evento: Solamente un 28% de las instituciones aseguraron aplicar procesos de conversión de formatos como estrategia de preservación, no obstante, el grueso de las elecciones de los formatos de ficheros no se basó en información imparcial suministrada por herramientas que fueron creadas para dicho fin o tan siquiera en una norma interna, estas acciones no permiten garantizar la estabilidad de los documentos que se necesitan preservar.



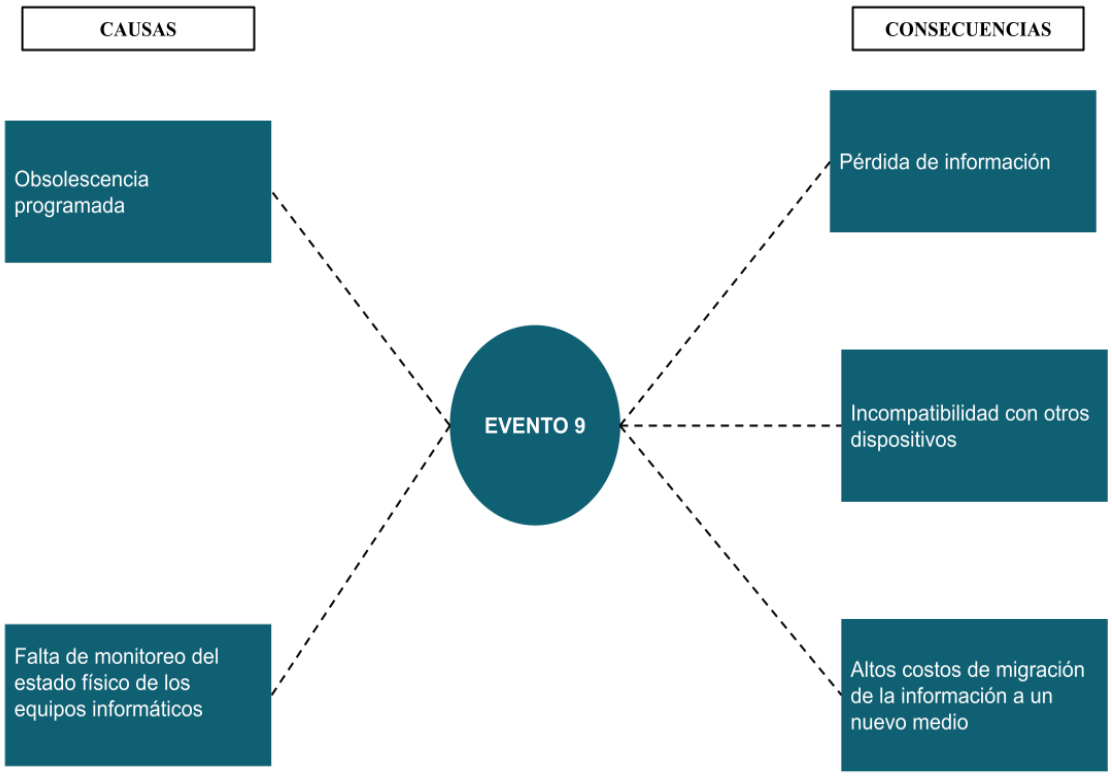
Riesgo 8: Obsolescencia del software

Descripción del evento: El software del sistema se vuelve obsoleto ya que no recibe actualizaciones periódicas; un 25% de las instituciones del SNA no controla el proceso de obsolescencia en su infraestructura tecnológica.



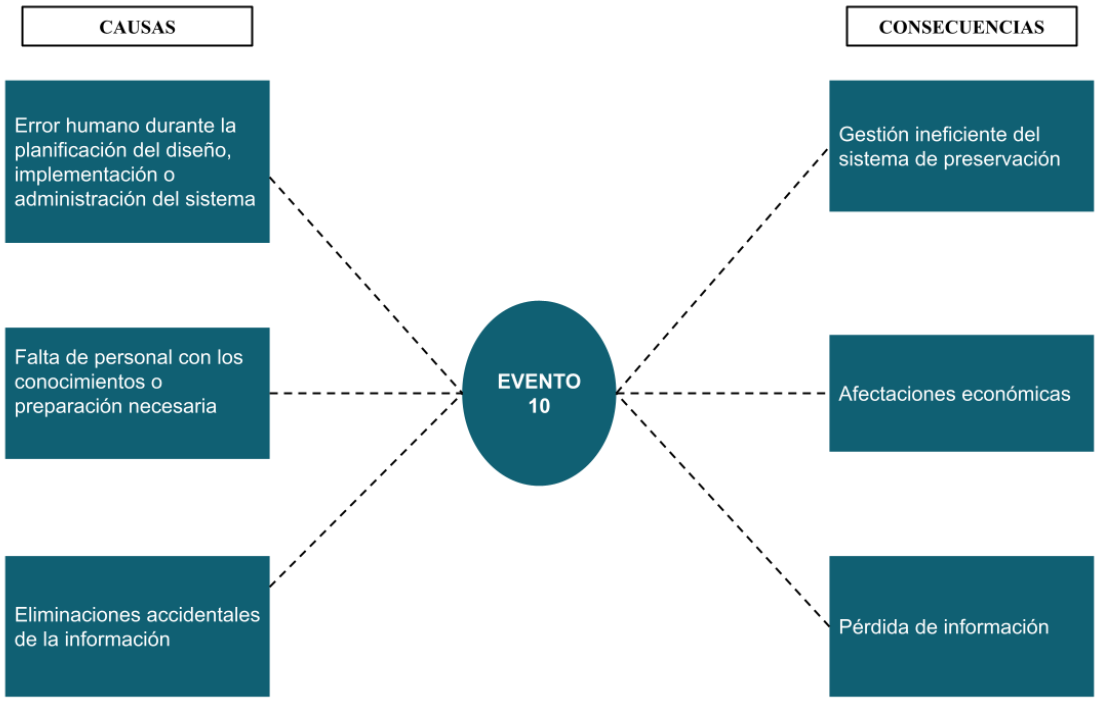
Riesgo 9: Obsolescencia del hardware

Descripción del evento: El hardware se vuelve obsoleto. Un 25% de las instituciones del SNA no controla el proceso de obsolescencia en su infraestructura tecnológica.



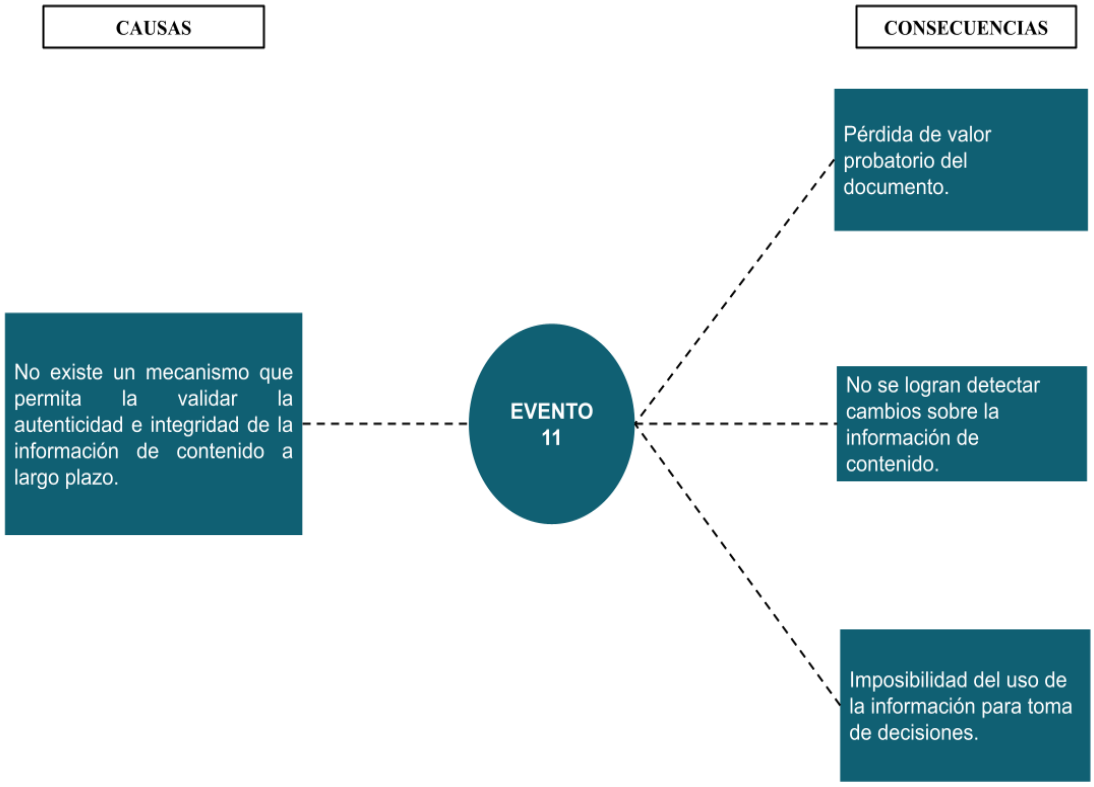
Riesgo 10: Errores humanos que afectan la preservación de la información digital

Descripción del evento: Se evidenció que el proceso de preservación de documentos digitales se está realizando sin ningún tipo de planificación a nivel institucional que permita controlar los procedimientos aplicados sobre los documentos, lo que se puede reflejar en la incurrencia de errores y una gestión ineficiente de los recursos digitales.



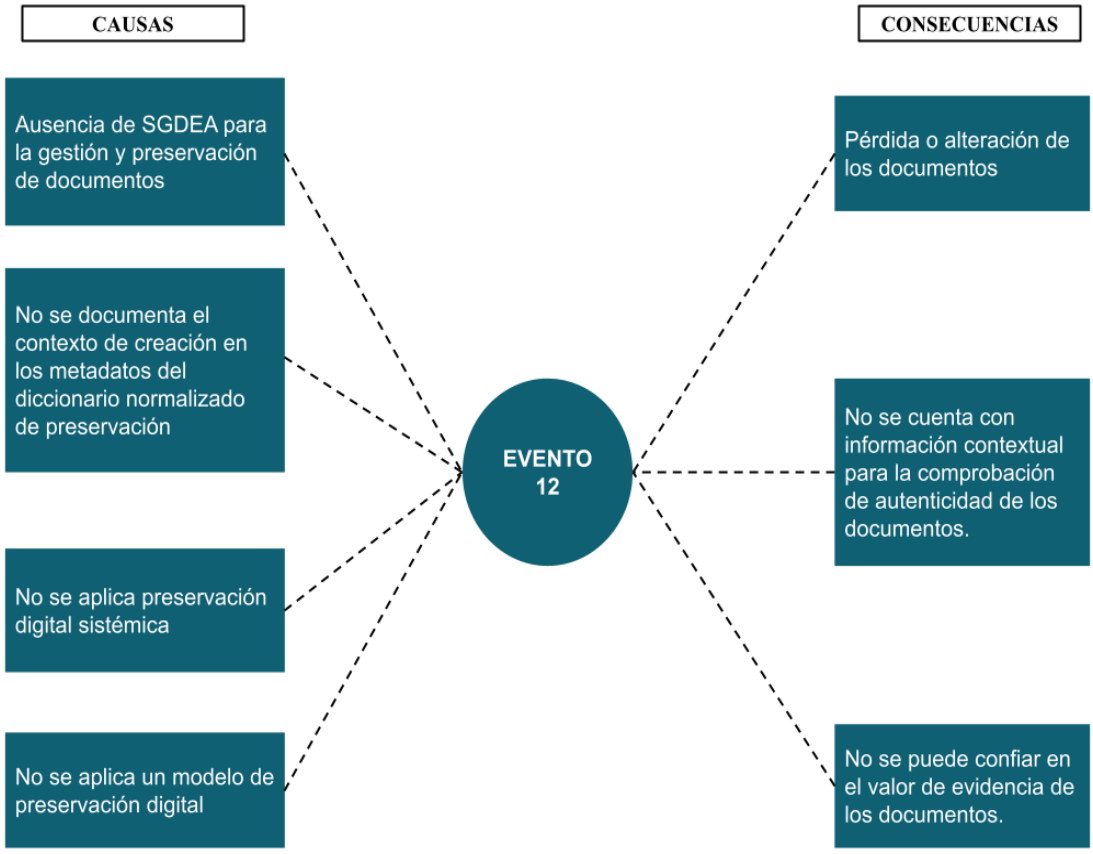
Riesgo 11: Expiración de la criptografía del Paquete de Información Archivística.

Descripción del evento: La criptografía del Paquete de Información Archivística expira por la ausencia de mecanismos para contener la información y ejecutar los procesos de preservación a la información de contenido que permitan a su vez validar la información de autenticidad e integridad.



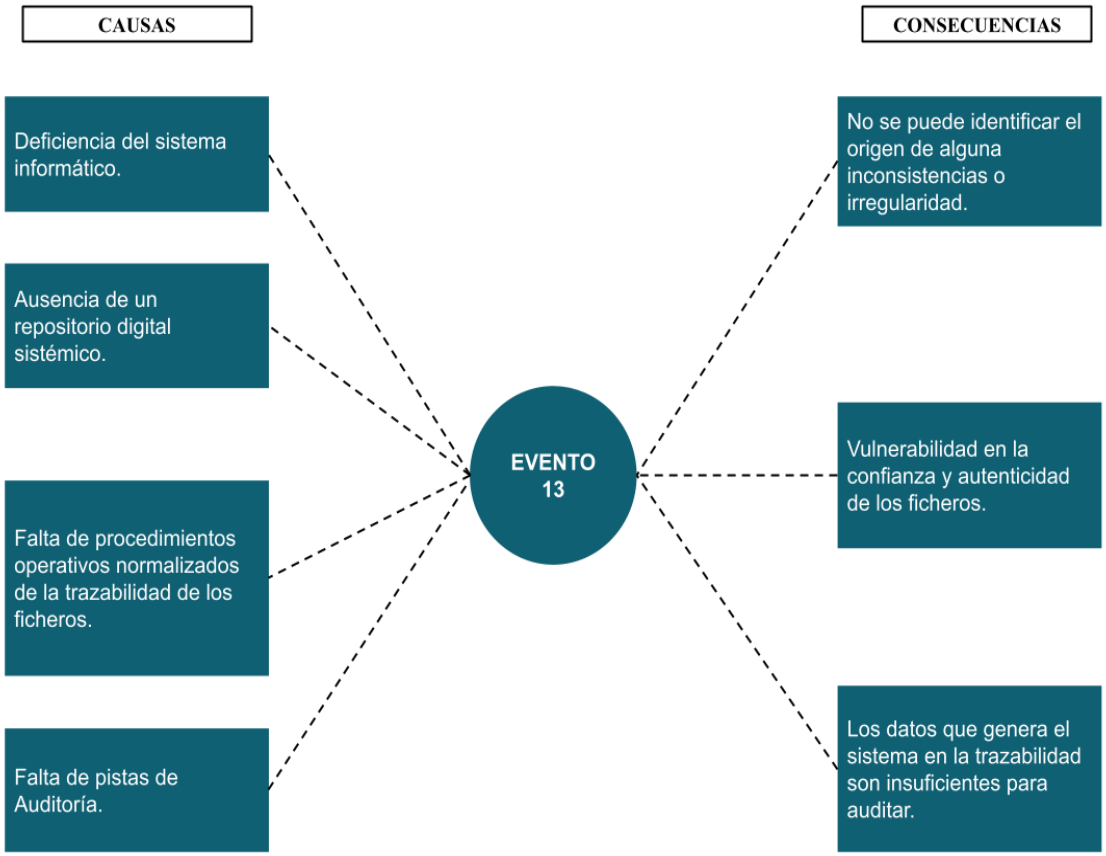
Riesgo 12: Ruptura de la cadena de custodia digital del documento

Descripción del evento: No se realiza una custodia ininterrumpida de los documentos digitales, al carecer de SGDE que apliquen los procesos técnicos archivísticos necesarios para una adecuada gestión del documento, ni con Repositorios Digitales o SGDEA que apliquen un modelo de preservación digital que posibilite la transferencia de los Paquetes de Información Archivística.



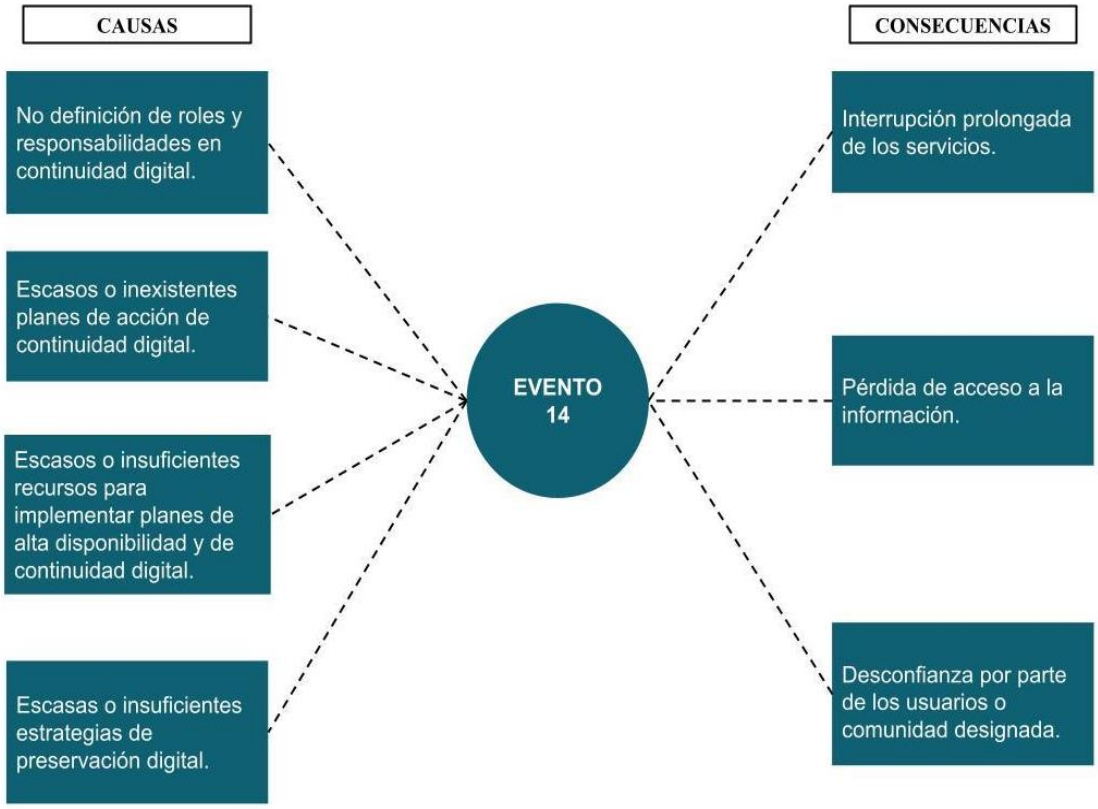
Riesgo 13: Falta de evidencia de registros de trazabilidad

Descripción del evento: El 39.2% de las organizaciones no mantienen los registros de la trazabilidad de todas las acciones realizadas sobre los ficheros, lo que a su vez genera que dichos registros o bitácoras no estén disponibles para futuras inspecciones con el fin de evidenciar cualquier tipo de evento o irregularidad, en cuanto a integridad y autenticidad de la información.



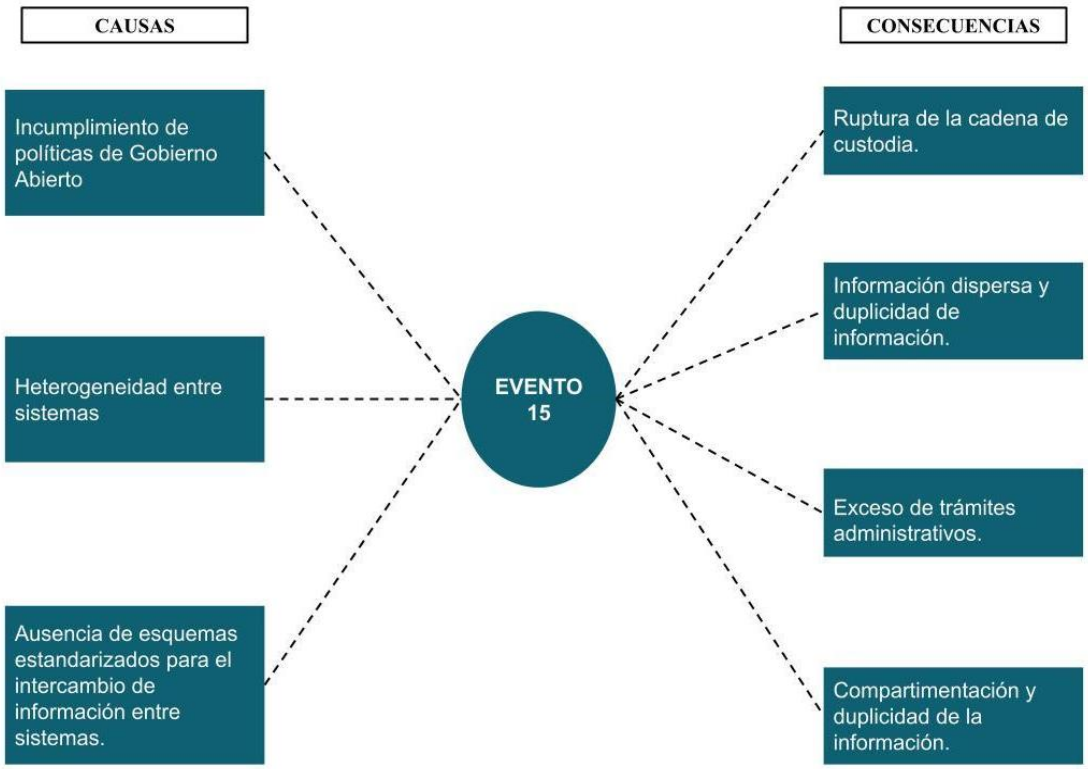
Riesgo 14: Gestión insuficiente de la continuidad digital

Descripción del evento: El 73,1% de las organizaciones carecen de un plan de acción para la continuidad digital; un 67,3% no tienen un marco de referencia para gestionar los riesgos que afectan la continuidad digital, únicamente un 32,7% tiene disponible para la toma de decisiones los informes de evaluación de riesgos para la continuidad digital, y un 67,3% no ha establecido roles ni responsabilidades para la gestión adecuada de la continuidad digital.



Riesgo 15: Ineficiencia en el intercambio y utilización de información entre sistemas.

Descripción del evento: Los sistemas de información utilizados para la producción, la gestión de documentos y la preservación digital son incapaces de comunicarse unos con otros debido a la ausencia de implementación de esquemas estandarizados para el intercambio de información.



3. Análisis del riesgo

Con base en los eventos identificados anteriormente, se realizará un análisis de riesgos, con el fin de obtener un panorama aún más amplio de los mismos, por lo que se estimará su probabilidad de ocurrencia de acuerdo con los datos recuperados del diagnóstico y la magnitud del impacto en caso de que se materialice el riesgo.

En la terminología de gestión del riesgo, de acuerdo con la norma UNE-ISO 31000: 2018, la palabra “probabilidad” se utiliza para indicar la posibilidad de que algo

suceda, teniendo esto en consideración, se establecieron los siguientes niveles y valores para estimar la probabilidad:

Cuadro 13. Niveles de probabilidad

Valor	Nivel de probabilidad	Descripción
1	Improbable	El evento ocurrirá en situaciones excepcionales.
2	Poco probable	El evento ocurrirá en escasas ocasiones.
3	Posible	El evento ocurrirá en algunas ocasiones.
4	Probable	El evento puede ocurrir en la mayoría de los casos.

Fuente: Elaboración propia.

Por otra parte, el impacto se considera como la consecuencia generada por la consumación de un riesgo, de esta manera, las implicaciones que puede acarrear un riesgo tendrán diversos grados de afectación sobre el proceso de preservación, por lo que se establecieron los siguientes niveles de impacto:

Cuadro 14. Niveles de impacto

Valor	**Nivel de impacto**	**Descripción**
1	Insignificante	Los daños no son perceptibles y posiblemente pasen inadvertidos.
2	Leve	Los daños son mínimos, no implican prejuicios.
3	Moderado	Los daños son considerables.
4	Grave	Los daños son adversos, no pueden ser reparados fácilmente, implican pérdidas significantes de información, de autenticidad o de integridad.

Fuente: Elaboración propia.

Por consiguiente, el nivel de riesgo se verá determinado por la relación entre el nivel de probabilidad asignado al riesgo y al nivel de impacto de las consecuencias, de esta manera el valor consignado al nivel de probabilidad será multiplicado por el valor

fijado al nivel de impacto, obteniendo así un valor numérico al nivel de riesgo, tal como refleja en la siguiente figura:

Figura 13. Conformación del nivel de riesgo

Fuente: Elaboración propia.

A su vez, esta información se puede reflejar de mejor forma en un mapa de calor del riesgo, el cual se encuentra constituido a partir de la relación que puede tener el nivel de probabilidad con el nivel de impacto, por lo tanto, se interpreta que entre más alto sea el resultado de la multiplicación de los valores de probabilidad e impacto, mayor será su nivel de criticidad.

Figura 14. Mapa de calor del riesgo

PROBABILIDAD	**Probable**	**4**	**8**	**12**	**16**
	Posible	**3**	**6**	**9**	**12**
	Poco Probable	**2**	**4**	**6**	**8**
	Improbable	**1**	**2**	**3**	**4**
		Insignificante	**Leve**	**Moderado**	**Grave**
	IMPACTO				

Fuente: Elaboración propia.

4. Valoración del riesgo

Una vez identificados los riesgos a los cuales se encuentran actualmente expuestas las instituciones encuestadas del SNA en materia de preservación de documentos digitales, se procederá a su ponderación, teniendo en consideración la relación entre la probabilidad de ocurrencia y el impacto reflejada en el mapa de calor del riesgo, de esta manera se fijaron los niveles de criticidad de los riesgos, como se muestra en el siguiente cuadro:

Cuadro 15. Niveles de criticidad de los riesgos

NR	Criticidad del riesgo	Descripción
0-2	Aceptable	El riesgo se encuentra en un nivel que puede ser aceptado sin necesidad de tomar medidas, teniendo un nulo efecto en la organización.
3-6	Moderado	El riesgo se encuentra en un nivel tolerable, puede ser corregido en el corto plazo tomando medidas adicionales para abordar los riesgos.
8-10	Alto	Debe establecerse de manera inmediata un plan de tratamiento a los riesgos para llevarlos a un nivel aceptable.
12-16	Crítico	Se debe dar tratamiento inmediato a las causas que generan el riesgo estableciendo un plan de tratamiento y gestión de riesgos, así como las medidas para fortalecer los procesos y controles existentes de modo que se verifique el control de la probabilidad y el impacto en el tiempo; la materialización del riesgo causaría afectaciones y pérdidas importantes.

Fuente: Elaboración propia.

Por lo tanto, a cada uno de los riesgos identificados y analizados anteriormente, se le asignó un nivel de impacto y de probabilidad, obteniendo de esta manera el grado de criticidad, como se logra observar en el cuadro 16, los riesgos encontrados fueron considerados como críticos o de un nivel alto, lo cual demuestra que los procedimientos seguidos actualmente no brindan un contexto seguro para los objetos digitales que permita garantizar su valor probatorio y su acceso a largo plazo.

Cuadro 16. Valoración de los riesgos y mitigación

Cod.	Probabilidad	Impacto	Nivel de riesgo	Criticidad del riesgo	Mitigación
R01	4	4	16	Crítico	Archivo Digital basado en un modelo de preservación digital.
R02	3	4	12	Crítico	Protocolos de acceso. Plan de Tecnologías de la Información actualizado y contextualizado. Sello de seguridad sobre el dominio web. Almacenamiento en Paquetes de Información Archivística protegidos por el sello electrónico.
R03	3	3	9	Alto	Aplicar un esquema de metadatos normalizado. Utilizar espacios de nombres normalizados para los esquemas de metadatos. Aplicarnormasdescripción archivística.
R04	3	4	12	Crítico	Aplicar mecanismos de monitoreo de autenticidad del documento. Disponer de sistemas automáticos desasistidos de custodia de preservación para los documentos. Almacenamiento en Paquetes de Información Archivística protegidos por el sello electrónico.

Cod.	Probabilidad	Impacto	Nivel de riesgo	Criticidad del riesgo	Mitigación
R05	3	3	9	Alto	Asegurar el perímetro. Asegurar las redes y comunicaciones. Asegurar los anfitriones de servicio (servidores de aplicación). Aislamiento y aseguramiento lógico de la capa de almacenamiento. Aseguramiento del objeto de custodia (AIP). Servicios anti-malware.
R06	2	4	8	Alto	Utilización de métodos de autenticación segura y de fuentes confiables. Implementar control de acceso.
R07	3	4	12	Crítico	Implementar un plan de revisión periódica de formatos utilizados. Optar por el uso de formatos estándares y abiertos. Aplicar transformación sistémica y automática de los formatos de fichero en función de la política emanada por el órgano rector, sin intervención humana.
R08	4	4	16	Crítico	Monitoreos y actualizaciones periódicas al software. El sistema de preservación debe tener un plan de actualización

Cod.	Probabilidad	Impacto	Nivel de riesgo	Criticidad del riesgo	Mitigación
					permanente.
R09	4	4	16	Crítico	Análisis de la oferta tecnológica y aplicación de actualización en tendencias de uso masivo.
R10	3	3	9	Alto	Planificar el proceso de preservación de documentos digitales. Establecer procedimientos para la preservación de documentos digitales. Limitar a la mínima expresión la necesidad de la operación humana en la cadena de custodia.
R11	4	4	16	Crítico	Implementar el uso del resello mediante firma digital de persona jurídica en los Paquetes de Información Archivística (AIP).
R12	4	4	16	Crítico	Implementar un modelo de preservación sistémica ininterrumpida. Mantener la información del contexto de creación de los objetos digitales. Archivo Digital basado en un modelo de preservación digital. Realizar la ingesta de los objetos digitales en los sistemas de preservación tan pronto como sea posible después de ser producidos. Utilizar un único repositorio digital para

Cod.	Probabilidad	Impacto	Nivel de riesgo	Criticidad del riesgo	Mitigación
					toda la organización.
R13	3	3	9	Alto	Implementar procedimientos de registros de trazabilidad registrando la información como metadatos de preservación dentro de los Paquetes de Información Archivística.
R14	3	3	9	Alto	Establecer un plan de acción de continuidad digital y alta disponibilidad de los servicios. Uso de sitio alterno para copias de seguridad y alta disponibilidad de los servicios Establecer roles y responsabilidades para gestionar la continuidad digital. Establecer una política de preservación digital.
R15	4	3	12	Alto	Establecer protocolos para el intercambio de información. Aplicar esquemas estandarizados que permitan la comunicación fluida entre sistemas. Implementar protocolos de integración e importación de datos de tipo abierto o no propietarios.

Fuente: Elaboración propia.

El cuadro anterior refleja los riesgos más comunes y generales que se lograron identificar en las organizaciones encuestadas del Sistema Nacional de Archivos, como se puede evidenciar, en su mayoría son riesgos con un alto nivel de criticidad lo que implica que, de llegar a efectuarse el evento, las consecuencias serían lamentables.

Por su parte, la valoración de riesgos evidencia que la información digital se encuentra en peligro y con ella su capacidad para servir como prueba y testimonio de su contenido a mediano y largo plazo, esto se debe principalmente a que institucionalmente no se están realizando la acciones correspondientes para reducir la posibilidad de que eventos adversos a los objetivos de la preservación digital se concreten, por ello además de enlistar y valorar los riesgos se propone una serie de mitigaciones de alcance general que se pueden aplicar a cada uno de los riesgos identificados.

5. Conclusiones de la evaluación de riesgos asociados

Según la evaluación de riesgos asociados a la preservación digital, se logra evidenciar que las organizaciones encuestadas no son conscientes de los riesgos a los que se encuentra expuesta la información digital que custodian, por lo que en su mayoría no han establecido roles y responsabilidades para la gestión de riesgos, no cuentan con marcos de referencia ni informes de evaluación que les permita tomar decisiones, priorizar, eliminar, reducir o controlar los riesgos que acechan a la información digital y su continuidad.

El diagrama de identificación de riesgos utilizado refleja de manera gráfica las principales causas que desencadenan los riesgos identificados, así como las consecuencias que enfrentaría la información y la continuidad digital, si estos riesgos llegaran a efectuarse, por su parte, en la valoración de riesgos se logra identificar que en su mayoría son riesgos con una alta criticidad lo que se traduce en consecuencias catastróficas, para las organizaciones, los ciudadanos, para el patrimonio documental y para el Estado Social de Derecho.

Finalmente, queda en evidencia que aplicar una evaluación de riesgos asociada la preservación y continuidad de la información, de manera cíclica y oportuna proporciona a las organizaciones información necesaria para decidir la necesidad de tomar medidas adecuadas para identificar, priorizar, reducir, eliminar y/o mitigar los riesgos a los que se enfrenta la información digital evitando consecuencias irreparables en el mediano o largo plazo.

CAPÍTULO V.
MARCO DE EVALUACIÓN PARA SOLUCIONES DE PRESERVACIÓN DE DOCUMENTOS DIGITALES EN COSTA RICA

CAPÍTULO V. MARCO DE EVALUACIÓN

El objetivo del presente capítulo es proporcionar un marco de evaluación para soluciones de preservación digital mediante la elaboración de un instrumento denominado Herramienta de Evaluación Integral (HEI). Su elaboración es el resultado de la investigación basada en normas de buenas prácticas como la UNE-ISO 15489, la familia de normas UNE-ISO 30300, la UNE-ISO 16363, UNE-ISO 14721, estándares, bibliografía relacionada con el tema y la normativa nacional que regula e interviene la preservación digital de la información.

Cabe mencionar que el marco de evaluación utiliza términos y vocabulario tanto de la Archivística, como del área de Tecnologías de Información y Comunicación, por lo que es importante que las organizaciones que deseen utilizar el marco de evaluación propuesto dispongan de equipos interdisciplinarios, que aporten sus conocimientos desde las diversas áreas para un mayor aprovechamiento. Además, para una mejor y mayor comprensión se elaboró un glosario de términos disponible en el Anexo 1.

El marco de evaluación para soluciones de preservación digital se estructura en 3 apartados generales, a saber:

- Requisitos Previos: compuesto por una serie de elementos necesarios para la preservación digital que deben ser aplicados por las organizaciones previamente a la adquisición o desarrollo de una solución de preservación de documentos digitales, contemplando la viabilidad organizacional, la gestión de documentos, las políticas y estrategias de preservación, la seguridad de la información y la continuidad del negocio.
- Modelo Funcional: utiliza como referencia el modelo OAIS, se encuentra constituido por seis servicios o entidades funcionales, entre ellas la ingesta, el almacenamiento, la gestión de datos, la administración, la planificación de la preservación y el acceso; y serán parte de la HEI.
- Modelo Tecnológico: se basa en el establecimiento de criterios tecnológicos básicos con los que debe cumplir una solución de preservación digital,

tomando en cuenta aspectos como la arquitectura tecnológica, la infraestructura tecnológica, la interoperabilidad y la neutralidad tecnológica; y serán parte de la HEI.

1. Requisitos previos

La preservación es un conjunto de elementos que se entrelazan para alcanzar un objetivo principal, que en el caso de la archivística es la preservación de la información a lo largo del tiempo. La preservación, por lo tanto, es un conjunto de "principios, políticas, reglas y estrategias destinadas a prolongar la existencia de un objeto manteniéndolo en una condición adecuada para su uso, ya sea en su formato original o en otro más persistente, dejando intacta la forma intelectual del objeto" (Bernard y Voutssas, 2014, p. 173).

En el caso de los objetos digitales, la preservación digital es un proceso específico para mantener dichos materiales digitales a través de las diferentes generaciones de tecnologías a lo largo del tiempo, con independencia de los soportes donde residan.

Además, es importante señalar que preservación digital no es, de acuerdo con la Coalición de Preservación Digital (DPC, por su siglas en inglés) solucionar un problema técnico del soporte digital, sino que conlleva solucionar problemas organizativos y de recursos financieros y humanos, asimismo la preservación digital no es solamente almacenar los objetos digitales en servidores propios de la organización o en la adquisición de servicios de almacenamiento como la nube, ya que la preservación digital abarca una amplia gama de actividades que deben emprenderse de manera proactiva y en conjunto con otros procesos.

La DPC también señala que preservación no es la adquisición solamente de una solución o un sistema de repositorio digital, aunque es un elemento esencial, es también importante que, en conjunto con una solución, haya buenas prácticas, procesos de mejora continua y la capacidad de responder a los cambios de la tecnología y las necesidades de los usuarios.

El principal reto que enfrenta el profesional en archivística y las organizaciones sobre el documento electrónico es la obsolescencia tecnológica, por lo tanto, la preservación digital se debe entender como el conjunto de principios, políticas, normas y estrategias diseñadas para asegurar que un objeto digital permanezca accesible, inteligible y usable a través del tiempo y de los cambios tecnológicos, y que su fiabilidad y exactitud estén protegidos y que su autenticidad sea verificable.

Para ello es importante que las organizaciones que gestionen y custodien documentos electrónicos consideren, como parte de la preservación digital, el concepto de cadena de preservación, el cual busca una secuencia de controles que se extienden sobre todos los procesos de gestión para asegurar su fiabilidad a lo largo del tiempo, para eso es fundamental realizar una identificación de requisitos administrativos, legales, técnicos y tecnológicos de los documentos electrónicos desde la creación del documento hasta su disposición final. La preservación digital debe estar integrada en todos los procesos de gestiones documentales y orientadas a los objetivos de la organización.

Como se indicó anteriormente, la preservación no solamente se va a solucionar por medio de un sistema o repositorio digital, para ello es necesario la integración de otros procesos organizativos e inclusive requisitos previos que la organización debe implementar y que una adquisición o desarrollo de solución de preservación digital debe ejecutar, por lo que es relevante que las organizaciones cumplan con una fase de aprendizaje y de culturización institucional, por medio del cual se tome conciencia sobre el impacto que trae consigo una adecuada preservación de la información digital.

Por esta razón, se identificaron una serie de elementos necesarios para la preservación digital que deben ser aplicados por las organizaciones previamente a la adquisición o desarrollo de una solución de preservación de documentos digitales, los mismos se dividieron en:

1.1 Viabilidad organizacional

Se debe identificar la capacidad de injerencia de los altos jerarcas en materia de la gestión documental, así como el recurso humano y económico, necesario para los procesos de preservación digital.

Es indispensable tener bien definida la estructura organizacional, para eso es importante la identificación y establecimiento de las responsabilidades necesarias para llevar a cabo la preservación digital, así como tener personal designado con adecuadas habilidades y experiencia para cumplir dichas funciones. También, la organización debe facilitar que el personal designado en materia de preservación digital tenga la posibilidad de capacitarse continuamente.

La asignación de roles, competencias y responsabilidades en el proceso de preservación debe encontrarse debidamente documentada y articulada mediante la aplicación de reglas organizacionales y prácticas normalizadas, lo anterior, le facilitará a la organización proporcionar una serie de directrices dirigidas al establecimiento de programas de comunicación, concientización y formación continua del personal que interviene en el proceso, ya sea por medio de la toma de decisiones o por medio de la ejecución de procesos técnicos.

1.2 Gestión de documentos

Dentro del concepto de cadena de preservación, además de que se busca una secuencia de controles sobre todo el proceso de gestión de los documentos de archivo, también este modelo considera un sistema de administración de documentos de archivo, conformado por un conjunto de sistemas, entre ellos, los Sistemas de Producción Documental que normalizan la producción de los documentos, el Sistema de Gestión de Documentos Electrónicos que aplique los procesos técnicos archivísticos y un Sistema de Preservación, en donde todos estos sistemas se deben ejecutar de acuerdo con normas de buenas prácticas.

El impacto de una adecuada aplicación de estos procesos para garantizar la preservación digital, radica principalmente en una producción de documentos

íntegros, fiables y auténticos, que se incorporen posteriormente al Archivo Digital, lo cual se logra, en gran medida, gracias a una fase preliminar denominada como identificación, por medio de la cual se logra conocer de manera exhaustiva y detallada al productor de los documentos, comprendiendo su naturaleza administrativa, sus funciones, sus relaciones y el por qué se generan los documentos, permitiendo el establecimiento de diversos instrumentos necesarios para la gestión de documentos.

En consecuencia, la organización debe disponer de una serie de instrumentos archivísticos necesarios para el control, organización y ordenación de los documentos, tal como un Cuadro de Clasificación donde se identifique todas las series documentales, y que además responda a un sistema de clasificación que permanezca estable ante los cambios administrativos y funcionales que puede sufrir una institución. Aunado a lo anterior, también se deben tener aprobadas por el CISED las Tablas de Plazos de Conservación de documentos, en el caso de las instituciones que conformen el Sistema Nacional de Archivos o por los altos jerarcas, en el caso de las organizaciones que no formen parte del SNA.

Finalmente, se deben tener las Tablas de Acceso (a nivel de serie documental, expediente y unidad documental), la identificación de los roles y permisos, un Plan de Seguridad y un esquema de metadatos diseñado para la preservación de la información. Para esta investigación se realizó un esquema de metadatos tomando en cuenta las normas internacionales de descripción (Anexo N.º 2).

1.3 Políticas y estrategias de preservación digital

El desarrollo de una política y estrategias de preservación es fundamental a la hora de implementar un proceso o proyecto de preservación digital, por ello la organización debe tener una Política de Preservación Digital, que disponga de una serie de reglas y principios que sean la guía para la toma de decisiones, así como las acciones para lograr los objetivos deseados para su fin.

Es necesario que la política sea aprobada por un alto nivel dentro de la organización y que no establezca acciones en particular, ya que eso le corresponde a otros

instrumentos administrativos como los manuales de procedimientos. De acuerdo con el proyecto de InterPARES, la política no debe ser prescriptiva y debe ser tecnológicamente neutral.

En el caso de las estrategias de preservación digital, se debe disponer un Plan Estratégico de Preservación, el cual debe ser aprobado por el administrador del Archivo Digital y debe indicar los métodos para proteger y conservar los objetos digitales y toda la información relativa al documento de archivo, así como definir y parametrizar reglas de transformación de formatos (conversión).

Los Planes Estratégicos de Preservación pueden estar diseñados para ser ejecutados tanto a largo como a corto plazo, esto dependerá de la situación actual de la organización en relación a los objetivos que se pretenden alcanzar en materia de preservación, por tanto, resulta de utilidad la realización de un diagnóstico o estudio previo que refleje las necesidades y riesgos que aquejan a la organización, de tal forma que un Plan Estratégico debe servir como guía para lograr las metas planteadas en un determinado período de tiempo.

Por consiguiente, la Política de Preservación debe ser consistente con el Plan Estratégico de Preservación. Para abordar más sobre el tema de la política y estrategias de preservación se puede consultar el Módulo 1 y 2 de la serie de temas fundamentales de preservación digital del ICA/InterPARES.

Si la organización ya ha desarrollado y aplicado los requisitos previos, es importante, como método de mejora continua, identificar la capacidad o nivel de los procesos de preservación. Para ello, existen instrumentos o herramientas básicas que permiten, de manera general, evaluar las capacidades de preservación digital y dar un seguimiento a los diferentes procesos implementados en materia de preservación.

1.4 Contratos y licencias

En el caso de contratar y adquirir una solución de preservación digital es necesario revisar con detalle el contrato, con el fin de que no se omita algún requisito o

información que a futuro pueda perjudicar alguna de las partes, para ello es necesario tener profesionales cualificados en la materia.

Aspectos importantes que tomar en cuenta a la hora de revisar los contratos, es identificar el tipo de licencia y verificar las limitaciones, así como el alcance y propiedad de la licencia que se va a adquirir.

También se debe revisar que se contemplen acuerdos de depósito que especifiquen todos los derechos de conservación, transferencias, mantenimiento, acceso y especificaciones sobre cómo se almacenan los AIP, y en caso de que la organización no disponga de recursos para continuar con el pago de las licencias es necesario contemplar y definir quién tiene la propiedad de las bases de datos y de lo que almacenan. Además, si están o no contempladas las migraciones de los objetos digitales y sus metadatos.

Para evitar y mitigar riesgos sobre la pérdida o acceso indebido a la información, es necesario que en el contrato se definan las responsabilidades entre el cliente y el prestador de servicios en el momento de cualquier disputa en caso de alteraciones, falsificaciones, pérdidas y fugas de información, entre otros aspectos que la organización crea necesario.

Por último, otro aspecto fundamental para contemplar en un contrato es estipular el tiempo de la implementación de las licencias a partir de la adquisición y compra de la solución de preservación digital. Además, se debe contemplar el marco normativo referente a la contratación administrativa que regula al país.

1.5 Seguridad de la información

La seguridad de la información es un aspecto que se debe considerar para el funcionamiento adecuado de un Archivo Digital, pues se encuentra estrechamente relacionado con la integridad, confidencialidad y disponibilidad de la información, por consiguiente, pretende garantizar que los activos de información se mantengan sin alteraciones y precisos, ocultos a quienes no cuenten con los permisos para utilizarlos y que sean fácilmente accesibles para quienes deban tener esa información.

Para ello a nivel organizacional se deben considerar y aplicar una serie de medidas que minimicen el riesgo de pérdida de información, en primera instancia, disponer de los procedimientos para la verificación periódica de vulnerabilidades, de esta manera se pueden identificar el nivel de exposición a posibles ataques, entender los riesgos que enfrentan los sistemas y posteriormente tomar medidas para reducir esos riesgos y supervisarlos.

En cuanto a la ciberseguridad, la organización debe velar por el desarrollo de su infraestructura tecnológica, implementando procedimientos para la actualización periódica de firmware, controladores (drivers) y parches del sistema operativo, aplicaciones y dispositivos, asimismo, como disponer de listas de software permitidos para la instalación y uso, la cual debe ser actualizada de manera periódica.

La autenticación es otro aspecto para considerar, pues por medio de ella se verifica que las personas que ingresan a la solución sean realmente quienes dicen ser, resulta especialmente relevante para proteger aquella información sensible que contiene información de carácter privado, de modo que las organizaciones deben generar y gestionar protocolos de autenticación de usuarios que sean seguros, pero que a su vez no sean excluyentes.

Existen diversos mecanismos para verificar la identidad de un individuo, el más conocido es el nombre usuario ligado a una contraseña, no obstante, este procedimiento debe ir acompañado de la capacitación de los usuarios para propiciar que se generen contraseñas seguras, de igual manera, se puede hacer uso de certificados digitales, como la firma digital, o bien la identificación biométrica.

A nivel físico, en caso de disponer de una infraestructura propia, se deben establecer un conjunto de políticas y procedimientos que proteja el centro de datos, esto permite proporcionar las mejores condiciones para la operación de los equipos que hospedan los servicios de la solución, para cumplir con este objetivo se pueden consultar diversos estándares que proporcionan los requisitos mínimos necesarios, como por ejemplo el estándar ANSI/TIA-942 *TelecommunicationsInfrastructure Standard for Data Centers* y las normas ISO 27000 *Information Security Management System*.

1.6 Continuidad del negocio

Otro aspecto importante que las organizaciones deben tenerpresente, como parte de los requisitos previos a la hora de adquirir una solución de preservación digital, es prevenir y anticiparse ante los desastres o eventos que se puedan presentar. Para mantener las operaciones y servicios es necesario la adopción de un plan de continuidad del negocio, con el fin de mitigar los riesgos y así poder recuperarse cuando ocurren eventos como los desastres naturales o incidentes de seguridad de la información como se mencionó en el punto anterior.

Los procesos que se deben contemplar para un plan de continuidad del negocio ya están normalizados y se pueden implementar utilizando la norma internacional UNE-EN ISO 22301: 2020 Sistema de Gestión de la Continuidad de Negocio. En el caso de la solución de preservación digital, se pueden presentar diversos desastres, para ello los análisis de riesgos son necesarios para mitigar cada uno de los eventos identificados y así continuar brindando el servicio.

También es necesario disponer de planes de continuidad, como el financiero en donde se demuestre la capacidad de obtener recursos y la planificación empresarial a corto y largo plazo, que permita la sostenibilidad de la solución de preservación en el tiempo, aplicar auditorías para garantizar la transparencia en los procesos de obtención de recursos económicos y la asignación de forma anual de los recursos necesarios para la aplicación de las estrategias de preservación digital.

Por último, es necesario que la organización supervise su entorno para determinar cuándo ejecutar su plan de sucesión, los planes de contingencia y/o acuerdos de garantía, así como estar comprometido con un programa regular de autoevaluación y de manera recomendable, con un programa de certificación externa.

2. Modelo Funcional

El marco de evaluación propuesto pretende brindar una serie de requisitos funcionales que sirvan como apoyo a las organizaciones, ya sean públicas o privadas,

al momento de tomar decisiones para la elección de una solución de preservación de documentos digitales.

Una herramienta cuyo fin primordial es salvaguardar la información contenida en los documentos digitales fidedignos, mediante la ejecución de procesos relacionados con envolver la información, realizar la conversión de formatos de ficheros, las verificaciones de integridad y autenticidad, la gestión de derechos y permisos de acceso y la captura de metadatos.

Para ello, se analizó lo propuesto por el modelo OAIS, pues es una iniciativa orientada a alcanzar una preservación sistémica y el respeto de la cadena de custodia de los documentos digitales, resulta viable considerar un entorno en donde el Archivo Digital tiene relación con diversos actores a los cuales se le conocerán como productor, administrador y comunidad designada o usuarios, quienes a su vez se pueden relacionar en su idea más básica de la siguiente manera:

Figura 15. Ambiente en el modelo OAIS

Fuente: Elaboración propia a partir de lo establecido en la norma UNE-ISO 14721:2015: Sistemas de transferencia de datos e información espaciales. Sistema abierto de información de archivo (OAIS).

De esta forma, cada uno de los actores cumple una función específica, de modo que, el productor proporcionará la información a conservar, la administración establecerá las políticas generales del Archivo Digital para la aplicación de procesos de preservación, mientras que la comunidad designada consulta y accede al material

digital conservado. Resulta conveniente aclarar que el productor puede ser a su vez la comunidad designada y que el Archivo Digital también puede fungir el papel de productor con otros archivos digitales, por lo cual dependerá del contexto organizacional la función o las funciones que cumplan dentro del ecosistema.

El modelo OAIS se basa en el concepto de Paquetes de Información, los cuales funcionan como un contenedor lógico ideado para la ingesta, almacenamiento y difusión de la información en el Archivo Digital, un paquete consta de un objeto digital junto con los metadatos necesarios para garantizar su preservación.

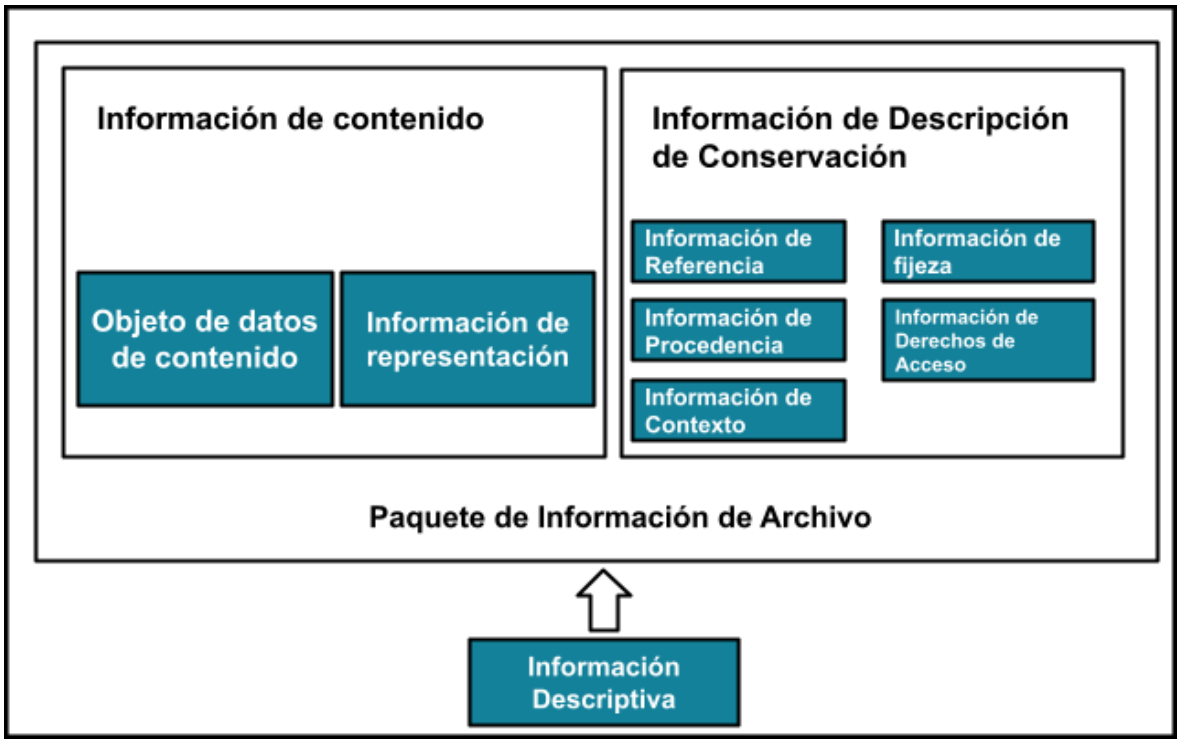
Existen tres variantes para un Paquete de Información dependiendo de la funcionalidad que este vaya a cumplir, en consecuencia, se puede tratar de un:

- **Paquete de Información de Envío o SIP:** es la versión que transfiere el productor y se encuentra conformado de acuerdo con el protocolo de transferencia acordado entre el Archivo Digital y el productor, puede ser entregado de dos formas diferentes, ya sea bajo el método push o pull, que serán explicados más adelante como parte del protocolo de transferencia propuesto en el Anexo 3.
- **Paquetes de Información de Archivo o AIP:** una vez que el SIP pase el control de calidad, estará listo para convertirse en la versión que se almacenará en el Archivo Digital, se puede establecer que la figura del AIP constituye una pieza clave, pues además de contener la información también es la vía para la aplicación de mecanismos necesarios en el proceso de preservación. Esto se debe a la composición del AIP en donde se encuentran cuatro tipos de información:
    - Información de empaquetado: usada para agrupar e identificar los componentes de un paquete de información.
    - Información descriptiva: permite la búsqueda y recuperación de los paquetes de información.
    - Información de contenido: almacena al objeto digital, por consiguiente, también se encuentra la información de representación, así como la cadena de bits que lo conforma.

- Información de descripción de conservación: proporciona los metadatos necesarios para llevar a cabo las funciones de preservación, puesto que puede contener la información que identifica la información de contenido (información de referencia), la información que documenta la cadena de custodia del documento (información de procedencia), la información que describe las relaciones del objeto digital con otros objetos (información contextual), la información sobre las validaciones de integridad de la información de contenido (información de fijeza) y la información de restricciones de acceso (información de derechos de acceso).

Como se logra notar, la conformación de un AIP es compleja y abarca una gran cantidad de elementos, sin embargo, a través de la figura 16 se alcanza a visualizar de mejor manera las relaciones y agrupaciones anteriormente descritas.

Figura 16. Conformación de un Paquete de Información de Archivo



Fuente: Digital Preservation Coalition. (2014). The Open Archival Information System (OAIS) Reference Model: Introductory Guide. 2° edición.

- **Paquete de Información de Consulta o DIP:** versión derivada del AIP que se entrega a los usuarios en respuesta a una solicitud de acceso, puede variar en forma o contenido al AIP para que pueda ser consultado fácilmente por los usuarios.

Al profundizar en los mecanismos utilizados por el modelo de referencia para asegurar la preservación a largo plazo de los Paquetes de Información, se encuentra el modelo funcional, constituido por seis servicios conocidos como entidades funcionales, entre los que se encuentran: la ingesta, el almacenamiento, la gestión de datos, la administración, la planificación de la preservación y el acceso.

No obstante, resulta relevante recordar que el proceso de evaluación de una solución de preservación de documentos también cubre aspectos organizativos y tecnológicos, por lo que algunas de las consideraciones propuestas se tomaron en cuenta como parte de los requisitos previos, ya que forman parte del proceso intelectual que se debe realizar de manera anticipada. En consecuencia, los requisitos funcionales se estructuraron de la siguiente manera:

- **Ingesta:** toma en consideración los procedimientos necesarios para la preparación del SIP para que este pueda ser transferido al almacenamiento permanente, de esta manera se asegura que la información sea trasladada en apego a los protocolos establecidos y que sean enviados de forma completa y sin alteraciones.
- **Generación del AIP:** se encuentra conformado por los requisitos necesarios para la aplicación del proceso de control de calidad de los SIP recibidos, además, de la incorporación de metadatos necesarios para la preservación del AIP y la conversión de los formatos de fichero en caso de ser necesario.
- **Almacenamiento de archivo:** abarca los servicios para que el contenido archivado permanezca completo y pueda ser accesible a largo plazo, para ello ejecuta procesos como la verificación de errores en la cadena de bits, la inclusión de metadatos que documenten los eventos de preservación, verificaciones de integridad y conversiones de formatos de fichero.

- **Gestión de datos:** se consignaron los requisitos relacionados con la gestión del sistema de base de datos, además, de la respectiva resolución de solicitudes de información provenientes de acceso para la transformación de un AIP a un DIP, o bien de la entidad administración para informar sobre el estado de los AIP en la entidad de almacenamiento.
- **Acceso:** coordina la entrega de información a los usuarios de la comunidad designada, por medio de la transformación de un AIP a un DIP que se adapta a sus necesidades y permisos de acceso brindados.
- **Seguridad**: integra la aplicación de mecanismos de autenticación de usuarios, el uso de llaves criptográficas y elementos relacionados con ciberseguridad.

De esta manera, el modelo OAIS proporciona un marco sistemático que busca garantizar la preservación y acceso de los materiales digitales, por medio de la ingesta, almacenamiento y difusión de Paquetes de Información, quienes, a su vez, posibilitan el uso de metadatos para documentar las relaciones del objeto digital con su contexto organizacional, los cambios en su custodia y los eventos ligados con su preservación.

Cada una de las categorías o apartados mencionados anteriormente, se subdividen, a su vez, en una serie de requisitos que serán la base y el principal insumo para realizar la evaluación. Los requisitos poseen una descripción asociada para una mejor comprensión de estos; tanto los criterios de evaluación como su descripción se detallan en el cuadro 17: Herramienta de Evaluación Integral.

3. Modelo Tecnológico (plataforma tecnológica)

El modelo tecnológico es el tercer y último apartado del marco de evaluación para soluciones de preservación digital, este marco además de basarse principalmente en el Modelo de Referencia OAIS, también toma en cuenta aspectos básicos del área de Tecnología de Información, por lo que para desarrollar los requisitos tecnológicos para evaluación se tomó como principal referencia el Código Nacional de Tecnologías Digitales, además de estándares, normas y demás bibliografía relacionada con la materia.

En este apartado se establecen los requisitos tecnológicos mínimos deseables que deben ser tomados en cuenta por una organización antes de adquirir o desarrollar una solución de preservación digital, con la finalidad que las Tecnologías de la Información y la Comunicación logren dar el mayor sustento, seguridad, funcionalidad y robustez al funcionamiento de las entidades funcionales mencionadas anteriormente.

Para desarrollar los requisitos del modelo tecnológico se contemplaron las siguientes categorías:

- **Arquitectura tecnológica:** la arquitectura tecnológica tiene que ver con el comportamiento y la relación existente entre el hardware, el software, los datos, las redes, que interactúan en el proceso de preservación digital, por lo que en esta categoría se evalúan aspectos como el sistemade gestión de base de datos, la escalabilidad, la distribución de cargas, entre otros.
- **Infraestructura tecnológica:** este apartado reúne los requisitos necesarios para evaluar la forma en que se gestiona un conjunto de elementos como el hardware, software u otros servicios necesarios para garantizar y optimizar el proceso de preservación digital.
- **Seguridad tecnológica:** los requisitos que componen el presente apartado buscan identificar la necesidad de las soluciones de preservación digital con respecto a los mecanismos y controles suficientes para evitar, prevenir, y mitigar amenazas, ataques o errores a los que se enfrenta y expone la información digital.
- **Interoperabilidad:** la categoría de interoperabilidad tiene como objetivo evaluar que las herramientas que van a ser valoradas implementan protocolos de datos abiertos o no propietarios y que además se puedan integrar, interactuar, conectar y funcionar con los sistemas necesarios para llevar a cabo el proceso de preservación digital.
- **Neutralidad tecnológica:** el apartado de neutralidad tecnológica tiene como objetivo evaluar los aspectos referentes a la no dependencia tecnológica, es decir que ni el proveedor del servicio ni el potencial usuario dependa de una tecnología (hardware o software) específica para acceder o para poner a

disposición la información digital de una manera segura, íntegra, auténtica y accesible a lo largo del tiempo.

4. Herramienta de Evaluación Integral (HEI)

Actualmente, en el mercado existen muchas opciones que pueden servir para el almacenamiento de datos, sin embargo, no todas consideran los requisitos funcionales y tecnológicos necesarios para que los objetos digitales sean preservados a largo plazo y que a su vez se mantengan íntegros, auténticos y accesibles.

HEI tiene como objetivo proporcionar una guía para realizar evaluaciones informadas, objetivas y equitativas para la adquisición de soluciones de preservación digital. Está diseñada principalmente para instituciones públicas y empresas privadas que hayan pasado por un proceso de autorreflexión sobre la madurez de la preservación digital en su organización.

Facilitará la evaluación mediante una serie de requisitos funcionales y tecnológicos con una descripción detallada y un nivel de cumplimiento por medio de una hoja de verificación (Excel), con una puntuación que devuelve un resultado como insumo para la toma de decisiones por medio de datos cuantitativos y cualitativos.

Además, según los resultados obtenidos, la HEI identificará y asociará los riesgos a los que se expone la información y la continuidad digital si la solución de preservación está incumpliendo los requisitos indispensables, lo cual permitirá tomar una decisión sobre la compra de la solución, y planificar cómo disminuir o mitigar los riesgos según sea el caso.

HEI tiene un impacto económico y social. Económico porque permitirá a las organizaciones evaluar diversas soluciones de preservación y hacer diferentes comprobaciones sobre su idoneidad, por tanto, minimizará los costos asociados a la implementación de una solución tecnológica alejada de la teoría archivística, ya que la herramienta propuesta se encuentra diseñada en estricto cumplimiento con modelos, normas y buenas prácticas nacionales e internacionales en materia de preservación digital.

Y un impacto social porque pretende que el país apunte a la gestión y preservación sistémica de la información, como herramienta para garantizar un Estado Abierto y fortalecer la cultura de transparencia y rendición de cuentas, así como materializar el derecho de acceso a la información, para fortalecer el Estado de Derecho y la democracia, con sistemas que garanticen la correcta gestión y protección de la información de evidencia en forma reutilizable y de calidad.

Finalmente, como parte complementaria de la HEI se desarrolló un glosario especializado que toma en cuenta términos tanto del ámbito archivístico como del tecnológico, con el fin de lograr una mayor comprensión de los términos utilizados y que a su vez facilite la utilización de la herramienta a los equipos de trabajo interdisciplinarios.

Cuadro 17. Herramienta de Evaluación Integral (HEI)

N° de Ítem	Requisito	Descripción	Nivel de cumplimiento	Riesgos asociados
1. Modelo funcional				
1.1. Ingesta				
1.1.1	La herramienta dispone de agentes para la ingesta de los SIP	El agente favorece la comunicación entre los distintos sistemas informáticos, a la vez que facilita la automatización de determinados procesos como la ingesta, además permite mantener la cadena de preservación.	Indispensable	**R12:** Ruptura de la cadena de custodia digital del documento.

N° de Ítem	Requisito	Descripción	Nivel de cumplimiento	Riesgos asociados
1.1.2	La herramienta permite el encapsulado y empaquetado de los documentos y su información de contexto en contenedores SIP.	El empaquetado en formato XML, va a proporcionar una cobertura, o escudo, que protege la información de contenido de una alteración no documentada, así como su información de contexto.	Indispensable	**R2:** Vulnerabilidad de la información digital. **R4:** Pérdida de equivalencia funcional y valor probatorio de los documentos.
1.1.3	La herramienta permite aplicar la firma digital en formato XAdES-XL o superior para el envío del SIP.	Con esto se busca asegurar la autenticidad y confiabilidad de los SIP, por lo que resulta necesario emplear una firma envolvente (Enveloping) al contenedor en formato XML.	Indispensable	**R4:** Pérdida de equivalencia funcional y valor probatorio de los documentos.
1.1.4	La herramienta permite la recepción de la lista de remisión del SIP compilatorio.	Es necesario para las transferencias realizadas bajo el método *push*, al carecer de un agente de "middleware" que "sale y recoge" el material se requiere que para la entrega y recepción de los SIP se adjunte una lista de remisión, con lo cual se logra tener control y verificación del contenido de las transferencias de documentos de archivo de una etapa a otra.	Deseable	**R12:** Ruptura de la cadena de custodia digital del documento.

N° de Ítem	Requisito	Descripción	Nivel de cumplimiento	Riesgos asociados
1.1.5	La herramienta permite validar la identidad del transferente por medio del cálculo y verificación del hash del paquete de contenidos.	Es necesaria la validación de la identidad del transferente para evitar conservar información de una procedencia errónea.	Indispensable	**R12:** Ruptura de la cadena de custodia digital del documento.
1.1.6	La herramienta permite la validación del contenido, la estructura y la forma del SIP, según lo establecido en el Protocolo de Transferencia.	Es necesario la validación/verificación de la integridad de los datos para asegurar que un determinado Objeto de Información de Contenido no ha sido alterado de una manera no documentada y que cumpla con los criterios establecidos en el Protocolo de Transferencia.	Indispensable	**R2:** Vulnerabilidad de la información digital. **R12:** Ruptura de la cadena de custodia digital del documento. **R13:** Falta de evidencia de registros de trazabilidad.
1.1.7	La herramienta reconoce y valida los formatos de fichero para el documento electrónico recibido.	Permite cumplir con las estrategias de preservación a largo plazo, ya que ayuda a asegurar que el transferente ha seleccionado la extensión correcta de los formatos de fichero que previamente se han establecido y que cumplen con los criterios de formatos para preservación.	Indispensable	**R7:** Obsolescencia del formato digital.

N° de Ítem	Requisito	Descripción	Nivel de cumplimiento	Riesgos asociados
1.1.8	La solución dispone de un almacenamiento aislado temporal, que permita el aseguramiento de la calidad.	Permite un adecuado proceso de aseguramiento de la calidad, es necesario que, durante el proceso de ingesta de los SIP, estos puedan primero ser analizados, ya que pueden contener algún virus u otra inconsistencia. Si el SIP pasa el procedimiento del aseguramiento de la calidad, este se convierte en AIP y se traslada a otro "storage" o almacenamiento permanente en el repositorio. El almacenamiento temporal no crece, ya que los SIP una vez convertidos en AIP, cambian de ubicación y el almacenamiento temporal estará vacío hasta una nueva ingesta de SIP.	Indispensable	**R2:** Vulnerabilidad de la información digital. **R5:** Ataquesinformáticos.
1.1.9	La herramienta permite verificar la validez de la firma digital de los documentos electrónicos.	Permite comprobar la validez del certificado digital asociado al firmante y permite determinar la integridad de la información firmada electrónicamente, verificando que no haya sido alterada después de la firma digital.	Indispensable	**R4:** Pérdida de equivalencia funcional y valor probatorio de los documentos.
1.1.10	La herramienta permite notificar a los responsables de administrar el repositorio digital en caso de rechazo o aprobación de la transferencia.	Es necesario supervisar el proceso de transferencia y en particular lo concerniente a la aprobación o rechazo de los SIP y en el caso de los SIP rechazados permite identificarlos y comunicar el evento al transferente.	Deseable	Es un proceso administrativo, no genera un riesgo asociado a la preservación digital.

N° de Ítem	Requisito	Descripción	Nivel de cumplimiento	Riesgos asociados
1.1.11	La herramienta permite la administración de los metadatos asociados en el SIP, según normas internacionales o diccionarios de descripción archivística.	Necesario para la inteligibilidad de la información en el futuro, sobre el contexto en que se crearon y usaron los documentos electrónicos, así como aspectos técnicos, descriptivos, y cualquier otro que garantice su comprensión y gestión a lo largo del tiempo.	Indispensable	**R4:** Limitado acceso a la información digital.
1.1.12	La solución permite revisar la existencia de virus en el formato de fichero.	Como parte del proceso de aseguramiento de la calidad, una vez que se procede con el ingreso del SIP, se debe asegurar que este no contenga ningún tipo de virus que pueda infectar al resto de los objetos digitales alojados en el almacenamiento permanente.	Indispensable	**R2:** Vulnerabilidad de la información digital. **R5:** Ataquesinformáticos.
1.1.13	La herramienta permite la conversión de formatos, según reglas de administración de formatos y preservación documental.	El proceso de transformación de un SIP a un AIP puede requerir de la conversión de formatos de fichero como estrategia de control de la obsolescencia de formatos, por lo que la institución debe contar con una política o procedimiento organización que describa el proceso de conversión y los parámetros para llevarlo a cabo de acuerdo con la gestión de riesgos asociados a los formatos utilizados.	Indispensable	**R7:** Obsolescencia del formato digital. **R10:** Errores humanos que afectan la preservación de la información digital.

N° de Ítem	Requisito	Descripción	Nivel de cumplimiento	Riesgos asociados
1.1.14	La herramienta registra los metadatos de preservación correspondientes al evento de conversión de formatos.	Necesaria para llevar a cabo, documentar y evaluar los procesos que apoyan la retención y accesibilidad a largo plazo de los contenidos digitales. Los metadatos de preservación documentan los procesos técnicos asociados con la preservación, especifican la información de gestión de derechos, establecen la autenticidad del contenido digital y registran la cadena de custodia y procedencia de un objeto digital.	Indispensable	**R3:** Limitado acceso a la información digital. **R10:** Errores humanos que afectan la preservación de la información digital. **R13:** Falta de evidencia de registros de trazabilidad.
1.1.15	La herramienta permite generar o extraer y guardar los metadatos relacionados con el contexto, la estructura y el contenido del documento.	Necesario para la inteligibilidad de la información en el futuro, sobre el contexto en que se crearon y usaron los documentos electrónicos, así como aspectos técnicos, de preservación, descriptivos, y cualquier otro que garantice la comprensión y su gestión a lo largo del tiempo.	Indispensable	**R3:** Limitado acceso a la información digital.

N° de Ítem	Requisito	Descripción	Nivel de cumplimiento	Riesgos asociados
1.1.16	La herramienta permite generar o extraer y guardar las propiedades significativas.	Necesario para la inteligibilidad de la información en el futuro, sobre las características de un objeto de información que deben ser mantenidas a lo largo del tiempo para asegurar su acceso continuado, uso, significación y su capacidad de ser aceptado como evidencia de lo que pretende ser como documento de archivo.	Indispensable	**R3:** Limitado acceso a la información digital. **R4:** Pérdida de equivalencia funcional y valor probatorio de los documentos.
1.1.17	La herramienta guarda los metadatos recibidos del SIP y aplica el esquema de metadatos vigente en el AIP.	Es necesario que se sigan custodiando los metadatos contenidos en el paquete SIP y, una vez este se transforme en un AIP con los respectivos metadatos de preservación, como evidencia de los cambios y acciones sobre los objetos digitales durante todo su proceso de gestión, permitiendo garantizar la fiabilidad del contenido preservado.	Indispensable	**R3:** Limitado acceso a la información digital. **R4:** Pérdida de equivalencia funcional y valor probatorio de los documentos.
1.1.18	La herramienta permite notificar al transferente el resultado del SIP.	Es necesario supervisar el proceso de transferencia y en particular lo concerniente a la aprobación o rechazo de los SIP para evitar errores y cumplir a cabalidad con lo estipulado en el protocolo de transferencia.	Deseable	**R13:** Falta de evidencia de registros de trazabilidad.
1.2. Generación del AIP				

N° de Ítem	Requisito	Descripción	Nivel de cumplimiento	Riesgos asociados
1.2.1	La herramienta permite conformar y registrar el AIP.	El empaquetado en formato XML, va a proporcionar una cobertura, o escudo, que protege la información de contenido de una alteración no documentada, así como su Información de Descripción de Conservación asociada, además este es el paquete que se conserva en la herramienta.	Indispensable	**R1:** Pérdida de información digital. **R12:** Ruptura de la cadena de custodia digital del documento. **R13:** Falta de evidencia de registros de trazabilidad.
1.2.2	La herramienta permite obtener las propiedades significativas y en especial los elementos de criptografía y guardarlos en los respectivos campos de metadatos de preservación PREMIS.	Asegurar e identificar en el tiempo si los documentos son fidedignos, y permiten su accesibilidad, usabilidad y valor evidencial.	Indispensable	**R4:** Pérdida de equivalencia funcional y valor probatorio de los documentos.

N° de Ítem	Requisito	Descripción	Nivel de cumplimiento	Riesgos asociados
1.2.3	La herramienta permite obtener los identificadores de número característicos de los documentos (*checksum*) y consignarlos en los atributos correspondientes junto con el tipo de algoritmo (*checksumtype*).	Para detectar cambios en una secuencia de datos y proteger su integridad, es necesario verificar que no haya discrepancias entre los valores obtenidos al hacer una comprobación inicial y otra final tras la transmisión. Para ello es necesario el uso de funciones *hash* criptográficas.	Indispensable	**R4:** Pérdida de equivalencia funcional y valor probatorio de los documentos. **R11:** Expiración de la criptografía del Paquete de Información Archivística.
1.2.4	La herramienta permite proteger la información del AIP mediante la aplicación de firma digital en formato XAdES-XL o superior.	Para asegurar la autenticidad y confiabilidad es necesario realizar una firma envolvente (Enveloping) al contenedor del AIP que se encuentra en formato XML.	Indispensable	**R4:** Pérdida de equivalencia funcional y valor probatorio de los documentos. **R11:** Expiración de la criptografía del Paquete de Información Archivística.

N° de Ítem	Requisito	Descripción	Nivel de cumplimiento	Riesgos asociados
1.2.5	La herramienta permite crear el asiento en el registro de transferencia y actualiza la información en los índices de búsqueda y los sistemas con la consulta.	Para facilitar posteriormente el acceso a los paquetes y consultas de los usuarios.	Indispensable	**R12:** Ruptura de la cadena de custodia digital del documento. **R13:** Falta de evidencia de registros de trazabilidad.
1.2.6	La herramienta registra la creación del AIP.	Garantiza que el identificador asignado a cada AIP sea único entre todos los identificadores utilizados para esos paquetes, con el propósito específico de generar un metadato que permita mantenerlos accesibles durante todo su proceso de gestión y permita una consulta de modo inequívoco para los usuarios.	Indispensable	**R3:** Limitado acceso a la información digital.
1.2.7	La herramienta genera identificadores unívocos para todos los AIP.	Garantiza que el identificador asignado a cada AIP sea único entre todos los identificadores utilizados para esos paquetes, con el propósito específico de generar un metadato que permita mantenerlos accesibles durante su gestión y permita una consulta de modo inequívoco para los usuarios.	Indispensable	**R3:** Limitado acceso a la información digital.

N° de Ítem	Requisito	Descripción	Nivel de cumplimiento	Riesgos asociados
1.2.8	La herramienta tiene acceso a softwares y recursos necesarios para proveer la Información de Representación fidedigna para todos los objetos digitales de archivo.	La información de representación es un conjunto de recursos, incluidos los metadatos estructurales, que son necesarios para una interpretación completa de una entidad intelectual u objeto de datos. Necesarios para asegurar que los objetos digitales custodiados son comprensibles por los usuarios, por lo tanto, debe existir un software que permita identificar el formato y versión precisa de todos los objetos digitales almacenados y vincular esa identificación a un registro central de información técnica sobre ese formato.	Indispensable	**R7:** Obsolescencia del formato digital. **R14:** Gestión insuficiente de la continuidad digital.
1.2.9	La herramienta ejecuta el proceso de verificación de la Información de Contenido de los AIP.	Para asegurarse de que sean exactamente los mismos y que no existan alteraciones en la Información de Contenido.	Indispensable	**R1:** Pérdida de información digital. **R4:** Pérdida de equivalencia funcional y valor probatorio de los documentos.
1.2.10	La herramienta amplía la Información de Descripción de Conservación desde otras fuentes.	Para proporcionar actualizaciones coordinadas y gestión de datos es necesario que la herramienta pueda extraer la Información de Descripción de Conservación desde otras fuentes para que los usuarios puedan buscar, solicitar y recuperar información sobre el fondo.	Indispensable	**R3:** Limitado acceso a la información digital.

N° de Ítem	Requisito	Descripción	Nivel de cumplimiento	Riesgos asociados
1.2.1 1	La herramienta permite extraer la Información de Descripción de Conservación desde los AIP para ser utilizada en los sistemas de consulta.	Es necesario que la herramienta permite extraer Información de Descripción de Conservación desde los AIP para que los usuarios puedan buscar, solicitar y recuperar información sobre el fondo.	Indispensable	**R3:** Limitado acceso a la información digital.
1.2.1 2	La solución permite la notificación a los responsables de cualquier cambio realizado en el AIP.	Para la toma de decisiones y supervisar el proceso de los eventos en el AIP y en particular para detectar algún cambio producido en un AIP.	Deseable	**R13:** Falta de evidencia de registros de trazabilidad.
1.2.1 3	La solución genera bitácoras correspondientes al procedimiento de ingreso del SIP hasta la generación del AIP.	Permite el seguimiento y la evaluación de los procedimientos de ingreso ejecutados en la herramienta.	Indispensable	**R13:** Falta de evidencia de registros de trazabilidad.

N° de Ítem	Requisito	Descripción	Nivel de cumplimiento	Riesgos asociados
1.3. Almacenamiento de archivo				
1.3.1	La herramienta dispone de algún mecanismo de optimización para el almacenamiento y recuperación de los objetos de información.	Es necesario un mecanismo automatizado para reducir errores, así como mejorar la flexibilidad en la recuperación de los activos de información.	Indispensable	**R3:** Limitado acceso a la información digital.
1.3.2	La herramienta monitorea activamente la integridad de los AIP.	Permite la identificación de cambios en las propiedades significativas del AIP ante posibles alteraciones producidas por la obsolescencia tecnológica; dos de los métodos más utilizados para este fin son la verificación de las criptografías anteriores o el uso de resello del AIP.	Indispensable	**R1:** Pérdida de la información digital. **R4:** Pérdida de equivalencia funcional y valor probatorio de los documentos. **R12:** Ruptura de la cadena de custodia digital del documento.

N° de Ítem	Requisito	Descripción	Nivel de cumplimiento	Riesgos asociados
1.3.3	La herramienta tiene registros (trazabilidad) de las acciones y procesos de administración relevantes para el almacenamiento y la conservación de los AIP.	Necesario para la inteligibilidad de la información en el futuro, sobre el contexto en que se creó y usó el documento electrónico, así como aspectos técnicos, de preservación, descriptivos, y cualquier otro que garantice la comprensión y gestión de estos a lo largo del tiempo.	Indispensable	**R1:** Pérdida de la información digital. **R5:** Ataques informáticos. **R14:** Gestión insuficiente de la continuidad digital.
1.3.4	La solución permite realizar copias de seguridad.	Tener copias de seguridad posibilita la recuperación de la información en caso de que se materialicen eventos que pongan en peligro la información preservada, además permite mejorar el tiempo de reacción ante desastres.	Indispensable	**R1:** Pérdida de la información digital. **R5:** Ataques informáticos. **R14:** Gestión insuficiente de la continuidad digital.
1.3.5	La solución permite dar persistencia a los AIP y a las copias remotas seguras.	La persistencia es un método de alta disponibilidad y los datos se almacenan en el disco duro para asegurar que los datos no se pierdan o se borren.	Indispensable	**R14:** Gestión insuficiente de la continuidad digital.

N° de Ítem	Requisito	Descripción	Nivel de cumplimiento	Riesgos asociados
1.3.6	La herramienta permite registrar y actualizar los AIP.	Los AIP pueden ser sujetos a actualizaciones de la información de representación que permitan garantizar la inteligibilidad de la información de contenido, así como aumentar o mejorar la Información de Descripción de Conservación asociada.	Indispensable	**R1:** Pérdida de información digital. **R3:** Limitado acceso a la información digital. **R7:** Obsolescencia del formato digital. **R11:** Expiración de la criptografía del Paquete de Información Archivística.
1.3.7	La solución permite llevar a cabo controles de fallas y rutinas de detección de errores.	Permite aplicar controles internos para identificar la causa principal de un funcionamiento defectuoso en la solución, con el fin de garantizar la operación continua.	Indispensable	**R13:** Falta de evidencia de registros de trazabilidad.
1.3.8	La herramienta registra y revisa todos los fallos y anomalías en la gestión de acceso de los documentos.	Ante posibles eventos es necesario que se registre para subsanar las inconsistencias y mantener la seguridad de la información.	Indispensable	**R13:** Falta de evidencia de registros de trazabilidad.

N° de Ítem	Requisito	Descripción	Nivel de cumplimiento	Riesgos asociados
1.3.9	La herramienta registra los problemas relativos a errores en los datos o en las respuestas de los usuarios.	Ante posibles eventos es necesario que se registre para subsanar las inconsistencias y mantener la continuidad del servicio.	Deseable	**R13:** Falta de evidencia de registros de trazabilidad. **R14:** Gestión insuficiente de la continuidad digital.
1.3.10	La solución permite habilitar los medios de continuidad de servicio en caso de desastres.	Aunque no se pueda mantener la continuidad del servicio se debe tratar de recuperar lo antes posible.	Indispensable	**R14:** Gestión insuficiente de la continuidad digital.
1.4. Gestión de datos				
1.4.1	La herramienta permite crear y firmar los índices electrónicos.	Como elemento de control y gestión de datos es necesario la creación de un índice de los AIP contenidos en un expediente, el cual debe ser firmado para dar fe de este tipo de evento y asegurar la autenticidad y validez del índice.	Indispensable	**R4:** Pérdida de equivalencia funcional y valor probatorio de los documentos.

N° de Ítem	Requisito	Descripción	Nivel de cumplimiento	Riesgos asociados
1.4.2	La herramienta permite recibir solicitudes de informe procedentes de Ingreso, Acceso o Administración y generar el informe que será entregado al solicitante.	Independientemente del proceso donde provengan las solicitudes de informes, la herramienta debe resolver cualquier solicitud que se presente y generar informes como resúmenes de los fondos de archivo por categoría, o estadísticas de uso para los accesos a los fondos de archivo. Tambiénofrece información descriptiva sobreun AIPconcreto.	Indispensable	**R13:** Falta de evidencia de registros de trazabilidad.
1.4.3	La herramienta permite modificar la estructura de un AIP, ampliando el contenido y los metadatos, y añadiendo mecanismos de aseguramiento de autenticidad e integridad (firma y sellado de tiempo).	Cuando los estándares tecnológicos cambien o lo demanden, es necesario que la herramienta permita la modificación de la estructura de un AIP.	Indispensable	**R3:** Limitado acceso a la información digital. **R4:** Pérdida de equivalencia funcional y valor probatorio de los documentos. **R11:** Expiración de la criptografía del Paquete de Información Archivística.

N° de Ítem	Requisito	Descripción	Nivel de cumplimiento	Riesgos asociados
1.4.4	La herramienta utilizada para administrar la base de datos permite generar informes periódicos sobre el estado de actualización de la base de datos.	Es necesario disponer de una herramienta intermediaria entre el usuario y la base de datos, la cual debe generar informes del estado de las bases de datos con el fin de tener un control para mantener la integridad de los datos, controlar el acceso de las personas a la información y, en caso de errores o fallas, la recuperación de los datos.	Indispensable	**R6:** Acceso no autorizado a información / documentos. **R14:** Gestión insuficiente de la continuidad digital.
1.5. Acceso				
1.5.1	La herramienta permite coordinar la ejecución de solicitudes de usuarios.	Es importante que la herramienta ofrezca los servicios y funciones de apoyo a los usuarios que les permitan descubrir la existencia, localización y disponibilidad de la información almacenada, permitiendo de esta manera la recuperación de la información solicitada.	Indispensable	**R3:** Limitado acceso a la información digital.

N° de Ítem	Requisito	Descripción	Nivel de cumplimiento	Riesgos asociados
1.5.2	La herramienta permite recuperar un AIP de almacenamiento de archivo para la creación del DIP.	Para facilitar la información es necesario que se cree un nuevo paquete a partir del AIP que sea más accesible para los usuarios, con el fin de mantener protegido el AIP que es el paquete que debe ser conservado a largo plazo y no debe ser manipulado por otros usuarios.	Indispensable	**R3:** Limitado acceso a la información digital.
1.5.3	La herramienta permite verificar los niveles de acceso a series documentales, expedientes y documentos antes de conceder el acceso a una solicitud.	La verificación de los niveles de acceso permite restringir el uso y visualización de determinados objetos digitales, esto con el fin de proteger la información personal y la intimidad de los usuarios, el secreto comercial, la seguridad de los bienes físicos o financieros y mantener los permisos de usuario brindados.	Indispensable	**R1:** Pérdida de información digital. **R6:** Accesos no autorizados a información/documentos.
1.5.4	La herramienta realiza búsquedas por medio de los índices y descriptores.	Para solventar una necesidad de información y la capacidad de identificar, localizar y utilizar la información de forma efectiva son necesarios los buscadores avanzados que permitan la búsqueda por medio de los índices y descriptores que se han generado en la herramienta.	Deseable	**R3:** Limitado acceso a la información digital.

N° de Ítem	Requisito	Descripción	Nivel de cumplimiento	Riesgos asociados
1.5.5	La herramienta registra ingresos e intentos fallidos.	Documentar los eventos relacionados con los ingresos a la herramienta permitirá tener un mayor control sobre los accesos no autorizados y por ende aplicar medidas para fortalecer los procesos de autenticación de usuarios.	Indispensable	**R2:** Vulnerabilidad de la información digital. **R6:** Acceso no autorizado a información/documentos.
1.5.6	La herramienta permite la función de descarga.	Con el fin de permitir la accesibilidad y disponibilidad de la información pública tanto en medios manuales como electrónicos, la herramienta debe permitir descargar la información en formatos accesibles y abiertos, permitiendo un ejercicio ágil y eficiente del derecho de acceso a la información.	Deseable	**R3:** Limitado acceso a la información digital.
1.5.7	La herramienta permite la selección de opciones para formatos de descarga.	Con el fin de permitir la accesibilidad y disponibilidad de la información pública tanto en medios manuales como electrónicos, la herramienta debe permitir descargar la información en formatos accesibles y abiertos, permitiendo un ejercicio ágil y eficiente del derecho de acceso a la información.	Deseable	**R3:** Limitado acceso a la información digital.

N° de Ítem	Requisito	Descripción	Nivel de cumplimiento	Riesgos asociados
1.5.8	La herramienta permite la conversión de formatos de preservación a formatos de difusión.	La conversión o transformación de formatos en esta instancia se debe adecuar a las necesidades de los usuarios para que puedan tener acceso a los documentos digitales, por lo tanto, este proceso debe ir acompañado de una monitorización constante de los formatos para que puedan ser actualizados conforme van cambiando las necesidades de los usuarios, además de mantener las propiedades significativas del objeto.	Indispensable	**R3:** Limitado acceso a la información digital. **R7:** Obsolescencia del formato digital. **R10:** Errores humanos que afectan la preservación de la información digital.
1.5.9	La herramienta permite aplicar la firma digital al DIP (sello electrónico de persona jurídica) en formato XAdES-XL o superior.	Para asegurar la autenticidad y confiabilidad de los paquetes DIP es necesario realizar una firma envolvente (Enveloping) al contenedor en formato XML.	Indispensable	**R4:** Pérdida de equivalencia funcional y valor probatorio de los documentos. **R11:** Expiración de la criptografía del Paquete de Información Archivística.

N° de Ítem	Requisito	Descripción	Nivel de cumplimiento	Riesgos asociados
1.5.10	La herramienta permite aplicar la firma digital en formato PAdES-LTV o superior a la copia certificada.	Con el fin de constatar y vincular jurídicamente la copia certificada con la información del contenido que se almacena en la herramienta.	Indispensable	**R4:** Pérdida de equivalencia funcional y valor probatorio de los documentos.
1.5.11	La herramienta permite visualizar en línea las copias de consulta de los documentos.	Tiene como finalidad permitir la visualización de documentos en formatos de difusión que presenten alta calidad y funcionalidad sin necesidad de descargar el documento.	Deseable	**R3:** Limitado acceso a la información digital.

N° de Ítem	Requisito	Descripción	Nivel de cumplimiento	Riesgos asociados
1.5.12	La herramienta permite generar metadatos de eventos relacionados con el acceso de usuarios.	Permite brindar un mayor control y seguridad de la información contenida en la herramienta.	Indispensable	**R1:** Pérdida de información digital. **R2:** Vulnerabilidad de la información digital. **R13:** Falta de evidencia de registros de trazabilidad.
1.6. Seguridad				

N° de Ítem	Requisito	Descripción	Nivel de cumplimiento	Riesgos asociados
1.6.1	La herramienta permite gestionar protocolos de permisos de acceso, roles, permisos y usuarios.	Para controlar y administrar adecuadamente el acceso a la herramienta de preservación digital mediante el registro y actualización de la información de los usuarios.	Indispensable	**R1:** Pérdida de información digital. **R2:** Vulnerabilidad de la información digital. **R6:** Accesos no autorizados a información/documentos.
1.6.2	La herramienta permite la autenticación segura de los usuarios.	Para maximizar la protección de la información contenida en la herramienta, las tecnologías de autenticación van a permitir la seguridad en el acceso a la información.	Indispensable	**R1:** Pérdida de información digital. **R2:** Vulnerabilidad de la información digital. **R6:** Accesos no autorizados a información/ documentos.

N° de Ítem	Requisito	Descripción	Nivel de cumplimiento	Riesgos asociados
1.6.3	La herramienta permite garantizar la seguridad de los AIP por medio de llaves criptográficas.	El uso de mecanismos de cifrado irreversible, conocidos como el *hash*, son requeridos para proteger la información que debe ser protegida de cambios que atenten contra su integridad y confidencialidad.	Indispensable	**R1:** Pérdida de información digital. **R2:** Vulnerabilidad de la información digital. **R5:** Ataquesinformáticos.
1.6.4	La herramienta permite la seguridad de los AIP que viajan por la plataforma y por la red.	La protección de la información en redes y la protección de la infraestructura de soporte, debe estar plasmada en los controles de aseguramiento de la Red, premisas de seguridad en los servicios de la red, así como en la segregación de estas, entre otros. (CNTD, 2020, p. 59)	Indispensable	**R1:** Pérdida de información digital. **R2:** Vulnerabilidad de la información digital. **R5:** Ataquesinformáticos.
2. Modelo tecnológico				
2.1. Arquitectura tecnológica				

N° de Ítem	Requisito	Descripción	Nivel de cumplimiento	Riesgos asociados
2.1.1	La solución permite escalar en la capacidad de almacenamiento.	Permite el cumplimiento del Código Nacional de Tecnologías Digitales y está enfocado en la arquitectura orientada a servicios (SOA). La escalabilidad está íntimamente ligada al diseño del sistema e influye en el rendimiento de forma significativa.	Indispensable	**R2:** Vulnerabilidad de información digital. **R3:** Limitado acceso a la información digital. **R14:** Gestión insuficiente de la continuidad digital.
2.1.2	La solución permite escalar en cantidad de usuarios servidos o concurrentes que puedan acceder a la información simultáneamente.	Permite el cumplimiento del Código Nacional de Tecnologías Digitales y está enfocado en la arquitectura orientada a servicios (SOA). La escalabilidad está íntimamente ligada al diseño del sistema e influye en el rendimiento de forma significativa.	Indispensable	**R2:** Vulnerabilidad de información digital. **R3:** Limitado acceso a la información digital. **R14:** Gestión insuficiente de la continuidad digital.

N° de Ítem	Requisito	Descripción	Nivel de cumplimiento	Riesgos asociados
2.1.3	La solución permite escalar y/o distribuir la carga de los servicios que atiende según demanda.	Permite el cumplimiento del Código Nacional de Tecnologías Digitales y está enfocado en la arquitectura orientada a servicios (SOA). La escalabilidad está íntimamente ligada al diseño del sistema e influye en el rendimiento de forma significativa.	Indispensable	**R2:** Vulnerabilidad de información digital. **R3:** Limitado acceso a la información digital. **R14:** Gestión insuficiente de la continuidad digital.
2.1.4	La solución permite gestionar copias en localizaciones geográficas alternas para la seguridad de los datos.	Permite el cumplimiento del Código Nacional de Tecnologías Digitales y además permite establecer condiciones adicionales respecto a la fiabilidad y disponibilidad del servicio, respaldo de datos y recuperación de desastres, más allá de las ofrecidas por defecto.	Indispensable	**R1:** Pérdida de información digital. **R14:** Gestión insuficiente de la continuidad digital.
2.1.5	La herramienta registra la información utilizando un Sistema de Gestión de Bases de Datos (SGBD).	Por medio del SGBD es posible administrar, controlar o supervisar la base de datos en donde se almacenan los objetos digitales, por lo que juega un papel importante en garantizar la fiabilidad y el acceso de la información, pues por medio de ella se realizan diferentes funciones como lo es el almacenamiento de datos, eliminación de datos administración de metadatos, seguridad de los datos y la optimización de consultas.	Indispensable	**R1:** Pérdida de información digital. **R2:** Vulnerabilidad de la información digital.

N° de Ítem	Requisito	Descripción	Nivel de cumplimiento	Riesgos asociados
2.1.6	La herramienta almacena los AIP en bases de datos.	Permite el cumplimiento del Código Nacional de Tecnologías Digitales, ya que es necesario la utilización de formatos estándares para la recolección y el almacenamiento de información en bases de datos, porque permiten agrupar y almacenar la información de manera fiable y segura.	Indispensable	**R1:** Pérdida de información digital. **R2:** Vulnerabilidad de la información digital.
2.2. Infraestructura tecnológica				
2.2.1	La herramienta puede ser implementada en ambientes o plataformas que garanticen la alta disponibilidad de sus servicios.	Permite el cumplimiento del Código Nacional de Tecnologías Digitales y además va a generar que existan procedimientos para la recuperación ante desastres, con miras a buscar la más alta disponibilidad posible de los servicios y los datos, para garantizar su continuidad.	Indispensable	**R14:** Gestión insuficiente de la continuidad digital.
2.2.2	La herramienta tiene la capacidad para recuperarse de fallas y/o tolerar problemas y mantener el nivel de prestación de servicio especificado.	Permite el cumplimiento del Código Nacional de Tecnologías Digitales y además va a generar que existan procedimientos para la recuperación ante desastres y la continuidad de los servicios.	Indispensable	**R14:** Gestión insuficiente de la continuidad digital.

N° de Ítem	Requisito	Descripción	Nivel de cumplimiento	Riesgos asociados
2.2.3	La herramienta no limita la posibilidad de implementarse en servidores virtuales.	Con la posibilidad de implementarse en servidores virtuales va a permitir un mayor aprovechamiento de los recursos, y permite la posibilidad a la ejecución en paralelo de varios servidores, tanto para un mejor rendimiento como para tener sistemas de redundancia, el cual es útil en caso de que un servidor falle.	Deseable	Se expresa la posibilidad de una de las opciones de uso de la herramienta, por lo tanto, no genera un riesgo asociado.
2.2.4	La herramienta no limita la posibilidad de implementarse en la nube.	Permite el cumplimiento del Código Nacional de Tecnologías Digitales y además permite su implementación y ejecución como un servicio en la nube.	Deseable	Se expresa la posibilidad de una de las opciones de uso de la herramienta, por lo tanto, no genera un riesgo asociado.
2.3. Seguridad tecnológica				

N° de Ítem	Requisito	Descripción	Nivel de cumplimiento	Riesgos asociados
2.3.1	La solución registra de forma segura los errores producidos en la herramienta.	Permite el cumplimiento del Código Nacional de Tecnologías, además es importante señalar que toda aplicación de software es susceptible a poseer errores, para ello se debe seguir el control de errores, estos deben registrarse de forma segura y privada donde los responsables o administradores los puedan recibir y analizar.	Indispensable	**R13:** Falta de evidencia de registros de trazabilidad.
2.3.2	La solución tiene sistemas de software o hardware especializados en protección contra amenazas.	Permite el cumplimiento del Código Nacional de Tecnologías Digitales y además es importante señalar que dentro de la infraestructura tecnológica de la organización se deben tener los sistemas de software o hardware especializados en protección contra amenazas, ya que los equipos deberán estar cubiertos por dichas soluciones para reducir los riesgos de infección por amenazas de malware.	Indispensable	**R2:** Vulnerabilidad de la información digital. **R5:** Ataquesinformáticos.
2.4. Interoperabilidad				

N° de Ítem	Requisito	Descripción	Nivel de cumplimiento	Riesgos asociados
2.4.1	La herramienta tiene la capacidad de interoperar con sistemas dentro y fuera de la organización.	Permite el cumplimiento del Código Nacional de Tecnologías Digitales, además permite una mejor disponibilidad de información en los servicios brindados al ciudadano, así como la confiabilidad en las comunicaciones.	Deseable	**R3:** Limitado acceso a la información digital. **R12:** Ruptura de la cadena de custodia digital del documento. **R15:** Ineficiencia para el intercambio y utilización de información entre sistemas.
2.4.2	Toda interfaz de la herramienta está implementada aplicando esquemas estandarizados.	La herramienta debe intercambiar información con otros productos, sistemas o componentes y/o realizar las funciones requeridas, mientras comparte entornos disímiles de hardware o software.	Indispensable	**R15:** Ineficiencia para el intercambio y utilización de información entre sistemas.

N° de Ítem	Requisito	Descripción	Nivel de cumplimiento	Riesgos asociados
2.4.3	La herramienta permite incorporar metadatos y agrupaciones de metadatos, para el intercambio e integración de los objetos digitales.	Permite un significado claro y adecuado que pueda ser interpretado de manera correcta.	Indispensable	**R3:** Limitado acceso a la información. **R13:** Falta de evidencia de registros de trazabilidad. **R15:** Ineficiencia para el intercambio y utilización de información entre sistemas.
2.4.4	La herramienta implementa protocolos de intercambio o exportación de tipos de datos abiertos o no propietarios.	Permite garantizar la interoperabilidad entre los sistemas interconectados u otros sistemas a futuro.	Indispensable	**R3:** Limitado acceso a la información. **R15:** Ineficiencia para el intercambio y utilización de información entre sistemas.

N° de Ítem	Requisito	Descripción	Nivel de cumplimiento	Riesgos asociados
2.4.5	La herramienta implementa protocolos de integración e importación de datos de tipo abierto o no propietarios.	Permite garantizar la interoperabilidad entre los sistemas interconectados u otros sistemas a futuro.	Indispensable	**R3:** Limitado acceso a la información. **R15:** Ineficiencia para el intercambio y utilización de información entre sistemas.
2.5. Neutralidad tecnológica				
2.5.1	La herramienta permite el acceso a los usuarios independientemente de la plataforma o sistema operativo que utiliza.	Permite el cumplimiento del Código Nacional de Tecnologías Digitales, además busca la independencia tecnológica, y que la administración y la herramienta no condicionen la tecnología que elijan los ciudadanos para relacionarse con ella.	Indispensable	**R3:** Limitado acceso a la información.
2.5.2	La herramienta emplea estándares abiertos, suficientemente documentados y de uso generalizado.	Permite el cumplimiento del Código Nacional de Tecnologías Digitales, además garantiza la pluralidad tecnológica y la libre competencia. Asimismo, este tipo de estándares no debe suponer una dificultad de acceso, y su uso y aplicación no está condicionado al pago de un derecho de propiedad.	Indispensable	**R3:** Limitado acceso a la información. **R15:** Ineficiencia para el intercambio y utilización de información entre sistemas.

N° de Ítem	Requisito	Descripción	Nivel de cumplimiento	Riesgos asociados
2.5.3	Los datos, incluyendo los AIP, se almacenan empleando estándares abiertos y de uso generalizado.	Por un asunto estratégico, si los AIP no se almacenan con el principio de neutralidad tecnológica, podría generar una dependencia con un estándar de marca comercial, el cual podría condicionar a los ciudadanos e iría en contra de los principios de Estado Abierto.	Indispensable	**R3:** Limitado acceso a la información. **R15:** Ineficiencia para el intercambio y utilización de información entre sistemas.

Fuente: elaboración propia.

4.1 Metodología de puntuación

Si bien todos los requisitos propuestos en la HEI son importantes y subsanan una necesidad que debe ser cubierta por la solución de preservación de documentos digitales, también se debe considerar que algunos de ellos permiten controlar y mitigar riesgos que de materializarse pueden implicar un impacto mayor para la organización. Por esta razón se ponderó a cada uno de los requisitos como indispensables o deseables.

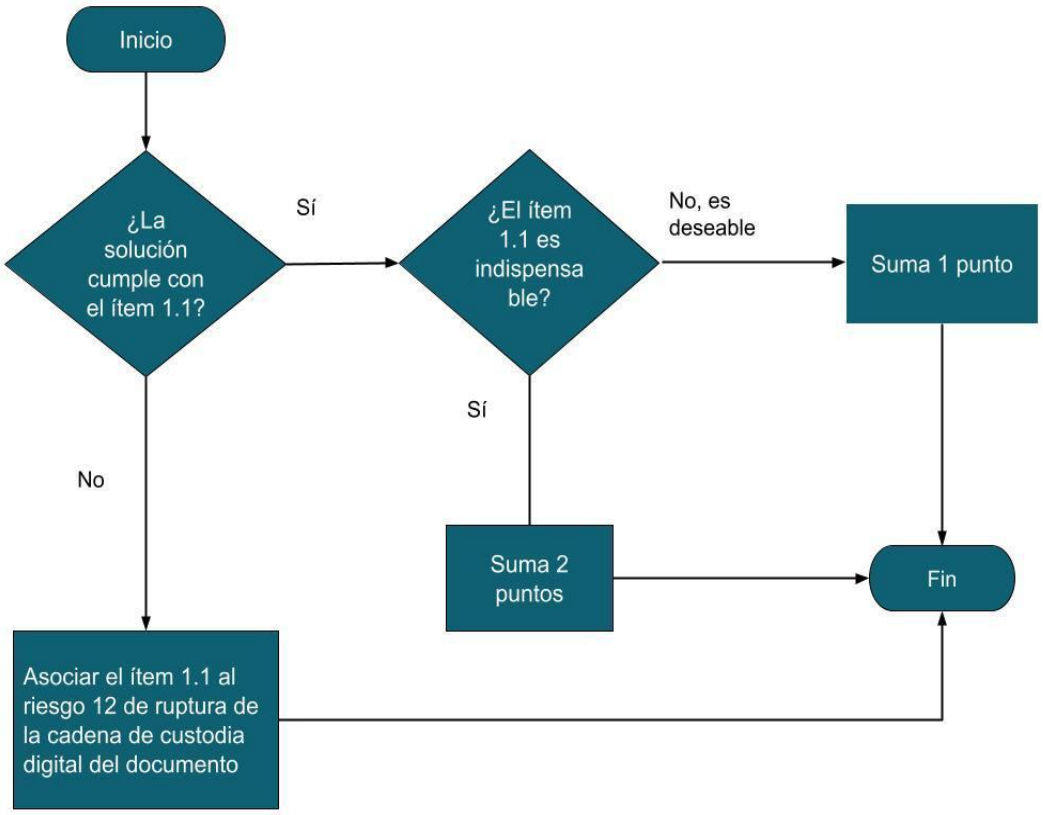
Cuando un requisito es clasificado en la categoría de deseable se le asigna unvalor de 1 punto, esto significa que éste no debe ser considerado como de aplicación estrictamente obligatoria, sin embargo, su contemplación le brinda un valor añadido a la solución que se está evaluando, por lo que la calificación final será más alta en comparación con las soluciones que no los toman en cuenta.

Por su parte, a los requisitos indispensables se les calificará con un valor de 2 puntos, puesto que estos deberían considerarse de carácter obligatorio, ya que se encuentran asociados a aquellos requisitos mínimos necesarios para que una solución logre preservar las características que permiten la perdurabilidad del documento o su información contenido a largo plazo.

En caso contrario, en donde la solución no aplique los requisitos propuestos no sumará puntos y dichos requisitos serán asociados a uno o más riesgos que pueden comprometer el objetivo de preservar la información, estos riesgos ya fueron evaluados y analizados previamente en el capítulo anterior, por lo que puede consultar las razones e implicaciones que estos riesgos conlleva para la información de su organización.

A continuación, se presenta un ejemplo por medio de un diagrama de flujo, en donde se representa visualmente la metodología de puntuación del marco de evaluación:

Figura 17. Flujograma de metodología de puntuación de la Herramienta de Evaluación Integral



Fuente: elaboración propia.

Como se observa en la figura 17, al momento de evaluar un requisito, en este caso el ítem 1.1 fue tomado para realizar el ejemplo, los usuarios verificarán si éste se cumple o no, si realmente es cubierto por la solución que se está sometiendo a evaluación, la HEI procederá a verificar si el requisito fue calificado como indispensable o deseable, asignando una calificación acorde con lo expuesto anteriormente.Mientras que, de no cumplir con el requisito, la HEI lo asocia con un riesgo, el cual permitirá al usuario al final de la evaluación corroborar a qué riesgos se está viendo expuesto en caso de adquirir la solución evaluada.

CONCLUSIONES Y RECOMENDACIONES

1. Conclusiones

Los archivos se enfrentan actualmente a constantes cambios de paradigmas y matices, en donde el uso de herramientas tecnológicas para la producción, gestión y custodia de los documentos de archivo ha ido ganando terreno, convirtiéndose en una realidad a la cual los profesionales en Archivística deben adaptarse, prepararse y hacer frente, es por esta razón, que al inicio del presente proyecto surgieron una serie de incertidumbres en relación a la capacidad de discernimiento de las organizaciones del sector público costarricense para la adquisición de una solución de preservación de documentos digitales.

En este sentido, el diagnóstico aplicado al Sistema Nacional de Archivos esbozó una serie de aspectos que deben ser abordados urgentemente por las autoridades competentes, puesto que el contexto actual reclama que se tomen las acciones necesarias para afrontar un panorama en donde no se garantiza la preservación de los objetos digitales a lo largo de su proceso de gestión y en consecuencia, su incapacidad como evidencia administrativa y legal para la toma de decisiones, la transparencia y la rendición de cuentas de la gestión institucional del país y, para proteger los derechos de los ciudadanos y de la propia administración.

Del diagnóstico de preservación digital, se determinó que la normativa nacional marca los lineamientos a seguir para garantizar la preservación de la información y puede interpretarse a la luz de las nuevas tecnologías y recursos virtualizados, sin embargo, resulta general e insuficiente como insumo para que las instituciones costarricenses puedan adquirir soluciones de preservación digital confiables, pues no delimita de forma clara y consistente los requisitos técnicos necesarios para la adecuada gestión y preservación de los recursos digitales.

De igual manera, por medio de la aplicación de la encuesta se desveló que en la mayoría de las instituciones no existe una cultura organizacional interesada en la preservación y continuidad de la información digital a largo plazo, además se evidenció un desconocimiento por parte de los encargados de los archivos centrales de lo que realmente es un repositorio o solución de preservación digital, puesto que

se suele limitar a la acción de almacenar información digital y en ausencia del establecimiento de políticas institucionales y planes estratégicos.

Teniendo en cuenta este panorama y la falta de un marco normativo de índole técnico que permita, actualmente, a las instituciones disponer de criterios técnicos para la adquisición de soluciones de preservación de documentos digitales, se ha dado paso a la adopción de soluciones incapaces de preservar la información digital. Ha sido, y es, práctica común en el SNA, la adquisición de soluciones que fueron creadas e ideadas principalmente para la producción de documentos, equiparando sus funcionalidades con las que cumple un Sistema de Gestión de Documentos Electrónicos (SGDE) e incluso con las de un Sistema de Gestión para los Documentos Electrónicos de Archivo (SGDEA), perdiendo la lógica individual del funcionamiento de cada sistema.

Lo anterior conducirá, de acuerdo con la evaluación de riesgos asociados a la preservación digital, a que se experimenten modificaciones, eliminaciones y grandes pérdidas del acervo digital custodiado en las instituciones. Tampoco se podrá esperar que los sistemas adquiridos garanticen una cadena de custodia digital de confianza, ni la conservación a lo largo del tiempo de las propiedades significativas de los objetos digitales para asegurar su continua accesibilidad, autenticidad y usabilidad como valor evidencial.

Asimismo, debido a las características del documento electrónico, y su dependencia de un medio de almacenamiento y de un formato de fichero, es vulnerable ante eventos como la obsolescencia tecnológica que es irreversible al continuo proceso de la evolución tecnológica. Por lo tanto, las consecuencias que pueden producirse en las instituciones públicas que producen y gestionan documentos digitales, al no disponer de las estrategias, planes y políticas de preservación digital que mitiguen el efecto de obsolescencia tecnológica, pueden ser catastróficas.

Transgrediendo la concepción de Estado de Derecho, generando problemas económicos y legales, entorpeciendo la gestión pública y la protección de los derechos de los ciudadanos. Si bien es cierto el Estado de Derecho está articulado a través de un marco legal que reconoce los derechos fundamentales, la no

arbitrariedad de las decisiones, la transparencia y la rendición de cuentas, también deben existir los mecanismos para que estas puedan ejecutarse, es decir la información auténtica, integra, accesible y completa, para garantizar su cumplimiento.

También se obstaculiza el impulso de estrategias como Gobierno y Estado Abierto, puesto que sin los sistemas de preservación digitales idóneos, resultaría imposible garantizar el cumplimiento efectivo del derecho de acceso a la información pública, de forma proactiva, oportuna, oficiosa, completa y accesible.

La preservación digital no se limita a enmendar un problema de tecnología y su obsolescencia, ni a solucionar el problema con el almacenamiento o copias de seguridad, sino que conlleva solucionar problemas organizativos y de recursos financieros y humanos. La preservación digital abarca una amplia gama de actividades que deben emprenderse de manera proactiva y para ello será importante que los procesos técnicos archivísticos en conjunto con la aplicación de las políticas y estrategias de preservación sean a través de soluciones tecnológicas.

Por tanto, el marco de evaluación para soluciones de preservación de documentos digitales, pretende servir como guía para todas las instituciones que se encuentren preparadas para la adquisición de un sistema de preservación seguro y confiable, que apunte a la gestión y garantía de acceso por un largo plazo, haciendo uso de técnicas, estándares y estrategias de manera sistémica, y esté adaptado a las circunstancias cambiantes, con el fin de garantizar la seguridad informática, la protección de los datos y el acceso a la información.

Para ello la Herramienta de Evaluación Integral (HEI) propuesta, ofrecerá a las instituciones una hoja de verificación para controlar el cumplimiento del listado de requisitos funcionales y tecnológicos de manera sistémica, lo que le permitirá a las organizaciones realizar comprobaciones de diferentes soluciones de preservación digital con el fin obtener resultados tanto cuantitativos como cualitativos que le permitan tomar una decisión de compra informada y acorde a sus necesidades y en pro de la continuidad y de la preservación de la información digital.

2. **Recomendaciones**

Como recomendacionesgenerales:

Fortalecer una cultura institucional para el cumplimiento efectivo de la normativa nacional relacionada a preservación de la información digital que, aunque resulta insuficiente, se está infringiendo y tiene un efecto negativo en el establecimiento de sistemas de preservación digital confiables que garanticen el resguardo de la información digital fidedigna y su accesibilidad en el tiempo.

Realizar evaluaciones de riesgos cíclicas asociadas a la preservación de la información digital y su continuidad a largo plazo, que actualmente se incumple y que permitiría identificar amenazas, implementar mejoras o reducir riesgos y tomar decisiones de manera informada en beneficio de la organización, del acceso a la información y de la protección de los derechos de los ciudadanos.

Evaluar las funcionalidades de las soluciones de preservación de documentos digitales previo a una decisión de adquisición, por medio de la Herramienta de Evaluación Integral propuesta en el presente proyecto de investigación y en compañía de un equipo interdisciplinario.

Como recomendaciones específicas:

A la Junta Administrativa del Archivo Nacional como órgano rector del SNA:

- Formular las recomendaciones técnicas necesarias que permitan la actualización y mejora de los procesos de preservación de documentos aplicados actualmente en los archivos del SNA.
- Generar los documentos técnicos necesarios para la normalización del proceso de preservación de documentos digitales, de tal manera que sirvan como elementos orientadores para las organizaciones del sistema en la aplicación de estrategias y procedimientos internos.

A la Dirección General del Archivo Nacional:

- Ofrecer programas de capacitación que abarquen la problemática actual generada por la ineficiente gestión de los documentos digitales con el fin de concientizar a los encargados de archivos del SNA, además de incorporar conocimientos técnicos actualizados relativos a la adecuada gestión y preservación de objetos digitales.

A las instituciones del SNA:

- Propiciar el proceso de culturización organizaciones sobre la importancia y necesidad de la adecuada preservación de los documentos digitales.

- Disponer de una política de preservación digital que les permita establecer una serie de reglas y principios a nivel institucional que funcione como guía para la toma de decisiones y delimite los campos de acción de las personas implicadas en el proceso de preservación de documentos digitales.

- Generar planes estratégicos de preservación que sean coherentes con la política de preservación digital, así como con la situación actual de la organización y los objetivos planteados con relación al proceso de preservación.

- Posibilitar la formación y capacitación continua del personal encargado del proceso de preservación digital.

- Apostar por la preservación digital sistémica, de tal forma que se cuente con Sistema de Gestión de Documentos Electrónicos de Archivo o Archivo Digital encargado de ejecutar tanto los procesos técnicos archivísticos, incluido el de preservación, en aquellos documentos que requieran ser custodiados de manera permanente o a largo plazo, de esta manera se evitará la ruptura de la cadena de custodia de los documentos, así como asegurar las características de fiabilidad que requieren los documentos de archivo para servir como fuente de prueba y el resguardo de derechos civiles.

A los encargados o jefes de archivos centrales:

- Capacitarse para incorporar y adquirir conocimientos sobre los estándares y estrategias de preservación de documentos digitales.

- Evaluar la situación actual de la organización en preservación digital e identificar qué acciones se están realizando y quiénes son los responsables.

- Realizar y aplicar los instrumentos archivísticos que permitan la adecuada identificación, descripción, clasificación y evaluación de los documentos, esto previamente a la adopción de herramientas y soluciones tecnológicas.

- Proponer y promover proyectos integrales de preservación de documentos digitales que busquen garantizar la preservación de la cadena de custodia de los documentos.

A los proveedores de soluciones de preservación digital:

- Contemplar el marco de evaluación de soluciones de preservación digital de documentos para el desarrollo de las soluciones que ofrecen, con el fin de que estas se encuentren en estricto cumplimiento con normas y estándares, nacionales e internacionales en materia de preservación digital. y los productos que brinden garanticen que la información permanecerá íntegra, auténtica, segura y accesible a largo plazo.

REFERENCIAS BIBLIOGRÁFICAS

Archivematica. (s.f.). archivematica.org. Recuperado de: https://www.archivematica.org/

Archivo Nacional de Costa Rica (2019). La información: el ADN de la transformación digital. XXXI Congreso Archivístico Nacional. San José, Costa Rica.

Archivo Nacional de Costa Rica (2019). Sistema Nacional de Archivos. Circular DSAE-02-2019. San José, Costa Rica.

Archivos Nacionales de Australia. (s.f.). Xena. Recuperado de: http://xena.sourceforge.net/

Asamblea Nacional Constituyente. (1949). Constitución Política de la República de Costa Rica. Publicada el 08.11.1949.

Asociación Española de Normalización y Certificación UNE-EN ISO/IEC 27000. (2019). Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Visión de conjunto y vocabulario. Recuperado de Bases de Datos del SIBDI: AENORMÁS.

Asociación Española de Normalización y Certificación UNE-EN ISO/IEC 27001. (2017). Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. Recuperado de Bases de Datos del SIBDI: AENORMÁS.

Asociación Española de Normalización y Certificación UNE-EN ISO/IEC 27002. (2017). Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información. Recuperado de Bases de Datos del SIBDI: AENORMÁS.

Asociación Española de Normalización y Certificación UNE-EN ISO/IEC 27037. (2016). Tecnología de la información. Técnicas de seguridad. Directrices para la identificación, recogida, adquisición y preservación de evidencias electrónicas. Recuperado de Bases de Datos del SIBDI: AENORMÁS.

Asociación Española de Normalización y Certificación UNE-ISO 9000. (2015). Sistemas de Gestión de la Calidad- Fundamentos y Vocabulario. Recuperado de Bases de Datos del SIBDI: AENORMÁS.

Asociación Española de Normalización y Certificación UNE-ISO 17021. (2011). Evaluación de la conformidad- Requisitos para los organismos que realizan la auditoría y la certificación de sistemas de gestión. Recuperado de Bases de Datos del SIBDI: AENORMÁS.

Asociación Española de Normalización y Certificación UNE-ISO 13008. (2013). Información y documentación. Proceso de migración y conversión de documentos electrónicos. Recuperado de Bases de Datos del SIBDI: AENORMÁS.

Asociación Española de Normalización y Certificación UNE-ISO 14641. (2012). Especificaciones para el diseño y funcionamiento de un sistema de información para la preservación de información digital. Parte 1. Recuperado de Bases de Datos del SIBDI: AENORMÁS.

Asociación Española de Normalización y Certificación UNE-ISO 14721. (2015). Sistemas de transferencia de datos e información espaciales Sistema abierto de información de archivo (OAIS) Modelo de referencia. Recuperado de Bases de Datos del SIBDI: AENORMÁS.

Asociación Española de Normalización y Certificación UNE-ISO 15489-1. (2016). Información y documentación. Gestión de documentos. Parte 1: Conceptos y principios. Recuperado de Bases de Datos del SIBDI: AENORMÁS.

Asociación Española de Normalización y Certificación UNE-ISO 16363. (2017). Sistemas de transferencia de información y datos espaciales. Auditoría y certificación de repositorios digitales de confianza. Recuperado de Bases de Datos del SIBDI: AENORMÁS.

Asociación Española de Normalización y Certificación UNE-ISO 17068. (2020). Información y documentación. Repositorio de tercero de confianza para

documentos electrónicos. Recuperado de Bases de Datos del SIBDI: AENORMÁS.

Asociación Española de Normalización y Certificación UNE-ISO 22300. (2020). Sistema de Gestión de la Continuidad del Negocio. Requisitos. Recuperado de Bases de Datos del SIBDI: AENORMÁS.

Asociación Española de Normalización y Certificación UNE-ISO 23081-2. (2011). Información y Documentación. Procesos de Gestión de Documentos. Metadatos para la Gestión de Documentos. Parte 2: Elementos de Implementación y Conceptuales. Recuperado de Bases de Datos del SIBDI: AENORMÁS.

Asociación Española de Normalización y Certificación UNE-ISO 30300. (2011). Sistema de gestión para los documentos. Fundamentos y vocabulario. Recuperado de Bases de Datos del SIBDI: AENORMÁS.

Asociación Española de Normalización y Certificación UNE-ISO 30301. (2011). Información y Documentación. Sistema de gestión para documentos. Requisitos. Recuperado de Bases de Datos del SIBDI: AENORMÁS.

Asociación Española de Normalización y Certificación UNE-ISO 30302. (2015). Sistema de gestión para los documentos. Guía para la implementación. Recuperado de Bases de Datos del SIBDI: AENORMÁS.

Asociación Española de Normalización y Certificación UNE-ISO 15801. (2019). Gestión de documentos. Información Almacenada Electrónicamente. Recomendaciones sobre confiabilidad y fiabilidad. Recuperado de Bases de Datos del SIBDI: AENORMÁS.

Asociación Española de Normalización y Certificación UNE-ISO 16175. (2012). Principios y requisitos funcionales para documentos en entornos de oficina electrónica. Generalidades y declaración de principios. Recuperado de Bases de Datos del SIBDI: AENORMÁS.

Asociación Española de Normalización y Certificación UNE-ISO/TR 18128 IN.

(2014). Información y documentación. Apreciación del riesgo en procesos y sistemas de gestión documental. Recuperado de Bases de Datos del SIBDI: AENORMÁS.

Asociación Española de Normalización y Certificación UNE-ISO/TR 18492 IN. (2008). Conservación a largo plazo de la información basada en documentos. Recuperado de Bases de Datos del SIBDI: AENORMÁS.

Asociación Española de Normalización y Certificación UNE-ISO 22300. (2018). Seguridad y resiliencia: Vocabulario. Recuperado de Bases de Datos del SIBDI: AENORMÁS.

Asociación Española de Normalización y Certificación UNE-ISO 22301. (2020). Seguridad y resiliencia: Sistema de Gestión de la Continuidad de Negocio. Requisitos. Recuperado de Bases de Datos del SIBDI: AENORMÁS.

Asociación Española de Normalización y Certificación UNE-ISO/TR 23081-3 IN. (2017). Información y Documentación. Procesos de Gestión de Documentos. Metadatos para la Gestión de Documentos. Parte 3: Método de auto-evaluación. Recuperado de Bases de Datos del SIBDI: AENORMÁS.

Asociación Española de Normalización y Certificación UNE-ISO/TR 26122:2008 IN. (2008). Información y documentación. Análisis de los procesos de trabajo para la gestión de documentos. Recuperado de Bases de Datos del SIBDI: AENORMÁS.

Asociación Española de Normalización y Certificación UNE-ISO 31000. (2018). Gestión del riego: directrices. Recuperado de Bases de Datos del SIBDI: AENORMÁS.

AUROL. (2013). Proyecto de preservación digital para la Universidad de Costa Rica. Modelo funcional y técnico del archivo digital.

Barnard, Alicia. Delgado, Alejandro. y Voutssás, Juan. (2014). Los archivos digitales, una visión integradora. (Cap. Estrategias de conservación y preservación de documentos de archivo digitales: Elementos técnicos).

Benemérita Universidad Autónoma de Puebla: México. Disponible en: http://iibi.unam.mx/voutssasmt/documentos/archivos_digitales_3_corto.pdf

Barnard, A. Delgado, A. y Voutssás, J. (2017). "Un marco de referencia para la preservación digital". Archivo General de la Nación: México.

Biblioteca Nacional de España. (2015). Diccionario de datos PREMIS. Recuperado de:http://www.bne.es/es/Micrositios/Publicaciones/PREMIS/001_Introduccion/002_Modelodatos/

Bulgarelli Fuentes, M. (2018). "Propuesta de una metodología para la evaluación de riesgos derivados de las Tecnologías de Información en las auditorías de Estados Financieros ejecutadas por la Contraloría General de la República de Costa Rica". [Maestría, Universidad de Costa Rica]. Repositorio Kerwa. Disponible en: https://www.kerwa.ucr.ac.cr/handle/10669/75576b

Business Integrators Systems Limitada. (s.f.). ¿Qué es ARCA? Disponible en: http://www.bis.co.cr/Products/Arca

Castillo, L. (2016). La firma digital en el nuevo contexto de transformación digital. En revista Red de Seguridad, Nº 74. Disponible en: http://www.redseguridad.com/revistas/red/074/files/assets/basic-html/page-30.html#

Castillo Guevara, J y Paz Martín, S. (2019). Reflexiones generales sobre el Sistema Nacional de Archivos de la República de Cuba desde la perspectiva del modelo de la continuidad de los documentos. *Revista Investigación Bibliotecológica.* 33 (81), 89-101. Recuperado de: http://www.scielo.org.mx/pdf/ib/v33n81/2448-8321-ib-33-81-89.pdf

Castillo-Solano. G. M y Umaña-Alpízar, R. (2018). Modelo de preservación de documentos digitales en la Administración Universitaria. Estudio de caso: Universidad Nacional. Universidad de Costa Rica. San José, Costa Rica.

Cedeño-Molina A, Granados-Peraza, N, Guevara Acon, G, Montero Paniagua C.

(2014). Propuesta de un *Modelo de Requisitos Archivísticos para un sistema de Gestión de Documentos Electrónicos de Archivo (SGDEA) en Costa Rica.* Universidad de Costa Rica. San José, Costa Rica.

Centro de Curación de la Universidad de California. (2012-2016). Unified Digital Format Registry (UDFR). Recuperado de: http://www.udfr.org/

Comisión Económica para América Latina y el Caribe. (2007). Libro blanco de interoperabilidad de gobierno electrónico para América Latina y el Caribe. Versión 3.0. Recuperado de: https://repositorio.cepal.org/bitstream/handle/11362/2871/1/S2007049_es.pdf

Comisión Europea. (2010) Moreq 1: Modelo de Requisitos para la Gestión de Documentos Electrónicos de Archivo. Ministerio de Cultura de España.

Consejo Internacional de Archivos. (2017). Diccionario de Terminología Archivística Multilingüe. Recuperado de:https://www.ica.org/es/recursos-y-eventos/terminolog%C3%ADa-archiv%C3%ADstica-multiling%C3%BCe

Contraloría General de la República. (2007). N-2-2007-CO-DFOE. Normas técnicas para la gestión y el control de las Tecnologías de Información. Recuperado de:https://www.pgr.go.cr/wp-content/uploads/2016/12/Normas_tecnicas_N_2_2007_CO_DFOE_de_la_CGR.pdf

Cruz Mundet, J.R. (2011). Principios, términos y conceptos fundamentales. *Administración de documentos y archivos. Textos fundamentales.* Coordinadora de Asociaciones de Archiveros y Gestores de Documentos (CAA). Madrid, España.

Cruz-Mundet, J.R. y Díez-Carrera. C. (2016). Sistema de Información de Archivo Abierto (OAIS): luces y sombras de un modelo de referencia. *Revista Investigación Bibliotecológica.* 30(70), 221-247.

De Giusti, M. R. (2014). Una metodología de evaluación de repositorios digitales para asegurar la preservación en el tiempo y el acceso a los contenidos. Tesis de grado. Facultad de Informática, Universidad Nacional de la Plata. Buenos Aires, Argentina. Recuperado de: http://sedici.unlp.edu.ar/handle/10915/43157

De la Vega, R. (2013). Preservación Digital en la Nube. Revista de biblioteconomía y documentación. 57, 126-143.

Decreto N.º 40554-C Reglamento Ejecutivo a la Ley del Sistema Nacional de Archivos. Alcance a la Gaceta Nacional No. 217, 7 de setiembre del 2017.

Decreto N.º 33018-MICIT Reglamento Ejecutivo a la Ley de Certificados, Firmas Digitales y Documentos Electrónicos. Alcance a la Gaceta Nacional No. 77, 21 de abril de 2006.

Delgado Gómez, A. (2013). "La nube". En boletín: Legajos. Archivo General de la Nación. 4 (16). 107-122 Disponible en: http://iibi.unam.mx/archivistica/AGN%20legajos16-delgado.pdf

Departamento de Servicios Archivísticos Externos. (2021). Circular DSAE-02-2019. Índice Anual de Desarrollo Archivístico 2018-2019.

Digital Curation Centre. (2018). Digital Repository Audit Method Based On Risk Assessment. Sitio web. Recuperado de: http://www.dcc.ac.uk/resources/repository-audit-and-assessment/drambora

Digital Curation Centre. (2021). Curation Lifecycle Model. Sitio web. Recuperado de: https://www.dcc.ac.uk/guidance/curation-lifecycle-model

Digital Preservation Coalition. (2021). Digital Preservation Coalition Rapid Assessment Model. Sitio web. Recuperado de: https://www.dpconline.org/

Digital Preservation Coalition. (2014). The Open Archival Information System (OAIS) Reference Model: Introductory Guide. 2° edición. Recuperado de:

https://www.dpconline.org/docs/technology-watch-reports/1359-dpctw14-02/file

Digital Preservation Europe. (2008). Planning Tool for Trusted Electronic Repositories. Recuperado de: https://digitalpreservationeurope.eu/platter/

Dirección de Certificadores de Firma Digital Ministerio de Ciencia y Tecnología. (2008). Política de sellado de tiempo del Sistema Nacional de Certificación Digital. Disponible en: http://www.firmadigital.go.cr/Documentos/PoliticadeSelladodetiempover100.pdf

Dirección Nacional de Notariado. (2020). "Justificación y decisión inicial de contratación de una Solución servicio como sistema (SaaS) de un gestor documental y repositorio digital". Disponible en: https://www.sicop.go.cr/index.jsp

Dura Space. (2018). DSPACE. Recuperado de: https://duraspace.org/dspace/

Dura Space. (2018). DuraCloud. Recuperado de: https://duraspace.org/duracloud/

Dura Space. (2018). Fedora. Recuperado de: https://duraspace.org/fedora/

Flores, D. (2020). "La Cadena de Custodia de Archivos Digitales- CCDA combinada con Preservación Digital Sistemática". Digital Preservation Coalition. Recuperado de: https://www.dpconline.org/blog/wdpd/blog-daniel-flores-wdpd

Flores, D. (2020). Los Repositorios Archivísticos Digitales Confiables - RDC-Arch como ambiente de Preservación y garantía de la Autenticidad, Confiabilidad y manutención de la Cadena de Custodia. Palestra Online para el Consejo de la Judicatura Federal. 57 slides. Ciudad de México, México. 23 de septiembre de 2020. Disponible en: http://documentosdigitais.blogspot.com

Florida Centre for Library Automation. (2011). DAITSS Digital Preservation Repository Software. Recuperado de: https://daitss.fcla.edu/

Gaspar Martínez, J. (2010). “El plan de continuidad de negocio: guía práctica para su elaboración”. España: Ediciones Díaz de Santos.

Harvard University Library. (s.f.). GDFR (Global Digital Format Registry). Recuperado de: https://library.harvard.edu/preservation/digital-preservation_gdfr.html

Junta Administradora del Archivo Nacional. (2018). *Norma técnica para la gestión de documentos electrónicos en el Sistema Nacional de Archivos.* Publicada en la Gaceta N° 105 del 21.05.2018.

Infotel. (s.f). Arcsys Software. Recuperado de: https://www.arcsys-software.fr/

InterPARES Project. (s.f). Página principal. Recuperado de: http://www.interpares.org/

InterPARES Trust. (2016). Lista de verificación. Asegurar la confianza en el almacenamiento de un servicio de infraestructura en la nube (IAAS por sus siglas en inglés. Recuperado de: https://interparestrust.org/assets/public/dissemination/EU08_20161110_IaaSChecklist_v1-2_Spanish.pdf

Ley N. º7202, Ley del Sistema Nacional de Archivos. Asamblea Legislativa. La Gaceta: Diario Oficial de Costa Rica, San José, Costa Rica, 27 de noviembre de 1990.

Ley N. º8279, Ley del Sistema Nacional para la Calidad. Asamblea Legislativa. La Gaceta: Diario Oficial de Costa Rica, San José, Costa Rica, 4 de marzo de 2019.

Ley N. º8454 de Certificados, Firmas Digitales y Documentos Electrónicos. La Gaceta: Diario Oficial de Costa Rica, San José, Costa Rica, 13 de octubre de 2005.

Library and Archives Canada.(2010). *File Format Guidelines for Preservation and*

Long-term. Disponible en: http://www.councilofnsarchives.ca/sites/default/files/LAC%20File%20Format%20Guidelines%20for%20Preservation%20and%20Long-term%20v1_2010-12_0.pdf

Library of Congress. (2016). METS: Introducción y tutorial. Recuperado de: http://www.loc.gov/standards/mets/METSOverview_spa.html#MHead

Libraryof Congress. (2019). Sustainability of Digital Formats: Planning for Library of Congress Collections. Recuperado de: :https://www.loc.gov/preservation/digital/formats/fdd/descriptions.shtml

Llansó-Sanjuan, J. (2006). Sistemas archivísticos y modelos de gestión de documentos en el ámbito internacional. Parte II. Revista Códice, 2 (2), 39-70. Recuperado de: http://eprints.rclis.org/20289/1/Sistemas%20archiv%C3%ADsticos%20y%20modelos%20de%20gesti%C3%B3n%20de%20documentos%20en%20el%20%C3%A1mbito%20internacional%20(Parte%20II)1.pdf

Marchionini, G y Shah, C. (2008). Preserving 2008 US Presidential Election Videos. Recuperado de: https://ils.unc.edu/vidarch/Shah-IWAW2007.pdf

Ministerio de Planificación Nacional y Política Económica. (2020). Código Nacional de Tecnologías Digitales. Versión 1.0. Recuperado de: https://www.micit.go.cr/sites/default/files/cntd_v2020-1.0_-_firmado_digitalmente.pdf.

Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones. Directriz N°.019-MP-MICITT: Desarrollo del Gobierno Digital del Bicentenario. Presidencia de la República, San José, Costa Rica, 20 de junio de 2018.

Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones. Directriz N°.067-MICITT-H-MEIC: Masificación de la Implementación y Uso de la Firma Digital en el Sector Público Costarricense. Presidencia de la República, San José, Costa Rica, 03 de abril de 2014.

Ministerio de Economía, Industria y Comercio. Directriz N.°073-MP-MEIC-MC: Transparencia y Acceso a la Información Pública. Presidencia de la República, San José, Costa Rica 27 de abril de 2017.

Ministerio de Planificación Nacional y Política Económica. (2010). Plan maestro de Gobierno Digital de la República de Costa Rica. Recuperado de: http://www.firma-digital.cr/plan_maestro_gob_digital.pdf

National Archives (NARA). (2004). Pautas para digitalizar materiales de archivo para acceso electrónico. Sitio web. Recuperado de: https://www.archives.gov/preservation/technical/guidelines.html

National Archives (NARA). (2020). *Digital File Types.* Disponible en:https://www.archives.gov/preservation/products/definitions/filetypes.html

National Archives of Australia. (2020). Long-term file formats. Disponible en:https://www.naa.gov.au/information-management/storing-and-preserving-information/preserving-information/preserving-digital-information/long-term-file-formats

National Archives of Australia. (2018). Política de Continuidad Digital 2020. Sitio web. Recuperado de: https://www.naa.gov.au/information-management/information-management-policies/digital-continuity-2020-policy

National Archive of Australia. (s.f). Records Management Risk Assessment Offsite data storage. Recuperado de: https://www.naa.gov.au/sites/default/files/2019-09/IM-risk-assessment-offsite-data-storage.pdf

National Digital Stewardship Alliance. (2018). Levels of Digital Preservation. Sitio Web. Recuperado de: https://ndsa.org/activities/levels-of-digital-preservation/

Nestor Working Group. (s.f.). Catalogue of Criteria for Trusted Digital Repositories. Recuperado de: http://files.dnb.de/nestor/materialien/nestor_mat_08-eng.pdf

NTP-ISO/IEC 17000. (2004). Evaluación de la conformidad: Vocabulario y principios generales. Recuperado de: http://www.sanipes.gob.pe/documentos/12_ISO_17000-2005.pdf

Observatorio Vasco de la Cultura. (2011). Formatos de Difusión y Formatos de Preservación de Contenidos Digitales. En Colección Cuadernos de Formación - Kultura 2.0 - número 2. Recuperado de: http://www.kultura.ejgv.euskadi.eus/contenidos/informacion/kultura2_0_prestakuntza/es_k20_form/adjuntos/cuaderno-DIG-52.pdf

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura. (2003). Actas de la Conferencia General, Carta para la Preservación del Patrimonio digital. Recuperado de: http://unesdoc.unesco.org/images/0013/001331/133171s.pdf#page=85

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura. (2003). Directrices para la Preservación del Patrimonio Digital. Recuperado de: http://unesdoc.unesco.org/images/0013/001300/130071s.pdf

Organización de las Naciones Unidas para la Educación y la Ciencia. (2012). Conferencia Internacional: "La Memoria del mundo en la era digital: digitalización y preservación". Recuperado de: http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/mow/unesco_ubc_vancouver_declaration_es.pdf

Organización Internacional de Normalización y Organización de las Naciones Unidas para el Desarrollo Industrial. (s.f). La Caja de Herramientas de Evaluación de la Conformidad. Recuperado de: https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/casco_building-trust-es.pdf

Open Preservation Foundation. (s.f.). Planets: Preservation and Long-term Access through NETworked Services. Recuperado de: http://openpreservation.org/about/projects/planets/

O´toole, J. (1994, Junio). “On the Idea of Uniqueness”. The American Archivist. *57*(4). https://meridian.allenpress.com/american-archivist/article/57/4/632/23625/On-the-Idea-of-Uniqueness

Política de Formatos Oficiales de los Documentos Electrónicos Firmados Digitalmente. Ministerio de Ciencia, Tecnología y Telecomunicaciones. La Gaceta: Diario Oficial de Costa Rica, San José, Costa Rica, 20 de mayo de 2013.

Promotora del Comercio Exterior de Costa Rica. (2019). “Perfil de la oferta costarricense especializada en tecnologías 4.0”. Disponible en: http://sistemas.procomer.go.cr/DocsSEM/20A998F7-39C0-4B39-99AC-083233A2367A.pdf

Public Record Office Victoria. (2019). VERS versión 3: PROS 15/03 Estándar para la encapsulación de información digital. Sitio web. Recuperado de: https://prov.vic.gov.au/recordkeeping-government/about-standards-framework-policies/vers-standard/vers-version-3

Quevedo, J. (2012). Revisión de modelos de gestión de continuidad del negocio. Recuperado en: https://revistasinvestigacion.unmsm.edu.pe/index.php/sistem/article/download/5620/4877/

Raventós-Pajares, P. (2013). Preservación digital: retos y propuestas actuales, Servicio de Archivo y Gestión de Documentos de la Universidad de Lleida. Recuperado de: https://dialnet.unirioja.es/servlet/extaut?codigo=2318209

Red de Bibliotecas Universitarias Españolas. (2020). Guía para la evaluación de los procesos de preservación en repositorios institucionales de investigación. Recuperado de: https://rebiun.xercode.es/xmlui/handle/20.500.11967/634

RedHat. (2020). “¿Qué son los proveedores de nube?”. Disponible en :https://www.redhat.com/es/topics/cloud-computing/what-are-cloud-providers

RLG-NARA Digital Repository Certification Task Force. (2007)0 "Trustworthy

repositories audit & certification: Criteria and checklist". Recuperado de: http://www.crl.edu/PDF/trac.pdf

RLG-OCLC Working Group on Digital Archive Attributes. (2002). ”Trusted digital repositories: Attributes and responsibilities”. Mountain View, CA: Research Libraries Group (RLG). Recuperado de: https://www.oclc.org/content/dam/research/activities/trustedrep/repositories.pdf

RODA: Repository of Authentic Digital Objets. (2018). Recuperado de: https://demo.roda-community.org/?locale=es_CL#welcome

Sánchez Martínez, D.(s.f). Curso de Administración Electrónica: Tema 3 – Formatos de firma electrónica. Universidad de Murcia. Recuperado de: https://webs.um.es/danielsm/miwiki/lib/exe/fetch.php?id=inicio&cache=cache&media=cursocarm-tema3.pdf

Sastre, G. (2015). Preservación y conservación de documentos digitales. En: ArchivPost. Salamanca: Asociación de Archiveros de Castilla y León. Recuperado de: http://www.acal.es/index.php/archivpost-a-fondo

Serra, J. (2001). Gestión de los documentos digitales: estrategias para su conservación. En: El profesional de la información, septiembre, v. 10, n. 9. Recuperado de: http://www.elprofesionaldelainformacion.com/contenidos/2001/septiembre/1.pdf

Serra, J. (2004). La firma electrónica y el archivo digital. En: Primeres Jornades de Signatura Electrónica. Agència Catalana de Certificació (CATCert), Barcelona, del 10 al 11 de Junio.

Serra, J. (2005). Valoración y Selección de documentos electrónicos: Principios y Aplicaciones. Recuperado del sitio web: http://eprints.rclis.org/7333/1/Jordi_Serra_-_TRIA_12.pdf

Smithsonian Institution Archives. (2020). Recommended Preservation Formats for Electronic Records. Disponible en: https://siarchives.si.edu/what-we-do/digital-

curation/recommended-preservation-formats-electronic-records

Stanford Libraries. (2018). InSPECT: Investigating the Significant Properties of Electronic content over time. Recuperado de: http://www.significantproperties.org.uk/significant-properties-and-digital-preservation/

Tamayo Tamayo, M. (2003). El proceso de la investigación científica incluye evaluación y administración de proyectos de investigación. Cuarta edición. Limusa. México. Recuperado del sitio web: https://clea.edu.mx/biblioteca/Tamayo%20Mario%20-%20El%20Proceso%20De%20La%20Investigacion%20Cientifica.pdf

The National Archives. (2009). Propiedades significativas y preservación digital. Recuperado de: https://significantproperties.kdl.kcl.ac.uk/

The National Archives. (2006). The PRONOM PUID Scheme: A scheme of persistent unique identifiers for representation information. Recuperado de: https://www.nationalarchives.gov.uk/aboutapps/pronom/pdf/pronom_unique_identifier_scheme.pdf

Trentin, G. (1992). Estructura y organización de una base de datos. Sitio web: Recuperado de: https://www.researchgate.net/publication/28269254_Estructura_y_organizacion_de_una_base_de_datos

Trusted Digital Repository. (s.f). European Framework for Audit and Certification of Digital Repositories. Recuperado de: http://www.trusteddigitalrepository.eu/Trusted%20Digital%20Repository.html

Universidad de Michigan. (2011). Deep Blue Preservation and Format Support Policy. Recuperado de :https://deepblue.lib.umich.edu/static/about/deepbluepreservation.html

Universidad de Stanford. (s.f.). LOCKSS: Lots of Copies Keep Stuff Safe.

Recuperado de: https://www.lockss.org/

U.S. National Archives and Records Administration. (s.f.). National Archives Electronic Records Archives (ERA). Recuperado de: https://www.archives.gov/era

Vázquez-Moctezuma, S. (2015). Tecnologías de almacenamiento de información en el ambiente digital. Disponible en: https://revistas.ucr.ac.cr/index.php/eciencias/article/view/19762/23190

Voutssas, J. (2009). Factores tecnológicos, legales y documentales de la preservación documental digital. Investigación Bibliotecológica, 23 (49). 67-124.

Voutssas, J. y Barnard, A. (2014). Glosario de Preservación Archivística Digital. Versión 4.0. México: Instituto de Investigaciones Bibliotecológicas y de la Información, UNAM. Recuperado de: http://iibi.unam.mx/archivistica/glosario_preservacion_archivistica_digital_v4.0.pdf

ANEXOS

Anexo N.º 1: Glosario de Preservación Digital

A

A largo plazo/ Long Term: período de tiempo lo suficientemente largo como para que haya preocupación por los impactos de las tecnologías cambiantes, incluido el soporte para nuevos medios y formatos de datos, y de una comunidad de usuarios cambiante, sobre la información que se mantiene en un repositorio. Este período se extiende hacia el futuro indefinido.
Fuente: UNE-ISO 14721:2015, p. 14.

Accesibilidad / Accessibility: la disponibilidad y usabilidad de la información, en el sentido de la capacidad o facilidad actual y futura para que esa información pueda ser reproducida y por tanto usada.
Fuente: Glosario de Preservación Archivística Digital Versión 4.0, 2014, p. 3.

Accesibilidad digital: se entiende por accesibilidad digital el grado en que la información y los servicios digitales están disponibles para personas con diferentes tipos de discapacidades.
Fuente: Código Nacional de Tecnologías Digitales, 2020, p. 111. Citando a Sui, H., & Dempsey, B. (2017).
Ejemplo: Aumento de tamaño de los caracteres, modificación de los colores, navegar sin mouse o navegadores Braille.

Acceso / Access: 1**.** El derecho, oportunidad o medios para encontrar o usar documentos y/o información [Archivos Society of American Archivists, A Glossary of Archival & Records Terminology]. 2. El permiso para localizar y recuperar información para uso (consulta o referencia) dentro de las restricciones legalmente establecidas respecto de privacidad, confidencialidad y autorización. 3. El proceso de recuperar información que se encuentra en un medio de almacenamiento [Informática]. 4.[ver Entidad Funcional de Acceso]
Fuente: Glosario de Preservación Archivística Digital Versión 4.0, 2014, p. 4.
Ejemplo:
1 Se garantiza el libre acceso a los departamentos administrativos con propósitos de información sobre asuntos de interés público (Artículo 30 de la Constitución Pública)
2 El expediente médico no es de acceso público.
3 Todos tuvieron acceso a la información que está almacenada en la nube.

Agente intermedio / Middleware: Middleware es el software que ayuda a una aplicación para interactuar o comunicarse con otras aplicaciones, redes, hardware y / o sistemas operativos. El software ayuda a los programadores liberándose de conexiones complejas necesarias en un sistema distribuido. Eso proporciona herramientas para mejorar la calidad del servicio, seguridad, paso de mensajes, servicios de directorio, archivo servicios, etc. que pueden ser invisibles para el usuario.
Fuente: Toni A. Bishop & Ramesh K. Karne. A SURVEY of MIDDLEWARE, 2003.
Ejemplo: Middleware ofrece una serie de servicios para distintas soluciones de problemas de conectividad entre aplicaciones, por ejemplo: servicios de acceso a datos, estos servicios permiten ejecutar consultas o distintas actualizaciones tanto a archivos planos como a bases de datos, ubicados en uno o más servidores, asegurando la integridad de los datos y la disponibilidad de la aplicación.

Agente: forma parte de la taxonomía del middleware. Los agentes se consideran un middleware que consta de varios componentes: entidades (objetos), medios (comunicación entre un agente y otro), y leyes (reglas sobre la coordinación de la comunicación del agente). Un agente es capaz de realizar acciones autónomas para cumplir sus objetivos de diseño. Esta adaptabilidad del agente debe ser genérico para que cubra una amplia base de estrategias. Los puntos fuertes del middleware de agentes son que los agentes pueden realizar tareas en nombre del usuario y son adaptables para cubrir una amplia gama de estrategias basadas en el entorno a su alrededor.
Fuente: Toni A. Bishop y Ramesh K. Karne. A SURVEY of MIDDLEWARE, 2003.

Archivo: entidades o secciones de entidades donde se reúnen, conservan, clasifican, ordenan, describen, seleccionan, administran y facilitan los documentos textuales, gráficos, audiovisuales y legibles por máquina, producidos por los individuos y las instituciones como resultado de sus actividades y que son utilizados por parte de la administración y para la investigación.
Fuente: Reglamento a la Ley del Sistema Nacional de Archivos Nº 7202, 2017, artículo 3.
Ejemplo: Archivo Nacional, Archivo Central o Archivo de Gestión.

Archivo Digital: consiste en la suma del repositorio digital como tal y la conjunción de personas y sistemas que han aceptado la responsabilidad de preservar la información y hacerla disponible a través del tiempo para una determinada población.
Fuente: Castillo Solano y Umaña Alpízar, 2019, p. 73.
Ejemplo: ADUNA.

Arquitectura Orientada a Servicios: se define como dos instancias computacionales (por ejemplo, programas) que interactúan de manera que una instancia ejecuta cargas de trabajo en función de la otra. Cada interacción del servicio está definida por un lenguaje de descripción, cada interacción es autocontenida y con bajo acoplamiento. Estas son independientes de otras interacciones.
Fuente: Código Nacional de Tecnologías Digitales, 2020, p. 111.
Ejemplo: Los Web Services (Servicios Web) que proporcionan una interfaz de acceso a un servicio escondiendo las particularidades de dicho servicio de modo que sea accesible desde cualquier tipo de cliente a través de protocolos estándar. (Análisis y diseño de una arquitectura SOA para una institución financiera, Mohor, 2006).

Autenticación: verificación de la identidad de un usuario, proceso o dispositivo, a menudo como un requisito previo para permitir el acceso a los recursos en un sistema de información.
Fuente: Código Nacional de Tecnologías Digitales, 2020, p. 111.
Ejemplo: usuario y contraseña, firma, reconocimiento facial, número de identificación o PIN.

Autenticación dependiente de tecnología: mecanismo que intenta establecer la autenticidad de los objetos digitales en un momento determinado.
Fuente: Digital Preservation Handbook, https://www.dpconline.org/handbook/glossary
Ejemplo: Firma Digital.

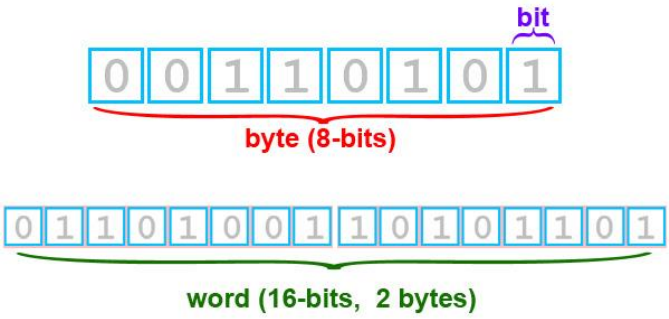
Autenticidad: consiste en acreditar que un documento de archivo es lo que pretende ser sin alteraciones ni corrupciones. Los documentos auténticos son los que han mantenido su identidad e integridad al paso del tiempo gracias a la evidencia de su carácter, requisitos o circunstancias inherentes.
Fuente: Glosario de Preservación Archivística Digital Versión 4.0, p. 24.

B

Base de datos: información relacionada que se encuentra almacenada y ordenada en estructuras especializadas que permiten a sistemas computarizados guardar, manejar y recuperar datos con rapidez.
Fuente: Coronel. C, Morris, S y Peter, R, 2011, Base de Datos: Diseño, Implementación y Administración.

Bit: es la unidad básica de información que puede tener solo uno de los dos valores comúnmente representados como 0 o 1.

Fuente: Digital Preservation Handbook, https://www.dpconline.org/handbook/glossary
Ejemplo: Los dos valores se pueden interpretar como cualquier atributo de dos valores, como podría ser: verdadero/falso, encendido/apagado, sí/no



C

Cadena de bits / Bitstream: datos contiguos o no contiguos dentro de un Fichero que presentan propiedades comunes a efectos de preservación. Una cadena de bits no puede convertirse en un fichero autónomo sin añadir una estructura de Fichero (cabeceras, etc.) ni reformatear la cadena de bits para adaptarse a un formato concreto. Esta definición es más concreta que las definiciones genéricas de cadena de bits (bitstream) que se utilizan en informática.
Fuente: Diccionario de Datos PREMIS, Versión 2.0, 2015, p. 14.

Cadena de custodia (Preservación) / chainofcustody: modelo de una secuencia o sistema de controles que se extiende sobre todo el ciclo de vida de los documentos de archivo para asegurar su identidad e integridad a lo largo del tiempo [Archivos-cadena de preservación]. Este modelo considera un sistema de administración de documentos de archivo tripartita, formado por un sistema de elaboración de documentos de archivo, un sistema de mantenimiento y un sistema de preservación.
Fuente: Glosario de Preservación Archivística Digital Versión 4.0, 2014, p. 61.

Cadena de interoperabilidad: expresión de la interoperabilidad en el despliegue de los sistemas y los servicios como una sucesión de elementos enlazados e interconectados, de forma dinámica, a través de interfaces y con proyección a las dimensiones técnica, semántica y organizativa.
Fuente: Código Nacional de Tecnologías Digitales, 2020, p. 112.

Centro de Datos: espacio físico destinado a las redes de datos.
Fuente: Código Nacional de Tecnologías Digitales, MICITT, 2020, p. 112.

Comunidad designada: un grupo identificado de usuarios potenciales que deberían poder comprender un conjunto particular de información. La comunidad designada puede estar compuesta por múltiples comunidades de usuarios.
Fuente: UNE-ISO 14721:2015, p. 21.
Ejemplo: Abogados que consultan los documentos notariales del Departamento Archivo Notarial del Archivo Nacional.

Comprobación de integridad: el proceso de usar para garantizar que el contenido digital no se haya alterado, perdido o dañado con el tiempo.
Fuente: Digital Preservation Handbook, https://www.dpconline.org/handbook/glossary
Ejemplo: Sumas de verificación (checksum) Existen herramientas que permiten comprobar la integridad del documento electrónico como Fixity y Checksum de Corv.

Confidencialidad: significa que la información solo está siendo vista o utilizada por personas que están autorizadas para acceder a ella, por tanto, se debe de suscribir el respectivo acuerdo de servicio donde se establezcan claramente las condiciones de las partes, que garanticen la confidencialidad de cualquier tipo de información que se gestione.
Fuente**:** Código Nacional de Tecnologías Digitales, 2020, p. 55.

Conversión de documentos de archivo / conversión of records: transformación de documentos de archivo digitales de un formato o versión de formato hacia otro en el curso usual y ordinario de las operaciones propias de la organización con propósitos de seguridad, prevención de desastres, mantenimiento, modernización o reducción de la obsolescencia de la tecnología, aseguramiento de la compatibilidad con diferentes generaciones o configuraciones de equipo y programas de cómputo, o para compactar la información, dejando intacta su forma intelectual.
Fuente: Glosario de Preservación Archivística Digital Versión 4.0, 2014, p. 54.
Ejemplo: Cambio de formato de archivo de un documento en .DOC a .PDF/A.

Copia auténtica / Authenticcopy: también llamada “copia certificada”, es aquella elaborada por una persona autorizada para llevar a cabo tal función, y por tanto tiene validez legal.
Fuente: Glosario de Preservación Archivística Digital Versión 4.0, 2014, p. 55.

Cuadro de Clasificación: estructura jerárquica y lógica que refleja las funciones y las actividades de una organización, así como los documentos que generan, producto de su identificación y análisis, es un sistema que organiza intelectualmente la información y reproduce las relaciones que median entre los documentos y las

agrupaciones, desde la base (la pieza simple) al nivel más amplio de agrupación (el fondo).
Fuente: Glosario único de términos, definiciones, conceptos y abreviaturas de las normas técnicas nacionales, 2020, p. 2.

Custodia: cuidado y control, especialmente para la seguridad y preservación.
Fuente: Dictionary of Archives Terminology, 2021.

D

Dato: una representación de hechos, conceptos o instrucciones de un modo formalizado, y adecuado para su comunicación, interpretación o procesamiento por medios automáticos o humanos.
Fuente: Glosario único de términos, definiciones, conceptos y abreviaturas de las normas técnicas nacionales, 2020, p. 2.

Datos abiertos: son datos disponibles en línea, sin procesar, en formato abierto, neutral e interoperable; que permite su uso y reuso, disponible para su descarga en forma completa, sin costo ni requisitos de registro y procesable en computadora.
Fuente: Decreto N° 40199-MP de Apertura de Datos Públicos.
Ejemplo: Datos de los presupuestos institucionales, su ejecución y evaluación.

Descripción de documentos: consiste en elaborar una representación exacta del documento de archivo o de sus agrupaciones, mediante la recopilación, análisis, organización y registro de la información, que sirve para identificar, localizar y explicar los documentos, así como su contexto y el sistema que los ha producido.
Fuente: Glosario único de términos, definiciones, conceptos y abreviaturas de las normas técnicas nacionales, 2020, p. 2.

Diccionario de Datos PREMIS: un estándar para metadatos de preservación digital.
Fuente: Diccionario de Datos PREMIS, Versión 2.0, 2015.

Disponibilidad: significa que la información es accesible cuando los usuarios autorizados la necesitan.
Fuente: Código Nacional de Tecnologías Digitales, 2020, p. 55.

Digitalización: forma de convertir documentos impresos o no digitales a formato digital.
Fuente: UNE-ISO 13028:2010, p. 7.

Documento electrónico con equivalencia funcional: cualquier manifestación con carácter representativo o declarativo, expresada o transmitida por un medio electrónico o informático, y se tendrá por jurídicamente equivalente a los documentos que se otorguen, residan o transmitan por medios físicos.
Fuente: Ley de Certificados, Firmas Digitales y Documentos Electrónicos Nº 8454, 2005, artículo 3.

Documento electrónico firmado digitalmente: aquel documento electrónico, cualesquiera que sean su contenido, contexto y estructura, que tiene lógicamente asociada una firma digital. En otras palabras, es un objeto conceptual que contiene tanto el documento electrónico como una firma digital, sin importar que estos dos elementos puedan encontrarse representados por conjuntos de datos diferentes.
Fuente: Política de Formatos Oficiales de los Documentos Electrónicos Firmados Digitalmente, 2013, p. 2.

E

Edición de Paquete de Información de Archivo (PIA) / (AIP edition): PIA cuya Información de Contenido o Información de Descripción de Conservación ha sido actualizada o mejorada no con la intención de conservar la información, sino para aumentarla o mejorarla. El resultado de una migración no se considera una edición de PIA.
Fuente: UNE-ISO 14721:2015, p. 25.

Emulación: uso de software (un emulador) para recrear un entorno de software y hardware obsoleto, permitiendo el acceso al contenido digital.
Fuente: Digital Preservation Handbook, https://www.dpconline.org/handbook/glossary
Ejemplo: KEEP: Keeping Emulation Environments Portable, plataforma de acceso de emulación para permitir la representación precisa de objetos digitales tanto estáticos como dinámicos: archivos de texto, sonido e imagen; documentos multimedia, sitios web, bases de datos, videojuegos, etc. Basadoen OAIS.

Entidad Funcional de Acceso (access funcional entity): Entidad funcional de OAIS que contiene los servicios y funciones que hacen que los fondos de información de archivo y los servicios relacionados sean visibles para los Usuarios.
Fuente: UNE-ISO 14721:2015, p. 22.

Entidad Funcional de Administración (Administration Functional Entity): Entidad Funcional de OAIS que consta de los servicios y funciones necesarios para

controlar el funcionamiento de las otras entidades funcionales de OAIS en su día a día.
Fuente: UNE-ISO 14721:2015, p. 22.

Entidad Funcional de Almacenamiento de Archivo (Archival Storage Functional Entity): Entidad funcional de OAIS que incluye los servicios y funciones que se utilizan para el almacenamiento y la recuperación de Paquetes de Información de Archivo.
Fuente: UNE-ISO 14721:2015, p. 22.

Entidad Funcional de Gestión de Datos (data management functional entity): Entidad funcional de OAIS que contiene los servicios y funciones para el ingreso de datos, el mantenimiento y el acceso a una amplia variedad de información. Algunos ejemplos de esta información son los catálogos e inventarios sobre lo que puede ser recuperado desde el Almacenamiento de Archivo, procesamiento de algoritmos que pueden ser realizados sobre los datos obtenidos, estadísticas de acceso por Usuario, facturación por Usuario, solicitudes basadas en eventos, controles de seguridad y calendarios de OAIS, políticas, y procedimientos.
Fuente: UNE-ISO 14721:2015, p. 22.

Entidad Funcional de Ingreso (ingest functional entity): Entidad funcional de OAIS que contiene los servicios y funciones que aceptan los Paquetes de Información de Transferencia de los Productores, prepara los Paquetes de Información de Archivo para su almacenamiento y se asegura de que estos y la Información Descriptiva de soporte se ingresen en el OAIS.
Fuente: UNE-ISO 14721:2015, p. 22.

Entidad Funcional de Planificación de la Conservación (preservation planing functional entity): Entidad funcional de OAIS que proporciona los servicios y funciones para la monitorización del entorno de OAIS y que proporciona recomendaciones y planes de conservación para asegurar que la información guardada en OAIS permanece accesible a, y comprensible por, y suficientemente utilizable por, la Comunidad Específica a Largo Plazo, incluso si el entorno informático original llega a ser obsoleto.
Fuente: UNE-ISO 14721:2015, p. 22.

Esquema de metadatos: Instrumento que define la incorporación y gestión de los metadatos de contenido, contexto y estructura de los documentos electrónicos a lo largo de su gestión.
Fuente: Código Nacional de Tecnologías Digitales, 2020, p. 114.
Ejemplo: Anexo 2: Esquema de Metadatos.

Estándar: Especificación técnica aprobada por un organismo de normalización reconocido para una aplicación repetida o continuada cuyo cumplimiento no sea obligatorio y que esté incluida en una de las categorías siguientes:
1) Norma internacional: norma adoptada por una organización internacional de normalización y puesta a disposición del público.
2) Norma nacional: norma adoptada por un organismo nacional de normalización y puesta a disposición del público.
Fuente: Código Nacional de Tecnologías Digitales, 2020, p. 114.
Ejemplo: EAD, EAC, METS.

Estándar abierto: Aquél que reúne las siguientes condiciones:
1) Es público y su utilización está disponible de manera gratuita o a un coste que no suponga una dificultad de acceso.
2) Su uso y aplicación no está condicionado por el pago de un derecho de propiedad intelectual o industrial.
Fuente: Código Nacional de Tecnologías Digitales, 2020, p. 114.
Ejemplo: Estándar ISO 26300 Information technology- Open Document Format for Office Applications.

Estrategia de preservación: Conjunto coherente de objetivos y métodos para proteger y mantener salvaguardar la autenticidad y asegurar la accesibilidad– componentes digitales e información relacionada a documentos de archivo digitales adquiridos a lo largo del tiempo, así como para poder reproducir los documentos de archivo auténticos interrelacionados y/o sus agregaciones archivísticas.
Fuente: Glosario de Preservación Archivística Digital Versión 4.0, 2014, p. 109.
Ejemplo: La conversión de formatos, la migración de sistemas, entre otras.

Expediente electrónico: Conjunto de documentos electrónicos o digitales, firmados digitalmente, ordenados cronológicamente, que son gestionados como un único objeto y almacenados en un medio electrónico que garantice que ninguno de los documentos sea alterado, eliminado o añadido.
Fuente: Glosario único de términos, definiciones, conceptos y abreviaturas de las normas técnicas nacionales, 2020, p. 3.

Evento: una acción que involucra o afecta al menos a un Objeto o Agente asociado o conocido por el repositorio de preservación.
Fuente: Data Dictionary for Preservation Metadata PREMIS 3.0.
Ejemplo: Intentos de ataques o fallos que descubren vulnerabilidades de seguridad existentes.

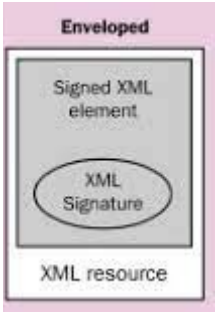
F

Fiabilidad: Representación completa y precisa de las operaciones, las actividades o los hechos de los que da testimonio y al que se puede recurrir en el curso de posteriores operaciones o actividades. Los documentos deberían ser creados en el momento, o poco después, en que tiene lugar la operación o actividad que reflejan, por individuos que dispongan de un conocimiento directo de los hechos o automáticamente por los instrumentos que se usen habitualmente para realizar las operaciones.
Fuente**:** UNE-ISO 15489:2016, p.11.

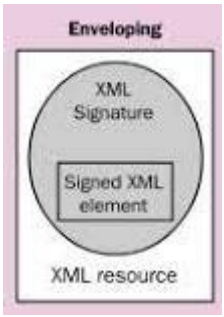
Firma digital: Conjunto de datos adjunto o lógicamente asociado a un documento electrónico, que permita verificar su integridad, así como identificar en forma unívoca y vincular jurídicamente al autor con el documento.
Fuente: Reglamento a la Ley de Certificados, Firmas Digitales y Documentos Electrónicos N° 33018, 2005, artículo 2: definiciones.

Firma digital certificada: Una firma digital que haya sido emitida al amparo de un certificado digital válido y vigente, expedido por un certificador registrado.
Fuente: Glosario único de términos, definiciones, conceptos y abreviaturas de las normas técnicas nacionales, 2020, p. 4.

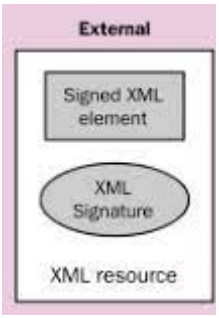
Firma envuelta (Enveloped): La firma está incluida dentro del documento y funciona en los formatos XML y PDF.
Fuente: Sánchez Martínez, 2010, Formatos de firma electrónica.
Ejemplo:



Firma envolvente (Enveloping): La firma contiene al documento.
Fuente: Sánchez Martínez, 2010, Formatos de firma electrónica.
Ejemplo:



Firma separada (Detached): La firma está separada del documento firmado.
Fuente: Sánchez Martínez, 2010, Formatos de firma electrónica.
Ejemplo:



Formato de fichero o fichero informático: codificación de un tipo de fichero que se puede representar o interpretar de una forma coherente, esperada y significativa, a través de la intervención de un determinado software o hardware que ha sido diseñado para manejar ese formato.
Fuente: UNE-ISO 13008:2013, p. 7.
Ejemplo: formatos .pdf, .odt.

Formato de difusión: formato de fichero que posibilita la reproducción o visión óptima del documento, su elección se fundamenta en la capacidad de transmitir y visualizar el documento, además de otros aspectos como la capacidad de carga, en el caso de ser utilizado por Internet.
Fuente: Observatorio Vasco de la Cultura, 2011.
Ejemplo: si el formato de preservación es PDF, un repositorio de preservación podría crear una versión de diseminación (digamos una imagen JPEG) sobre la marcha para el acceso del usuario, mientras que otro repositorio podría entregar el formato origen Un tercer repositorio podría almacenar y procesar tanto el formato origen como la copia de acceso a JPEG.

Formato de preservación: varía de acuerdo con el uso que se le vaya a dar a la información contenida en el documento, pero deben utilizarse aquellos que tengan

mayor inmunidad a la obsolescencia, tomando en cuenta la compatibilidad, popularidad, uso, mantenimiento (actualizaciones) y respaldo.
Fuente: Modelo para la preservación de documentos digitales, 2019.
Ejemplo: PDF.

G

Gobierno Abierto / Open Government Partnership: busca promover un estilo de gobernanza basado en la transparencia, la participación ciudadana y el trabajo colaborativo interinstitucional y ciudadano.
Fuente: N° 40200-MP-MEIC-MC.

H

Herramientade software: se pueden identificar dos tipos:

a. **Herramienta** cuya funcionalidad está relacionada con una acción específica dentro del proceso de preservación, como el empaquetamiento, la verificación de archivos, la captura de metadatos, etc.,

Ejemplo: DROID: Identifica formatos de archivo.

b. **Sistema de Preservación Digital (SPD)**: herramienta de software que permite llevar el control del proceso de preservación digital de acuerdo con un plan previamente establecido, por lo cual puede contemplar, dentro de sus funcionalidades, acciones específicas, como el empaquetamiento, la verificación de integridad, el monitoreo de versiones, la captura de metadatos, además de un repositorio de objetos y capacidades que permiten supervisar que estas acciones se lleven a cabo según lo planeado.

Ejemplo: RODA: Plataforma que permite la gestión del proceso de preservación digital.
Fuente: Instituto de Investigaciones Bibliográficas, 2020, Criterios básicos para valorar sistemas de preservación digital.

Identificador único: Una cadena que identifica de forma exclusiva un objeto dentro de un esquema de identificación.
Fuente: Glosario NDSA.

Información de Contenido / Content Information: Conjunto de información que es el propósito original de la conservación o que incluye parte o la totalidad de esa información. Es un Objeto de Información compuesto por su Objeto de Datos de Contenido y su Información de Representación.

Fuente: UNE-ISO 14721:2015, p. 23.

Información de Contexto / Context Information: Información que documenta las relaciones de la Información de Contenido con su entorno. Esto incluye por qué la Información de Contenido se creó y cómo se relaciona con otros objetos de Información de Contenido.
Fuente: UNE-ISO 14721:2015, p. 23.

Información de los Derechos de Acceso (Access Rights Information): Información que identifica las restricciones de acceso a la Información de Contenido, incluye el marco legal, los términos de las licencias y el control de acceso. Contiene las condiciones de acceso y consulta establecidos en el Convenio de Transferencia, relacionados tanto con la conservación (por OAIS) y con el uso final (por el Usuario). También se incluyen las especificaciones para la aplicación de las medidas de cumplimiento de los derechos.
Fuente: UNE-ISO 14721:2015, p. 23.

Información de Empaquetado / Packaging Information: La información que se utiliza para vincular e identificar los componentes de un Paquete de Información.
Fuente: UNE-ISO 14721:2015, p. 23.
Ejemplo: La información de directorio y volumen ISO 9660 utilizada en un CD-ROM para proporcionar el contenido de varios archivos que contienen Información de Contenido e Información de Descripción de Conservación.

Información de Procedencia / Provenance Information: Información que documenta la historia de la Información de Contenido. Esta información explica el origen o la fuente de la Información de Contenido, cualquier cambio que haya podido sufrir desde que se creó y quien ha tenido su custodia desde que se originó. El Archivo es responsable de crear y conservar Información de Procedencia desde el momento del Ingreso; sin embargo, la Información de Procedencia anterior debería ser proporcionada por el Productor. La Información de Procedencia se añade a la evidencia para apoyar la autenticidad.
Fuente: UNE-ISO 14721:2015, p. 23.
Ejemplo: Aplicación de Metadatos Administrativos desde la creación de los documentos.

Información de Representación / Representation Information: Información que representa un Objeto de Datos en conceptos más comprensibles.
Fuente: UNE-ISO 14721:2015, p. 23.
Ejemplo: Un ejemplo de Información de Representación para una secuencia de bits que es un fichero FITS, podría consistir en la norma FITS que define el formato más

un diccionario que define el significado en el fichero de las palabras clave que no forman parte de la norma.
Otro ejemplo es el software JPEG que se usa para reproducir un fichero JPEG; reproducir el fichero JPEG como bits no es muy significativo para las personas, pero el software, que atiende la comprensión del estándar JPEG, representa los bits en píxeles que entonces pueden ser reproducidos como una imagen para la visión humana.

Integridad: significa que cualquier cambio en la información por parte de un usuario no autorizado es imposible (o al menos detectado), y se realiza un seguimiento de los cambios realizados por usuarios autorizados; garantizando la exactitud, completitud de la información y los métodos de procesamiento.
Fuente: Código Nacional de Tecnologías Digitales, 2020, p. 55.

Interfaz: "Dispositivo o programa que habilita a un usuario a comunicarse con un computador"
Fuente: Código Nacional de Tecnologías Digitales, 2020, p. 115. Citando a Oxford (2019).
Ejemplo: Interfaces de usuario: un teclado y un ratón, interfaces físicas: los puertos USB de computadoras y consolas, interfaces lógicas: la API y el DOM.

Interoperabilidad: Habilidad de organizaciones y sistemas dispares y diversos para interactuar con objetivos consensuados y comunes, con la finalidad de obtener beneficios mutuos. La interacción implica que las organizaciones involucradas compartan información y conocimiento a través de sus procesos de negocio, mediante el intercambio de datos entre sus respectivos sistemas de tecnología de la información y las comunicaciones.
Fuente: Código Nacional de Tecnologías Digitales, 2020, p. 73. Citando a Criado, Gascó y Jiménez, 2010.

Interoperabilidad organizativa: Aborda la definición de los objetivos de procesos y servicios de las organizaciones implicadas en la prestación de servicios telemáticos o de iniciativas de cooperación e integración de back offices. Específicamente, hace referencia a la colaboración de organizaciones que desean intercambiar información manteniendo diferentes estructuras internas de gobierno y procesos de negocio variados. La interoperabilidad organizativa asegura la coordinación y el alineamiento de los procedimientos administrativos que intervienen en la provisión de los servicios de Gobierno Electrónico. En la práctica, ello implica definir de manera colaborativa el por qué y el cuándo de los intercambios de información, las normas y reglas que garantizarán la seguridad en dichos intercambios o los planes que guiarán la implantación de las iniciativas.

Fuente: Código Nacional de Tecnologías Digitales, 2020, p. 115. Citando a Criado, Gascó y Jiménez, 2010.

Interoperabilidad semántica: Se ocupa del significado en el uso de los datos y la información y, en concreto, garantiza que el significado preciso de la información intercambiada pueda ser entendido por cualquier aplicación. Para ello, habilita a los sistemas para combinar la información proveniente de otras fuentes y para procesarla de una manera integrada y con el sentido adecuado.
Fuente: Código Nacional de Tecnologías Digitales, 2020, p. 116. Citando a Criado, Gascó y Jiménez, 2010.
Ejemplo: Sistemas de clasificación, los tesauros, los metadatos y las ontologías.

Interoperabilidad técnica: Se refiere a aquellas cuestiones técnicas que garantizan que los componentes tecnológicos de los sistemas de información de las entidades participantes estén preparados para colaborar con los demás. Permite, por tanto, proporcionar mecanismos comunes de transferencia de datos y de invocación de funciones, transparentes al sustrato de redes y sistemas informáticos existentes.
Fuente: Código Nacional de Tecnologías Digitales, 2020, p. 55. Citando a Criado, Gascó y Jiménez, 2010.
Ejemplo: Interfaces, servicios de interconexión, integración de datos, middleware, presentación e intercambio de datos, accesibilidad o servicios de seguridad.

L

Lenguaje marcado: Un sistema de codificación legible por máquina, así como sus reglas asociadas, que son utilizados para describir la estructura lógica, distribución, forma de despliegue y estilo de un cierto documento digital.
Fuente: Glosario de Preservación Archivística Digital Versión 4.0, 2014, p. 143.
Ejemplo: Lenguaje XML.

Lista de verificación: instrumento que contiene criterios o indicadores a partir de los cuales se miden y evalúan las características del objeto, comprobando si cumple con los atributos establecidos. La lista de verificación se utiliza básicamente en la práctica de la investigación que forma parte del proceso de evaluación.
Fuente: Glosario básico de evaluación, 2013.

M

Marco de evaluación: referente en el cual se fundamenta una decisión con el que culmina un proceso evaluativo, su objetivo es clasificar por niveles de competencia a los sujetos evaluados.

Fuente: Diccionario de términos clave ELE.

Medios de almacenamiento: Dispositivos que almacenan el contenido digital.
Fuente: Digital Preservation Handbook, https://www.dpconline.org/handbook/glossary
Ejemplo: memoria de acceso aleatorio (RAM), Unidades de discos duros y discos de estado sólido.

Metadato: información que caracteriza o describe a otro recurso de información, especialmente con el propósito de documentar, describir, preservar o administrar ese recurso.
Fuente: Código Nacional de Tecnologías Digitales, 2020, p. 116.
Ejemplo: Metadatos administrativos, descriptivos y estructurales.

Metadatos administrativos: Describen la procedencia de un objeto digital, los procesos realizados para su creación, sus características técnicas, sus condiciones de acceso y derechos de propiedad intelectual, y las acciones previstas para su preservación.
Fuente: Diccionario de Datos PREMIS, Versión 2.0, 2015, p. 238.
Ejemplo: Las fechas de creación o adquisición, los permisos de acceso, derechos o procedencia.

Metadatos descriptivos: Metadatos que ayudan a la recuperación (cómo encontrar un recurso), la identificación (cómo distinguir un recurso de otros) y la selección (cómo establecer si un recurso responde a una determinada necesidad. Por ejemplo, la versión en DVD de una grabación en vídeo). (Traducción de un extracto de Caplan, Metadata Fundamentals for All Librarians, ALA Editions, 2003)
Fuente: Diccionario de Datos PREMIS, Versión 2.0, 2015, p. 238.
Ejemplo: título, autor, fechas, firmas.

Metadatos estructurales: Reflejan la estructura interna de los recursos digitales y las relaciones entre sus partes. Se utilizan para permitir la navegación y la presentación. (Traducción de un extracto de la NINCH Guide to Good Practice.
Fuente: Diccionario de Datos PREMIS, Versión 2.0, 2015, p. 238.
Ejemplo: Datos de los capítulos, la tabla de contenido o los detalles del diseño de la página se consideran metadatos estructurales.

Metadatos de preservación: Información contextual necesaria para llevar a cabo, documentar y evaluar los procesos que apoyan la retención y accesibilidad a largo plazo de los contenidos digitales. Los metadatos de preservación documentan los procesos técnicos asociados con la preservación, especifican la información de

gestión de derechos, establecen la autenticidad del contenido digital y registran la cadena de custodia y procedencia de un objeto digital.
Fuente: Glosario NDSA.

METS: Estándar de Transmisión y Codificación de Metadatos, un estándar para presentar metadatos mediante XML.
Fuente: Estándar de codificación y transmisión de metadatos METS.

Migración: Un medio para superar la obsolescencia técnica mediante la transferencia de recursos digitales de una generación de hardware / software a la siguiente. El propósito de la migración es preservar el contenido intelectual de los objetos digitales y mantener la capacidad de los clientes para recuperarlos, mostrarlos y utilizarlos de otro modo frente a la tecnología en constante cambio.
Fuente: Beagrie, Neil y Jones, Maggie, 2001, Preservation Management of Digital Materials: A Handbook, (The British Library: Londres)/ Glosario DCC.

Modelo de madurez: una herramienta que permita comparar las capacidades de preservación digital con niveles de buenas prácticas. El uso de un modelo de madurez ayuda a monitorear el progreso y planificar desarrollos futuros.
Fuente: Digital Preservation Handbook, https://www.dpconline.org/handbook/glossary.
Ejemplo: DPC-RAM.

N

Nacido digital: materiales digitales que no están destinados a tener un equivalente analógico, ya sea como fuente de origen o como resultado de la conversión a forma analógica.
Fuente: Digital Preservation Handbook, https://www.dpconline.org/handbook/glossary
Ejemplo: documentos generados, gestionados y almacenados en Sistemas de Gestión de Documentos Electrónicos.

Neutralidad tecnológica: independencia en la elección de las alternativas tecnológicas escogidas por los oferentes e interesados, para lo cual se deben emplear estándares abiertos o de uso generalizado (v. gr. software libre o de código abierto).
Fuente: Código Nacional de Tecnologías Digitales, 2020, p. 116.

No propietario: se llama así a las tecnologías de equipo, programas y aplicaciones de cómputo y/o formatos de archivos que no se encuentran protegidos por una

patente o marca o que no son poseídos ni controlados por una sola compañía o institución, o cuyo uso es permitido bajo esquemas de acceso abierto.
Fuente: Glosario de Preservación Archivística Digital Versión 4.0, 2014, p. 157.
Ejemplo: el formato word office perteneciente a la empresa Microsoft.

No repudio: la capacidad de un servicio de seguridad digital de certificar que un cierto mensaje transferido ha sido enviado y recibido por las partes que dicen ser, ofreciendo prueba de la integridad y origen del mensaje y sus datos, en una forma no falsificable que puede ser verificada por cada una de las partes en cualquier momento.
Fuente: Glosario de Preservación Archivística Digital Versión 4.0, 2014, p. 158.
Ejemplo: imposibilidad de una persona física o jurídica de negar la autoridad de un documento firmado digitalmente.

O

Objeto de datos: ya sea un objeto físico o un objeto digital.
Fuente: UNE-ISO 14721:2015, p. 24.

Objeto de datos de contenido: el objeto de datos, que, junto con la información de representación asociada, es el objetivo original de preservación.
Fuente: UNE-ISO 14721:2015, p. 24.

Objeto de información: un objeto de datos junto con su información de representación.
Fuente: UNE-ISO 14721:2015, p. 24.

Objeto digital: objeto compuesto por un conjunto de secuencias de bits.
Fuente: UNE-ISO 14721:2015, p. 24.
Ejemplo: Un documento de texto codificado o una imagen digitalizada.

Obsolescencia: estado de un equipo, programa o estructura que ya se considera anticuado, poco adecuado a las circunstancias actuales, que ha caído en desuso o está cerca de ello.
Fuente: Glosario de Preservación Archivística Digital Versión 4.0, 2014, p. 163.

P

PAdes: PDF Advanced Electronic Signature, Para documentos en formatos PDF y sus formatos extendidos.

Fuente: Política de Formatos Oficiales de los Documentos Electrónicos Firmados Digitalmente, 2013, p. 6.

Paquete: cualquier contenedor arbitrario de datos digitales.
Fuente: Glosario del Curso del Digital Preservation Coalition.

Paquete de información: contenedor lógico compuesto por la Información de Contenido opcional y la Información de Descripción de Conservación opcional asociada. Relacionada con este Paquete de Información, la Información del Empaquetado, se usa para delimitar e identificar la Información de Contenido y la Información de Descripción del Paquete usada para facilitar búsquedas de la Información de Contenido.
Fuente: UNE-ISO 14721:2015, p. 25.

Paquete de Información de Archivo (PIA) / (AIP): Paquete de Información, que se conserva en un OAIS, y que consta de la Información de Contenido y de la Información de Descripción de Conservación (IDC) asociada.
Fuente: UNE-ISO 14721:2015, p. 25.

Paquete de Información de Consulta (PID) / (DIP): Un Paquete de Información, derivado de uno o más API, y enviado por el Archivo al Usuario en respuesta a su solicitud al OAIS.
Fuente: UNE-ISO 14721:2015, p. 25.

Paquete de Información de Transferencia (PIT) / (SIP): Paquete de Información que se entrega por el Productor al OAIS para usarlo en la construcción o actualización de uno o más API y/o la Información de Descripción asociada.
Fuente: UNE-ISO 14721:2015, p. 25.

Persistencia: en informática hay varios ámbitos donde se aplica y se entiende la persistencia:

a. la capacidad del sistema para guardar la información.
b. En la programación orientada a objetos, los objetos deben poder permanecer, si así se desea, después de la ejecución de un programa.

Fuente: glosarioit.com

Plan de continuidad del negocio: procedimientos documentados que sirven de guía a una organización para resolver una disrupción y recuperar y restablecer un nivel predefinidos de actividades tras ella.
Fuente: UNE-EN ISO 22300:2020, p. 10.

Plan Estratégico de Preservación: documento escrito, sancionado por el administrador del Archivo Digital, que fija las metas y objetivos para alcanzar la parte de la misión del Archivo Digital concerniente con la preservación. Los Planes Estratégicos de Preservación pueden incluir planes a largo y a corto plazo.
Fuente: UNE-ISO 16363:2017, p. 18.

Plan de seguridad: medidas planificadas para garantizar que la seguridad se gestiona de manera adecuada.
Fuente: UNE-EN ISO 22300:2020, p. 37.

Plataforma informática: Una plataforma es un conjunto de tecnologías que se utilizan como base sobre la que se desarrollan otras aplicaciones, procesos o tecnologías.
Fuente: Techopedia Inc. https://www.techopedia.com/definition/3411/platform-computing

---

Política archivística: conjunto de orientaciones o directrices para producir y gestionar documentos auténticos, fiables y utilizables, capaces de sostener las funciones y actividades de las organizaciones y de los individuos durante tanto tiempo como sea necesario, y de servir como memoria y fuente para la historia. Incluye el establecimiento de un marco normativo, así como la dotación de los medios materiales y humanos necesarios para el desarrollo. La política archivística debe ser adoptada al más alto nivel de decisión y promulgada, comunicada e implementada en todos los niveles de una organización.
Fuente: Reglamento a la Ley del Sistema Nacional de Archivos N° 40554 -C, 2017, artículo 1: glosario.

Política de Gestión de Documentos Electrónicos: orientaciones o directrices que define una organización para la creación y gestión de documentos auténticos, fiables y disponibles a lo largo del tiempo, de acuerdo con las funciones y actividades que le son propias. La política se aprueba al más alto nivel dentro de la organización, y asigna responsabilidades en cuanto a la coordinación, aplicación, supervisión y gestión del programa de tratamiento de los documentos a través de su ciclo de vida, de acuerdo con las políticas establecidas por el Archivo Nacional.
Fuente: Código Nacional de Tecnologías Digitales, 2020, p. 117.

Política de Preservación Digital: documento escrito, sancionado por el administrador del Archivo Digital, que describe el enfoque que toma el archivo para la preservación de los objetos introducidos en él. La Política de Preservación es consistente con el Plan Estratégico de Preservación.
Fuente: UNE-ISO 16363:2017, p. 18.

Preservación: la totalidad de principios, políticas, reglas y estrategias destinadas a prolongar la existencia de un objeto manteniéndolo en una condición adecuada para su uso, ya sea en su formato original o en otro más persistente, dejando intacta la forma intelectual del objeto.
Fuente: Glosario de Preservación Archivística Digital Versión 4.0, 2014, p. 173.

Preservación 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.
Fuente: Glosario de Preservación Archivística Digital Versión 4.0, 2014, p. 173.

Procedencia: las relaciones entre los documentos de archivo y las organizaciones o individuos que los producen acumulan y usan en el transcurso de sus actividades personales o corporativas.
Fuente: Glosario de Preservación Archivística Digital Versión 4.0, 2014, p. 178.

Procedimiento: 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.
Fuente: Glosario de Preservación Archivística Digital Versión 4.0, 2014, p. 178.

Productor: el papel que juegan aquellas personas o sistemas clientes que proporcionan la información para ser preservada. Puede incluir otros OAIS o personas o sistemas internos de OAIS.
Fuente: UNE-ISO 14721:2015, p. 25.

PRONOM: sistema de información en línea sobre formatos de archivos, productos de software y otros componentes técnicos necesarios para respaldar el acceso a los objetos digitales a largo plazo.
Fuente: National Archives, https://www.nationalarchives.gov.uk/PRONOM/

Propiedades significativas: características de un objeto de información que deben ser mantenidas a lo largo del tiempo para asegurar su acceso continuado, uso, significación y su capacidad de ser aceptado como evidencia de lo que pretende ser como documento de archivo.
Fuente: Glosario de Preservación Archivística Digital Versión 4.0, 2014, p. 181.
Ejemplo: fecha de creación, formato, cantidad de caracteres.

Propietario: régimen de uso de los programas, formatos, estructuras y otras herramientas que están protegidas bajo una patente u otro registro de propiedad industrial, que pertenecen a una empresa u organización y cuyo uso y licenciamiento

está restringido, por lo general bajo pago de derechos, y cuya fuente o tecnología no está disponible al público y no puede ser modificada.
Fuente: Glosario de Preservación Archivística Digital Versión 4.0, 2014, p. 180.

Protección de datos: es el proceso de proteger la información importante de la corrupción y/o pérdida.
Fuente: Código Nacional de Tecnologías Digitales, 2020, p. 117.

Protocolo de recuperación: los procesos y procedimientos de recuperación que se ejecutan y se mantienen para asegurar la restauración de los sistemas o activos afectados por incidentes de seguridad informática.
Fuente: Código Nacional de Tecnologías Digitales, 2020, p. 62.

Protocolo de Transferencia: documento de carácter obligatorio, que trabajará en conjunto la instancia productora y el Archivo Institucional. Implementa el mecanismo que establece las condiciones y los requisitos para la transferencia de los documentos al repositorio.
Fuente: Castillo Solano y Umaña Alpízar, 2019, p. 181.
Ejemplo: en un protocolo de transferencia se define el alcance, formas de transferencia, estructura del SIP, formatos de fichero admitidos, esquema de metadatos, mecanismos de control y validaciones, derechos para realizar acciones de preservación sobre los documentos, plazo de conservación, propiedades significativas coleccionables, derechos de uso y acceso, fecha de vigencia del protocolo.

Pull: método de transferencia en que la solución cuenta con un agente de middleware que sale y recoge el material.
Fuente: Castillo Solano y Umaña Alpízar, 2019, p. 170.

Push: método de transferencia donde el SIP se entrega en la solución para su procesamiento por parte del sistema u organismo productor original.
Fuente: Castillo Solano y Umaña Alpízar, 2019, p. 170.

R

Reempaquetado (repackaging): migración Digital en la que se produce una modificación en la Información del Empaquetado del AIP.
Fuente: UNE-ISO 14721:2015, p. 26.

Refrescamiento/Recopiado (refreshment): migración Digital cuyo efecto es sustituir una instancia de soporte con una copia que sea adecuadamente exacta para

que todo el hardware y software de Almacenamiento de Archivo siga funcionando como antes.
Fuente: UNE-ISO 14721:2015, p. 26.

Repositorio Archivístico Digital Confiable: es un repositorio digital que almacena y gestiona documentos de archivo durante su gestión. Como tal, un Repositorio Digital Confiable debería: 1. administrar documentos y metadatos de acuerdo con las prácticas y estándares de archivo, específicamente relacionados con la gestión, descripción y preservación de documentos de archivo y salvaguardar sus características del documento de archivo, en particular la autenticidad (identidad e integridad).
Fuente: Flores Daniel, 2020, Los Repositorios Archivísticos Digitales Confiables - RDC-Arch como ambiente de Preservación y garantía de la Autenticidad, Confiabilidad y manutención de la Cadena de Custodia, slide 53.

Repositorio electrónico: archivo centralizado donde se almacenan y administran datos y documentos electrónicos, junto con sus metadatos.
Fuente: Código Nacional de Tecnologías Digitales, 2020, p. 118.

Respaldo / backup: es una copia de un archivo de datos hecha con el fin de recuperarlo en caso de falla dentro de un sistema.
Fuente: Glosario de Preservación Archivística Digital Versión 4.0, 2014, p. 191.
Ejemplo: duplicación de un conjunto de datos a una base de datos en una ubicación alterna.

Restricciones de acceso: también llamado acceso restringido. Autoridad especial otorgada a una persona, oficial, puesto u oficina dentro de una organización o dependencia para leer un documento de archivo.
Fuente: Glosario de Preservación Archivística Digital Versión 4.0, 2014, p. 191.
Ejemplo: autorización conferida por la Ley General de Administración Pública a las partes involucradas y sus representantes legales o cualquier abogado de leer y copiar partes de un expediente de procedimiento administrativo.

S

Seguridad de la información: consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.
Fuente: Código Nacional de Tecnologías Digitales, 2020, p. 118.

Seguridad informática: conjunto de herramientas, procedimientos y estrategias que tienen como objetivo garantizar la integridad, disponibilidad y confidencialidad de la información de una entidad en un sistema.
Fuente: Código Nacional de Tecnologías Digitales, 2020, p. 118.

Sello de tiempo: certificación de un tercero confiable de que un cierto documento de archivo fue recibido en una fecha y/o horas determinadas.
Fuente: Glosario de Preservación Archivística Digital Versión 4.0, 2014, p. 194.

Sistemas de Gestión de Bases de Datos (SGBD): consiste en una colección de datos interrelacionados y un conjunto de programas para acceder a dichos datos. Su objetivo principal es proporcionar una forma de almacenar y recuperar la información de base de datos de manera que sea tanto práctica como eficiente.
Fuente: Silberschatz, A, 2006, Fundamentos de las bases de datos. 5ta ed. Madrid: MacGraw-Hil.
Ejemplo: Microsoft Access, MySQL, Oracle Database, entre otros.

Sistema de Gestión de Documentos Electrónicos de Archivo (SGDEA): herramienta informática destinada a la gestión de documentos electrónicos de archivo. También se puede utilizar en la gestión de documentos de archivo tradicionales. El sistema debe encargarse de aplicar los procesos de la gestión documental, producción, gestión y trámite, organización, transferencia, disposición, preservación a largo plazo y valoración; esto se realiza mediante flujos de trabajo, gestión de contenidos, clasificación documental, conformación de expedientes entre otras, aplicando funciones sobre las entidades y capturando metadatos.
Fuente: Archivo General de la Nación Colombia.

Sistema de Información de Archivo Abierto (OAIS): marco conceptual que describe el entorno, los componentes funcionales y los objetos de información asociados con un sistema responsable de la preservación a largo plazo. Como modelo de referencia, su propósito principal es proporcionar un conjunto común de conceptos y definiciones que puedan ayudar a la discusión entre sectores y grupos profesionales y facilitar la especificación de archivos y sistemas de preservación digital. La abreviatura OAIS también se usa comúnmente para referirse al estándar del modelo de referencia del Sistema de Información de Archivo Abierto que definió el término.
Fuente: UNE-ISO 14721:2015, p. 27.

Sistema de preservación de documentos de archivo: conjunto de principios, políticas, reglas y estrategias, así como las herramientas y mecanismos utilizados para implementarlas y que han sido adoptadas por una institución o programa archivísticos, para mantener a largo plazo los componentes digitales y su información relacionada así como para reproducir documentos de archivo auténticos y/o

agregaciones de ellos que hayan sido producidos mediante la interpretación de controles externos, aplicando éstos últimos a los documentos de archivo seleccionados para su preservación.
Fuente: Glosario de Preservación Archivística Digital Versión 4.0, 2014, p. 200.

Sistema datacéntrico: sistema basado en el uso de datos a través de sus relaciones. La información depende del sistema que lo creó.
Fuente: Código Nacional de Tecnologías Digitales, 2020, p. 119.
Ejemplo: Sistema de Pagos Integra del Ministerio de Hacienda.

Sistema docucéntrico: sistema basado en el uso de documentos electrónicos, para su gestión, clasificación, preservación.
Fuente: Código Nacional de Tecnologías Digitales, MICITT, p. 119.

Software de acceso (Access software): tipo de software que presenta parte o todo el contenido de información de un Objeto de Información en formas comprensibles para las personas o los sistemas.
Fuente: UNE-ISO 14721:2015, p. 27.

Solución de preservación digital: herramienta de software y la plataforma tecnológica en donde se ejecuta el proceso de preservación digital.
Fuente: Elaboración propia.

Suma de verificación / Checksum: es una cadena de caracteres que se relacionan con un objeto digital y que actúan como firma o huella digital única del objeto. Las sumas de verificación se pueden utilizar para comprobar la integridad de un objeto digital mediante la comparación de la suma de verificación a lo largo del tiempo. Se usa para comparar copias.
Fuente: Digital Preservation Handbook, https://www.dpconline.org/handbook/glossary
Ejemplo: el checksum MD5 para la frase “thisis a test” o “esto es una prueba” es 120EA8A25E5D487BF68B5F7096440019. Se trata de una larga cadena de caracteres representando dicha oración.

T

Tablas de Control de Acceso: son el instrumento archivístico que permite identificar condiciones de acceso, uso y restricciones que aplican a los documentos de archivo, ya sean producidos física o electrónicamente de acuerdo con las normas tanto internas como externas que afecten el acceso a los documentos.

Fuente: Guía de Implementación de un Sistema de Gestión de Documentos Electrónicos de Archivo, 2017, p. 56.

Tabla de Plazos de Conservación: instrumento en el que constan todas las series y tipos documentales producidos o recibidos en una oficina o institución, en el cual se anotan todas sus características y se fija el valor administrativo y legal.
Fuente: Glosario único de términos, definiciones, conceptos y abreviaturas de las normas técnicas nacionales, 2020, p. 7.

U

Usuario: el papel que juegan aquellas personas, o sistemas, que interactúan con los servicios que brinda el archivo digital para encontrar información de interés preservada y acceder a esa información en detalle.
Fuente: UNE-ISO 14721:2015, p. 27.

V

Valor hash: ver suma de verificación
Fuente: Digital Preservation Handbook, https://www.dpconline.org/handbook/glossary

---

Verificación de firma: con relación a la firma digital, significa determinar con precisión: (1) que la firma ha sido creada durante el período operacional de un certificado válido, utilizando la llave pública listada en el certificado; y, (2) que el mensaje no ha sido alterado desde que la firma fue creada.
Fuente: Reglamento a la Ley de Certificados, Firmas Digitales y Documentos Electrónicos N° 33018, 2005, artículo 2: definiciones.

Versión AIP: un atributo de un AIP cuyo contenido de información ha sufrido una transformación en un AIP de origen y es un candidato para reemplazar el AIP de origen. El resultado de una Migración Digital se considera una versión de AIP.
Fuente: UNE-ISO 14721:2015, p. 27.

X

XAdES: XML Advanced Electronic Signature, para documentos en formatos XML. Se recomienda para el desarrollo de soluciones informáticas en donde sea necesaria la interoperabilidad con otras instituciones.

Fuente: Política de Formatos Oficiales de los Documentos Electrónicos Firmados Digitalmente, 2013, p. 6.

XML: acrónimo de “Extensible Markup Language” o “Lenguaje de Marcado Extendido".
Fuente: Glosario de Preservación Archivística Digital Versión 4.0, 2014, p. 223.

Anexo Nº 2: Esquema de Metadatos

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
1	ICA	ISAAR-CPF/EAC	Abreviatura	Abbreviation	Identificar un tesauro, vocabulario controlado u otra norma utilizada en la elaboración de la descripción	El valor debe ser seleccionado de una lista autorizada de códigos	<conventionDeclaration> <abbreviation>UCR</abbreviation> <citation>UCR (Universidad de Costa Rica)</citation> <conventionDeclaration>	SI	SI	NO	
2	ICA	ISAAR-CPF/EAC	Resumen histórico o biográfico	Abstract	Ayudar al lector a identificar rápidamente la entidad descrita	Resumen en texto libre, según información consignada en la historia de la institución o biografía de la persona. Máximo 150 caracteres	<biogHist> <abstract>Creada el 7 de marzo de 1941, con el propósito de contribuir a la formación de investigadores, docentes y profesionales con excelencia académica, visión humanista y responsabilidad social.</abstract> <biogHist>	SI	SI	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
3	ICA	ISAAR-CPF/EAC	Una dirección postal o de otro tipo	Address	Proporcionar la información completa o suficiente para identificar una dirección postal o de otro tipo relacionada con la entidad que se describe	Se redacta en texto libre, según la dirección oficial. Máximo 100 caracteres	<address> <addressLinelocalType "provincia"> San José </addressLine> <addressLinelocalType "cantón"> Montes de Oca </addressLine> <addressLinelocalType "distrito"> San Pedro </addressLine> <adrressLinelocalType "código postal"> 11501 </addressLine> </address>	SI	SI	SI	
4	ICA	ISAAR-CPF/EAC	Línea de dirección	Address Line	Registrar una o varias líneas de una dirección postal o de otro tipo	Se redacta en texto libre, según la dirección oficial. Máximo 100 caracteres		NO	NO	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
5	ICA	ISAAR-CPF/EAC	El código que representa la institución o servicio responsable de la creación, mantenimiento y/o difusión de la instancia EAC-CPF	Agency Code	proporciona un código que representa la institución o servicio responsable de la creación, mantenimiento y/o difusión de la instancia EAC-CPF	A partir de la guía de fondos se pueden codificar las instituciones pertenecientes al SNA. Máximo 35 caracteres	<agencyCode>506-291</agencyCode>	SI	NO	SI	
6	ICA	ISAAR-CPF/EAC	El nombre de la institución o servicio responsable	Agency Name	Proporcionar el nombre de la institución o servicio responsable de la creación, mantenimiento y/o difusión de la instancia EAC-CPF	Redactado a partir de texto libre, según nombre oficial de la entidad o persona	<agencyName> Universidad de Costa Rica </agencyName>	SI	SI	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
7	ICA	ISAAR-CPF/EAC	El agente (humano o máquina) responsable de un evento en el mantenimiento de la instancia EAC-CPF.	Agent	Facilitar el nombre del agente responsable de dicho evento	El metadato se genera a partir del nombre de usuario de la persona a cargo de un evento	<maintenanceEvent> <eventType> created </evenType> <evenDateTime> 2018-09-28 </evenDateTime> <agentType> human </agentType> <agent> Pérez Gómez, J </agent> </maintenanceEvent>	SI	SI	SI	
8	ICA	ISAAR-CPF/EAC	El tipo de agente responsable de un evento de mantenimiento de la instancia EAC-CPF.	AgentType	Indicar si es humano o máquina	Máximo 8 caracteres donde se indica el tipo de agente		SI	SI	SI	
9	ICA	ISAAR-CPF/EAC	Se refiere a una forma alternativa	AlternativeForm	Indicar formas alternativas o no autorizadas del nombre	Se ingresa en texto libre, a partir de otros nombres por lo que es conocida la entidad o persona	<alternativeForm>ucr</alternativeForm>	SI	SI	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
10	ICA	ISAAR-CPF/EAC	Conjunto alternativo, contiene dos o más registros de autoridad, derivados de dos o más sistemas de autoridades, expresados en una sola instancia EAC-CPF	AlternativeSet	Permite incluir diferentes descripciones de la misma entidad dentro de una sola instancia EAC-CPF	Texto libre	<alternativeSet> <setComponentxlink:href="https://archivo.ucr.ac.cr/aurol.html" xlink:type="simple"> <componentEntry>Archivo Universitario Rafael ObregónLoría</componentEntry> </setComponent> </alternativeSet>	NO	NO	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
11	ICA	ISAAR-CPF/EAC	El nombre de una entidad EAC-CPF, tal como está construido en los elementos <nameEntry> o <nameEntryParallel>, puede ser la forma autorizada del nombre de acuerdo con unas reglas o convenciones concretas, o bien una forma alternativa o no autorizada según otras reglas.	AuthorizedForm	Califica los nombres que figuran como puntos de acceso autorizados	En texto libre, pueden ser abreviaturas o siglas consignadas en algún documento oficial	<authorizedForm>Universidad de Costa Rica</authorizedForm>	NO	SI	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
12	ICA	ISAAR-CPF/EAC	Nota histórica o biográfica	BiogHist	Mostrar detalles significativos sobre la historia administrativa de una institución, o sobre la vida de una persona o familia.	Texto libre	<biogHist> <abstract>Creada el 7 de marzo de 1941, con el propósito de contribuir a la formación de investigadores, docentes y profesionales con excelencia académica, visión humanista y responsabilidad social.</abstract> <biogHist>	SI	SI	NO	
13	ICA	ISAAR-CPF/EAC	Ítemcronológico	ChronItem	Mostrar una fecha o rango de fechas emparejado con un evento asociado y un lugar opcional, dentro de un <chronList> (Lista cronológica).	Alfanumérico AAAA-MM-DD	<chronItem> <date standardDate="1974">1974</date> <event> Creación de la Vicerrectoría de Acción Social. </event> </chronItem>	SI	SI	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
14	ICA	ISAAR-CPF/EAC	Una lista cronológica estructurada de eventos, fechas, lugares, que puede utilizarse dentro del elemento <biogHist>	ChronList	Comprende una lista estructurada secuencialmente de eventos significativos de la vida de la persona o de la existencia de la familia o institución que se describe en la instancia EAC-CPF	Texto libre	<chronList> <chronItem> <date standardDate="1974">1974</date> <event>Creación de la Vicerrectoría de Acción Social. </event> </chronItem> <chronItem> <dateRange> <fromDatestandardDate="1980">1980</fromDate> <toDatestandardDate="1989">1989</toDate> <event> se crean 11 unidades de investigación </event> </dateRange> </chronItem> </chronList>	NO	NO	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
15	ICA	ISAAR-CPF/EAC	Elemento de enlace que cita un recurso externo.	Citation	Proporcionar datos descriptivos que no se darían de otra manera en la instancia EAC-CPF, como un documento original que establece la regulación de una institución	Texto libre	<conventionDeclaration> <abbreviation> ISAD (G) </abbreviation> <citation> General International Standard Archival Description </citation> </conventionDeclaration>	SI	SI	NO	
16	ICA	ISAAR-CPF/EAC	La entrada de componente proporciona identificación y acceso a un recurso vinculado.	ComponentEntry	Proporcionar un lugar en que se puede describir un registro de autoridad alternativo, o bien explicarlo en relación con los otros registros de autoridad.	Texto libre	<componentEntry> Archivo Universitario Rafael Obregón Loría</componentEntry>	NO	NO	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
17	ICA	ISAAR-CPF/EAC	Contiene información de control sobre su identidad, creación, mantenimiento, estado, y sobre las reglas y autoridades utilizadas en la elaboración de la descripción.	Control	Contiene la información necesaria para controlar la instancia EAC-CPF	Este metadato se genera de forma automática, según el evento llevado a cabo	<control> <recordId>ucr-eac.cpf-68895</recordId> <maintenanceStatus>revisado</maintenanceStatus> <publicationStatus>aprobado</publicationStatus> <maintenanceAgency> <agencyCode>506-291</agencyCode> <agencyName>Universidad de Costa Rica</agencyName> </maintenanceAgency> <LanguageDeclaration> <Language languageCode="spa"></language> <script scriptCode="Latn"></Script> </LanguageDeclaration> </control>	SI	SI	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
18	ICA	ISAAR-CPF/EAC	Declaración de convención. Una declaración de las reglas, incluye vocabularios controlados y tesauros autorizados), aplicadas en la creación de la instancia EAC-CPF.	ConventionDeclaration	Utilizado para declarar, en el elemento <citation> (Cita), referencias a cualquier regla	Texto libre	<conventionDeclaration> <citation>ISO 8601 - Elementos de datos y formatos de intercambio — Intercambio de información Representación de fechas y horas</citation> </conventionDeclaration>	SI	SI	SI	
19	ICA	ISAAR-CPF/EAC	Descripción de institución, persona o familia. Contiene la descripción de una identidad. Normalmenteuna entidadtiene unaidentidad.	CpfDescription	Proporcionar información contextual de la entidad que se describe, incluyendo la relación de esa entidad con otras entidades, recursos y funciones.	Texto libre	<cpfDescription> <identity>[...]</identity> <description>[...]</description> <relations>[...]</relations> </cpfDescription>	SI	SI	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
20	ICA	ISAAR-CPF/EAC	Una institución, persona o familia relacionada con la entidad descrita.	CpfRelation	Describir una persona, familia o institución relacionada con la estancia descrita	Texto libre	<cpfRelationcpfRelationType="Jerárquica"> <relationEntry>Instittución superior</relationEntry> <dateRange> <fromDatestandardDate="1975">1975</fromDate> <toDatestandardDate="actualidad">actualidad</toDate> </dateRange> </cpfRelation>	SI	SI	SI	
21	ICA	ISAAR-CPF/EAC	La fecha única de un evento en la historia de (o de una relación con) la institución, persona o familia descrita en la instancia EAC-CPF	Date	Expresar la fecha de algún evento histórico	Alfanumérico AAAA-MM-DD	<date standardDate="1940-08-29">August 29, 1940</date>	SI	SI	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
22	ICA	ISAAR-CPF/EAC	El rango de fechas de un evento en la historia de (o de una relación con) la institución, persona o familia descrita en la instancia EAC-CPF.	DateRange	Mostrar un rango de fechas	Alfanumérico AAAA-MM-DD	<dateRange> <fromDatestandardDate="1980">1980</fromDate> <toDatestandardDate="1989">1989</toDate> </dateRange>	SI	SI	SI	
23	ICA	ISAAR-CPF/EAC	Agrupación de un conjunto de fechas	DateSet	Facilitar expresiones complejas de fechas, al combinar un conjunto que comprende fechas únicas y rangos de fechas, múltiples fechas únicas o múltiples rangos de fechas.	Alfanumérico AAAA-MM-DD	<dateSet> <dateRange> <fromDatestandardDate="1956">1956</fromDate> <toDatestandardDate="1957">1957</toDate> </dateRange> <dateRange> <fromDatestandardDate="1980">1980</fromDate> <toDatestandardDate="1989">1989</toDate> </dateRange></dateSet	SI	SI	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
24	ICA	ISAAR-CPF/EAC	Elemento contenedor de todos los elementos de contenido relativos a la descripción	Description	Registrar información descriptiva de manera estructurada o no, o bien combinando ambos enfoques	Texto libre	<description> <existDates> <dateRange> <fromDatestandardDate="1941-03-07">1941-03-07 </from <toDateStandardDate="actualidad">actualidad </toDate> </existDates> <place> <address> <addressLinelocalType "provincia"> San José </addressLine> <addressLinelocalType "cantón"> Montes de Oca </addressLine> <addressLinelocalType "distrito"> San Pedro </addressLine> <adrressLinelocalType "código postal"> 11501 </addressLine> </address> </place> <biogHist> <abstract>Creada el 7 de marzo de 1941, con el propósito de contribuir a la formación de investigadores, docentes y profesionales con excelencia académica, visión humanista y responsabilidad social.</abstract> <biogHist> </description>	NO	SI	NO	290

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
25	ICA	ISAAR-CPF/EAC	Nota descriptiva	DescriptiveNote	Proporcionar información adicional y especificaciones del elemento descriptivo en el que está contenido.	Texto libre	<descriptiveNote> Record created based on ISAAR(CPF) 2nd ed - institutional description </descriptiveNote>	NO	NO	NO	
26	ICA	ISAAR-CPF/EAC	Contexto Archivístico Codificado – Instituciones, personas y familias	Eac-cpf	Elemento raíz y, como tal, contiene la descripción EAC-CPF completa de la institución, persona o familia.	El metadato se alimenta de otros metadatos como, resumen histórico, fechas, funciones, etc.	<eac-cpf> <control>[...]</control> <cpfDescription>[...]</cpfDescription> </eac-cpf>	NO	NO	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
27	ICA	ISAAR-CPF/EAC	Identificador de entidad	EntityId	Cualquier identificador formal utilizado para designar a la entidad que se describe	Texto libre, en caso de que exista	<identity> <entityId>506-291</entityId> <entityType>Institución autónoma</entityType> </identity>	SI	NO	NO	La información de este metadato se incluirá en el metadato "agentIdentifier" del modelo PREMIS
28	ICA	ISAAR-CPF/EAC	Tipo de entidad, (persona, institución o familia)	EntityType	Identificar el tipo de entidad descrito	Lista desplegable	<entityType>corporateBody</entityType>	SI	SI	NO	La información de este metadato se incluirá en el metadato "agentType" del modelo PREMIS

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
29	ICA	ISAAR-CPF/EAC	Evento	Event	Registrar un evento asociado con una fecha y, opcionalmente, con un lugar, dentro de una cronología estructurada.	Información de un evento en texto libre. Máximo 50 carácteres	<chronItem> <date standardDate="1974">1974</date> <event> Creación de la Vicerrectoría de Acción Social. </event> </chronItem>	NO	NO	NO	La información de este metadato se incluirá en el metadato "eventIdentiifer" del modelo PREMIS.
30	ICA	ISAAR-CPF/EAC	Fecha y hora del evento de mantenimiento	EventDateTime	Describir la fecha y hora de un evento de mantenimiento de la instancia EAC-CPF	Alfanumerico AAAA-MM-DD	<maintenanceEvent> <eventType> created </evenType> <evenDateTime> 2018-09-28 </evenDateTime> </maintenanceEvent>	SI	SI	NO	La información de este metadato se incluirá en el metadato "EventDateTime" del modelo PREMIS.

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
31	ICA	ISAAR-CPF/EAC	Descripción del evento de mantenimiento	EventDescription	Describir un evento de mantenimiento en la vida de la instancia EAC-CPF.	Información de un evento en texto libre. Máximo 50 carácteres	<maintenanceEvent> <eventType> created </evenType> <evenDateTime> 2018-09-28 </evenDateTime> <agentType> human </agentType> <agent>Mondragón Cordero, K </agent> <eventDescription>Created from original in ISAAR (CPF) </eventDescription> </maintenanceEvent>	SI	SI	SI	
32	ICA	ISAAR-CPF/EAC	Tipo de evento de mantenimiento	EventType	Muestra el tipo de evento de mantenimiento de la instancia EAC-CPF.	El metadato se genera de forma automática, según el evento llevado a cabo	<eventType>created</evenType>	SI	SI	SI	La información de este metadato se incluirá en el "EventType" del modelo PREMIS.

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
33	ICA	ISAAR-CPF/EAC	Fechas de existencia	ExistDates	Muestra las fechas de existencia de la entidad que se describe, como las fechas de establecimiento y disolución de instituciones y las fechas de nacimiento y muerte, o de florecimiento de personas.	Alfanumérico AAAA-MM-DD	<existDates> <dateRange> <fromDatestandardDate="1941-03-07">1941-03-07 </fromDate> <toDateStandardDate="actualidad">actualidad </toDate> </existDates>	NO	NO	NO	
34	ICA	ISAAR-CPF/EAC	Fechainicial	FromDate	Muestra la fecha de inicio en un rango de fechas.	Alfanumérico AAAA-MM-DD		SI	SI	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
35	ICA	ISAAR-CPF/EAC	Función, actividad o rol que realiza la entidad descrita	Function	Proporcionar información sobre una función, actividad, rol o finalidad realizada o manifestada por la entidad que se describe.	La información se proporciona en texto libre, según lo indique la normativa o infografía de la persona	<function> <term>Gestión de la Acción Social</term> <descriptiveNote> integra y realimenta permanentemente a la Universidad con la comunidad nacional e internacional, con el objetivo de poner a su servicio la capacidad académica institucional y lograr, en conjunto, las transformaciones requeridas para el mejoramiento de la calidad de vida en el país. </descriptiveNote> </funtion>	SI	SI	NO	
36	ICA	ISAAR-CPF/EAC	Una función relacionada con la entidad descrita.	FunctionRelation	Contiene la descripción de una función relacionada con la entidad descrita	Texto libre	<functionRelationfunctionRelationType="performs"> <relationEntry> Gestión de la acción social de la Universidad con la sociedad </relationEntry> <descriptiveNote> La sociedad con la Acción Social de la Universidad </descriptiveNote> </functionRelation>	NO	NO	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
37	ICA	ISAAR-CPF/EAC	Funciones. Elemento opcional que puede agrupar una o más apariciones de funciones para ser manipuladas como un paquete.	functions	Agrupareleme ntosindividuales.	Se redacta en texto libre Debe registrarse las funciones, actividades o tareas.	<functions> <function> <term>Gestión de la Acción Social</term> </function> <function> <term>Gestión de la Docencia</term> </function> </functions>	SI	NO	NO	
38	ICA	ISAAR-CPF/EAC	Contexto General. Elemento que proporciona amplia libertad para registrar información contextual no acomodada a otros elementos de descripción.	general Context	Registrar información del contexto general, social y cultural de la organización.	Se redacta en texto libre. Debe registrar información del contexto organizacional.	<generalContext> La Universidad de Costa Rica es una institución de educación superior y cultura, autónoma constitucionalmente y democrática, constituida por una comunidad de profesores y profesoras, estudiantes, funcionarias y funcionarios administrativos, dedicada a la enseñanza, la investigación, la acción social, el estudio, la meditación, la creación artística y la difusión del conocimiento . <generalContext>	SI	NO	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
39	ICA	ISAAR-CPF/EAC	Identidad. Contenedor que agrupa todos los elementos para la identificación de la instancia.	identity	Agrupa elementos necesarios para identificar el nombre de la entidad.	Incluir datos en texto libre. Debe registrar el nombre de la entidad: institución, persona o familia y otros nombres utilizados.	<identity> <entityId>506-291</entityId> <entityType>Institución autónoma</entityType> </identity>	SI	NO	SI	La información de este metadato se incluirá en "agentName" del modelo PREMIS
40	ICA	ISAAR-CPF/EAC	ítem. Se utiliza para listas generales dentro de elementos descriptivos.	item	Registrar las entradas individuales que componen las listas generales.	El metadato registra listas generales en texto libre.	<outline> <level> <item>I.</item> </level> <level> <item>II.</item> <level> <item>A.</item> </level> </outline>	SI	NO	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
41	ICA	ISAAR-CPF/EAC	Lengua. Proporciona la lengua principal en la que está escrita la instancia.	language	Especificar una lengua concreta utilizada por EAC-CPF	Incluye información en forma alfabética. Este metadato debe indicar la lengua(s) utilizada (s) por la organización.	<languageDeclaration> <language languageCode="eng">English</language> <script scriptCode="Latn">Latin</script> </languageDeclaration>	SI	SI	SI	Se toma de la ISO 639-1
42	ICA	ISAAR-CPF/EAC	Declaración de lengua. Lengua y escritura	languageDeclaration	Declarar la lengua y escritura predominante en la organización.	Se debe redactar en texto libre. Indicar la principal lengua y escritura utilizada en una organización.		SI	NO	SI	
43	ICA	ISAAR-CPF/EAC	Lengua utilizada. Lengua y escritura utilizadas por la entidad.	languageUsed	Indicar la lengua y escritura utilizadas por la entidad.	El metadato especifica la lengua y escritura utilizadas en la organización.		SI	NO	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
44	ICA	ISAAR-CPF/EAC	Lenguas utilizadas. Apariciones de lenguajes.	languagesUsed	Agrupar una o más apariciones de lenguaje en la organización.	Texto libre. Debe indicar apariciones de lenguaje en la organización.	<languagesUsed> <languageUsed> <language languageCode="eng">English</language> <script scriptCode="Latn">Latin</script> </languageUsed> <languageUsed> <language languageCode="spa">Spanish</language> <script scriptCode="Latn">Latin</script> </languageUsed> </languagesUsed>	SI	NO	SI	
45	ICA	ISAAR-CPF/EAC	Estatus jurídico. Agencias autorizadas para brindar información sobre la situación legal de la institución.	legalStatus	Registra información del estado jurídico de la institución.	Debe indicar el estatuto jurídico definido por una autoridad competente. Puedenincluirse: fechas, rangos y lugaresentexto libre.	<legalStatus> <term>Institucióñautónoma</term> </legalStatus>	SI	NO	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
46	ICA	ISAAR-CPF/EAC	Estatus jurídicos. Agrupa una o más apariciones de <legalStatus> de modo que pueden manipularse como un paquete.	legalStatuses	Agrupar apariciones de estatutos jurídicos	Según el marco legal, este metadato debe indicar los estatutos jurídicos correspondientes a una organización en texto libre.	<legalStatuses> <legalStatus> <term>Institucióñautónoma</term> <dateRange> <fromDate> "1941">1941</fromDate> <toDate>"actualidad">actualidad</toDate> </dateRange> </legalStatus>	SI	NO	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
47	ICA	ISAAR-CPF/EAC	Nivel. Formato de visión esquemática.	level	Indicarnivelesjerárquicos.	El metadato debe esquematizar los niveles jerárquicos de la organización a través de una lista desplegable.	<outline> <level> <item>I. AsamleaUniversitaria</item> </level> <level> <item>II. Consejo Universitario</item> </level> <level> <item>III. Rectoría</item> <leven> <item>A. Vicerrectoría de Administración</item> </level> <level> <item>B. Vicerrectoría de Investigación</item> </level> <level> <item>C. Vicerrectoría de Vida Estudiantil</item> </level> <level> <item>D. Vicerrectoría de Docencia</item> </level> <level> <item>E. Vicerrectoría de Acción Social</item> </level> </outline>	SI	NO	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
48	ICA	ISAAR-CPF/EAC	Lista. Lista general que pueden estar embebidas dentro de un amplio número de elementos descriptivos.	list	Registraunalista simple.	Incluir listas generales en elementos descriptivos.	<list> <functions> <function> <term>Gestión de la Acción Social</term> </function> <function> <term>Gestión de la Docencia</term> </function> </functions> </list>	SI	NO	SI	
49	ICA	ISAAR-CPF/EAC	Control local. Lista simple que consta de dos o más elementos.	localControl	Registrar y definir información de control.	Se debe registrar información de control por medio de términos y fechas.	<localControllocalType="detailLevel"> <term>básico</term> </localControl>	SI	NO	NO	
50	ICA	ISAAR-CPF/EAC	Descripción local. Categorías descriptivas disponibles en un sistema local.	localDescription	Extender categorías descriptivas disponibles en un sistema.	Describir términos de indización estructurados por medio de texto libre, rango de fechas y lugares.	<localDescriptions> <localDescriptionlocalType="http://...."> <termvocabularySource="http://....">Español</term> <placeEntrycountryCode="ESP" vocabularySource="http://...." >Costa Rica</placeEntry> </localDescription>	SI	SI	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
51	ICA	ISAAR-CPF/EAC	Descripciones locales. Agrupa y mantiene juntos elementos de <localDescription>.	localDescriptions	Acomodar una mayor complejidad de información a registrar.	El metadato debe agrupar descripciones locales para manipularlas como un paquete de información.		SI	SI	SI	
52	ICA	ISAAR-CPF/EAC	Declaración de tipo local. Declara cualquier convención local usada en el atributo @localType en la instancia EAC.CPF.	localTypeDeclaration	Declarar convenciones y vocabularios locales.	Metadato encargado de citar el alcance sobre reglas o convenciones.		SI	NO	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
53	ICA	ISAAR-CPF/EAC	Agencia de mantenimiento. Información sobre la institución o servicio responsable de la creación, mantenimiento y difusión de la instancia EAC-CPF.	maintenanceAgency	Identifica las ambigüedades de la institución o servicio.	El metadato funciona por medio de códigos institucionales e información de la institución para identificar ambigüedades.	<maintenanceAgency> <agencyCode>CRI-506</agencyCode> <agencyName>Universidad de Costa Rica</agencyName> </maintenanceAgency>	SI	NO	NO	
54	ICA	ISAAR-CPF/EAC	Evento de mantenimiento. Información sobre un evento concreto de mantenimiento en el historial de la instancia EAC-CPF.	maintenanceEvent	Registra información de un evento concreto	Metadato que registra información sobre agente, tipo de agente fecha y hora de eventos de mantenimiento en texto libre.	<maintenanceEvent> <eventType> created </evenType> <evenDateTime> 2018-09-28 </evenDateTime> </maintenanceEvent>	SI	NO	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
55	ICA	ISAAR-CPF/EAC	Historial de mantenimiento. Historial de la creación y mantenimiento de la instancia EAC-CPF.	maintenanceHistory	Registrar creación de la organización.	Debe registrar eventos y actividades de mantenimiento de la instancia en texto libre.	<maintenanceHistory> <maintenanceEvent> <eventType> created </evenType> <eventDateTimestandardDateTime="2018-09-28T00: 20:00.000-00:00">28 septiembre 2018</eventDate Time><agentType> human </agentType> <agent>Mondragón Cordero, K </agent> <eventDescription>Created from original in ISAAR (CPF)</eventDescription> </maintenanceEvent> </maintenanceHistory>	SI	NO	NO	
56	ICA	ISAAR-CPF/EAC	Estado de mantenimiento. Estado actual de elaboración de una instancia EAC-CPF.	maintenanceStatus	Registrar modificaciones de eventos sobre el estado de elaboración.	Metadato capaz de crear un historial de registros de autoridad del sistema descriptivo por medio de una lista desplegable.	<maintenanceStatus>new</maintenanceStatus>	SI	NO	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
57	ICA	ISAAR-CPF/EAC	Regulación. Fuente de autoridad o regulación de una institución desde el punto de vista de sus potestades, funciones, responsabilidades o actividades.	mandate	Identifica la fuente de autoridad o regulación de una institución.	Metadato que identifica la fuente de autoridad de una institución, debe utilizarse fechas o rangos y lugares con texto libre.	<mandates> <mandate> <term> Constitución Política de Costa Rica </term> </mandate> <mandate> <term> Estatuto Orgánico de la Universidad de Costa Rica </term> </mandate> </mandates>	SI	NO	NO	
58	ICA	ISAAR-CPF/EAC	Regulaciones. Agrupa una o más apariciones de <mandate> de modo que puedan manipularse como un paquete.	mandates	Acomodar una mayor complejidad en la expresión o representación de las regulaciones que se describen.	El metadato debe agrupar relaciones de regulaciones que se describen de forma alfanúmerica.		SI	NO	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
59	ICA	ISAAR-CPF/EAC	Identidades múltiples. Codifica más de un elemento <cpfDescription> en una sola instancia EAC-CPF.	multipleIdentities	Agruparvarios elementos<cpfDescription>	Debe representar más de una entidad o representar una identidad de colaboración.	<multipleIdentities> <cpfDescription> <identity>[...]</identity> <description>[...]</description> <relations>[...]</relations> </cpfDescription> <cpfDescription> <identity>[...]</identity> <description>[...]</description> <relations>[...]</relations> </cpfDescription> </multipleIdentities>	SI	NO	SI	
60	ICA	ISAAR-CPF/EAC	Entrada de nombre. Contiene una entrada de nombre de una institución, persona o familia.	nameEntry	Registrar nombre de la institución.	El metadato debe identificar la forma autorizada del nombre de la institución, persona o familia. Pueden incluir la forma alternativa del nombre de la entidad de forma alfabética.	<nameEntry> <part> Universidad de Costa Rica </part> <useDates> <dateRange> <fromDatestandardDate="1940">1940 </fromDate> <toDatestandardDate="Actualidad">Actualidad</toDate> </dateRange> </useDates> <authorizedForm>UCR</authorizedForm> </nameEntry>	SI	NO	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
61	ICA	ISAAR-CPF/EAC	Entrada de formas paralelas del nombre. Contenedor utilizado para agrupar dos o más elementos <nameEntry> que representan formas paralelas del nombre de la misma entidad	nameEntryParallel	Agrupar dos o más formas paralelas del nombre de la entidad.	Se debe indicar formas paralelas del nombre de la organización en texto libre.		SI	NO	SI	
62	ICA	ISAAR-CPF/EAC	Contenedor de objeto binarioElemento que proporciona un lugar para una representación binaria codificada en base 64 de un recurso.	objectBinWrap	Proporcionarrepresentaciónbinariacodificada.	El metadato codifica datos en base 64 de forma numérica.	<objectBinWrap>[Base64 Binary code]</objectBinWrap>	SI	NO	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
63	ICA	ISAAR-CPF/EAC	Contenedor de objeto XML. Elemento que proporciona un lugar para incluir datos codificados en otro lenguaje XML. Facilita la interoperabilidad.	obectXMLWrap	Incluirelementos XML.	El metadato incluye datos en esquema XML estándar y abierto de forma alfanumérica.	<objectXMLWrap>[...]</objectXMLWrap>	SI	NO	SI	
64	ICA	ISAAR-CPF/EAC	Ocupación. Elemento que proporciona información sobre la ocupación de la entidad que se describe.	occupation	Proporcionar información de la ocupación de la entidad.	Identificar la ocupación ejercida por la organización, puede utilizar fechas y lugares en texto libre.	<occupation> <term>Educación</term> </occupation>	SI	NO	NO	
65	ICA	ISAAR-CPF/EAC	Ocupaciones. Elemento que proporciona información sobre la ocupación de la entidad que se describe.	occupations	Agrupareleme ntos de <occupation>	Metadato que agrupa ocupaciones de la organización de forma conjunta entre profesión y función.	<occupations> <occupation> <term>Educación</term> </occupation> <occupation> <term>Investigación</term> </occupation> </ocupations>	SI	NO	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
66	ICA	ISAAR-CPF/EAC	Otro código de agencia. Código de institución alternativo y/o local para representar la institución o servicio responsable de la creación, mantenimiento y/o difusión de la instancia EAC-CPF.	otherAgencyCode	Proporcionar código alternativo para la institución	Debe asignar un código único de la organización mediante un formato de identificación estándar internacional. El código alfanumérico debe contener un máximo de 35 caracteres.	<otherAgencyCode>UCR-001</otherAgencyCode>	SI	NO	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
67	ICA	ISAAR-CPF/EAC	Otro identificador de registro. Identificadores de registro que pueden estar asociados con la instancia EAC-CPF, alternativos al identificador obligatorio indicado en <recordl> identificador de registro.	otherRecordld	Proporcionaridentificadores de registro.	Identifica el tipo de institución o servicio responsable de cada identificador de registro asociado mediante un código alternativo. El código es alfanumérico con un máximo de 50 caracteres.	<otherRecordId>ARC-ID-976172</otherRecordId>	SI	NO	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
68	ICA	ISAAR-CPF/EAC	Visión esquemática. Información en un formato de visión esquemática.	outline	Registro de información en formato de visión esquemática.	Metadato capaz de estructurar elementos de nivel de forma jerárquica mediante una lista desplegable.	<outline> <level> <item>I.</item> </level> <level> <item>II.</item> <level> <item>A.</item> </level> <level> <item>B.</item> <level> </level> </level> </outline>	SI	NO	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
69	ICA	ISAAR-CPF/EAC	Párrafo . Elemento genérico del área de descripción que marca una o más frases que componen un fragmento textual lógico en prosa.	p	Describe una marca o frase de texto en prosa.	Debe aplicarse a una descripción general de la instancia CPF en texto libre.	La Universidad de Costa Rica es una institución de educación superior y cultura, autónoma constitucionalmente y democrática, constituida por una comunidad de profesores y profesoras, estudiantes, funcionarias y funcionarios administrativos, dedicada a la enseñanza, la investigación, la acción social, el estudio, la meditación, la creación artística y la difusión del conocimiento .	SI	NO	NO	
70	ICA	ISAAR-CPF/EAC	Parte. Elemento <part> se utiliza para distinguir los componentes del nombre de la entidad que se describe.	part	Distingue componentes del nombre de la entidad.	Metadato que identifica el nombre de pila, apellido o título honorífico de la organización de forma alfabética.	<part localType="apellido">Monge</part> <part localType="nombre">Carlos</part> <authorizedForm>Carlos Monge</authorizedForm>	SI	NO	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
71	ICA	ISAAR-CPF/EAC	Lugar. Información sobre un lugar o jurisdicción donde la entidad EAC-CPF tuvo su sede o vivió, o con el cual tuvo otra conexión significativa.	place	Proporcionar información del lugar o jurisdicción de la entidad.	El metadato identifica lugares o jurisdicciones donde la organización tuvo su sede o vivió con una conexión significativa, debe redactarse en texto libre.	<place> <placeEntry> San José, Costa Rica</placeEntry> <placeRole>Sede</placeRole> </place>	SI	NO	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
72	ICA	ISAAR-CPF/EAC	Entrada de lugar. Elemento utilizado en el área de descripción y en el área de relaciones para registrar información sobre un lugar o jurisdicción donde la entidad EAC-CPF tuvo su sede o vivió, o con el cual tuvo otra conexión significativa.	placeEntry	Registra información sobre el lugar o jurisdicción de la entidad.	Debe asignar información del lugar por medio de vocabularios controlados en texto libre.		SI	NO	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
73	ICA	ISAAR-CPF/EAC	Rol del lugar. Proporciona un rol contextual para un elemento <placeEntry> (Entrada de lugar) dentro de <place>.	placeRole	Proporcionar un rol contextual de la entidad.	El metadato utiliza un vocabulario controlado para designar la localidad, características y jurisdicción política de la organización.		SI	NO	SI	
74	ICA	ISAAR-CPF/EAC	Lugares. Elemento opcional <places> para agrupar una o más apariciones de <place>, de modo que puedan manipularse como un paquete.	places	Acomodar una mayor complejidad en la expresión o representación de las regulaciones que se describen.	Debe registrarse en texto libre los lugares.	<places> <place> <place> <placeEntry> San José, Costa Rica</placeEntry> <placeRole>Sede</placeRole> </place> <place> <place> <placeEntry> San Ramón, Costa Rica</placeEntry> <placeRole>Sede</placeRole> </place> <place> <placeEntry> Turrialba, Costa Rica</placeEntry> <placeRole>Sede</placeRole> </place> </places>	SI	NO	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
75	ICA	ISAAR-CPF/EAC	Forma preferente del nombre. Elemento utilizado para indicar cuál de los nombres paralelos registrados dentro de <nameEntryParallel> (Entrada de formas paralelas del nombre) se considera preferente para su visualización en un contexto determinado.	preferredForm	Indicarnombresparalelosregistrados.	El metadato indica la forma preferente del nombre que será visualizado frente a nombres paralelos de forma alfabética.	<preferredForm>UCR</preferredForm>	SI	NO	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
76	ICA	ISAAR-CPF/EAC	Estado de publicación. Estado actual de la publicación de la instancia EAC-CPF.	publicationStatus	Indicar estado actual de la publicación de la instancia.	El metadato indica el estado de publicación de EAC-CPF en "aprobado" o "en proceso" en conjunto con la versión mediante lista desplegable.	<publicationStatus>borrador</publicationStatus>	SI	NO	SI	
77	ICA	ISAAR-CPF/EAC	Identificador de registro. Elemento que designa un identificador único de la instancia EAC-CPF.	recordld	Designar identificador único de la organización.	Proporciona el identificador único global de la organización. El código alfanumérico debe contener un máximo de 100 caracteres.	<recordId>CRI47161UCR RA 00001 </recordId>	SI	NO	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
78	ICA	ISAAR-CPF/EAC	Entrada de relación. Texto libre, que identifica una entidad relacionada, la cual puede ser otra: otra entidad (institución, persona o familia), un recurso creado por la entidad que se describe o relacionado con está.	relation Entry	Descripción de las relaciones de la entidad con texto libre.	El metadato debe incluir texto libre para identificar la entidad en: institución, persona o familia, o bien, en recursos creados por la misma como documentos de archivo.	<relationEntry> Gestión de la acción social de la Universidad con la sociedad </relationEntry>	SI	NO	NO	La información del metadato se incluirá en "likingAgentIdentifierType" del modelo PREMIS

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
79	ICA	ISAAR-CPF/EAC	Relaciones. Elementos de relación, cada uno de los cuales denota una relación específica.	relations	Agruparrelacionesespecíficas.	Debe señalar las relaciones de la organización con otras entidades a nivel de: institución, persona familia, funciones, fondos y colecciones en texto libre.	<relations> <cpfRelation>[...]</cpfRelation> <functionRelation>[...]</functionRelation> <resourceRelation>[...]</resourceRelation> </relations>	SI	NO	NO	
80	ICA	ISAAR-CPF/EAC	Relación con recurso. Contiene la descripción de un recurso relacionado con la entidad descrita.	resourceRelation	Describe recursos relacionados con la entidad.	Metadato que específica cuándo se aplicó la relación por medio de la indicación de lugar con una nota descriptiva a través de una lista desplegable.	<resourceRelationresourceRelationType="creatorOf"> <objectXMLWrap>[...]</objectXMLWrap> </resourceRelation>	SI	NO	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
81	ICA	ISAAR-CPF/EAC	Escritura principal en la que está escrita la instancia EAC-CPF.	script	Específica escritura concreta de la organización.	Metadato que indica la escritura principal utilizada por la organización de forma alfabética.	<languageDeclaration> <language languageCode="spa">Spanish</language> <script scriptCode="Latn">Latin</script> </languageDeclaration>	SI	SI	SI	
82	ICA	ISAAR-CPF/EAC	Componente de un conjunto. Múltiples registros de la misma identidad, de distintos sistemas de autoridad o en diferentes lenguas, pueden combinarse dentro de una sola instancia EAC-CPF.	setComponent	Registro de autoridad completo de la entidad.	Registro del enlace al registro de autoridad del sistema de autoridad externa.	<setComponentxlink:href="https://archivo.ucr.ac.cr/aurol.html" xlink:type="simple">	SI	SI	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
83	ICA	ISAAR-CPF/EAC	Fuente. Fuente concreta de evidencia utilizada al describir la entidad o entidades.	source	Identificar la fuente concreta utilizada para describir la entidad.	Metadato que utiliza la fuente utilizada por la organización en n en texto libre.	<sources> <source> <sourceEntry>Estatuto Orgánico de la Universidad de Costa Rica</sourceEntry> </source> <Source> <sourceEntry> Colección de las Disposiciones Legislativas y Administrativas emitidas en el año 1888</sourceEntry> </source> </sources>	SI	SI	SI	
84	ICA	ISAAR-CPF/EAC	Entrada de fuente. Fuente concreta de evidencia utilizada al describir la entidad en la instancia EAC-CPF.	sourceEntry	Identifica directamente una fuente usada.	Identifica fuentes usadas por la organización.		SI	NO	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
85	ICA	ISAAR-CPF/EAC	Fuentes. Un registro de las fuentes utilizadas para la descripción de la entidad o entidades en la instancia EAC-CPF.	sources	Registrar una o más fuentes consultadas.	Metadato que registra fuentes consultadas.		SI	NO	SI	
86	ICA	ISAAR-CPF/EAC	Fragmento. Especifica el inicio y final de un fragmento de texto.	span	Marca palabras o frases arbitrarias por enfatizar.	Identifica frases o palabras para señalar cualidades en texto libre.	“(…) Crease, con el nombre de Universidad de Costa Rica, una institución docente y de cultura superior que tendrá por misión cultivar las ciencias, las letras y las bellas artes, difundir su conocimiento y preparar para el ejercicio de las profesiones liberales (...)”	SI	NO	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
87	ICA	ISAAR-CPF/EAC	Estructura o genealogía. Registra dentro del área de descripción información (como organigramas fechados) que expresa la(s) estructura(s) administrativa(s) interna(s) de una institución y las fechas de cualquier cambio de dicha estructura, que sean relevantes para conocer la forma en que esa institución llevó a cabo sus actividades.	structureOrGenealogy	Conocer la forma en que la institución llevó a cabo sus actividades.	Registra información de la estructura administrativa interna de la organización y un registro de fechas de cambio en texto libre.	<structureOrGenealogy> <outline> <level> <item>I. AsamleaUniversitaria</item> </level> <level> <item>II. Consejo Universitario</item> </level> <level> <item>III. Rectoría</item> <leven> <item>A. Vicerrectoría de Adaministración</item> </level> <level> <item>B. Vicerrectoría de Investigación</item> </level> <level> <item>C. Vicerrectoría de Vida Estudiantil</item> </level> <level> <item>D. Vicerrectoría de Docencia</item> </level> <level> <item>E. Vicerrectoría de Acción Social</item> </level> </outline> </structureOrGenealogy>	SI	NO	NO	325

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
88	ICA	ISAAR-CPF/EAC	Término. Término descriptivo de acuerdo con reglas descriptivas locales.	term	Registrar eltérminodescriptivo.	Metadato encargado de describir un término en texto libre.	<term>Institución con autonomía funcional y administrativa</term>	SI	NO	SI	
89	ICA	ISAAR-CPF/EAC	Fecha final. Rango de fechas, expresadas como en un mes, día o año o en cualquier formato.	toDate	Contener fechas reales o aproximadas.	Alfanumerico AAAA-MM-DD	<nameEntry> <part> Universidad de Santo Tomás </part> <useDates> <dateRange> <fromDatestandardDate="1843">1843</fromDate> <toDatestandardDate="1888">1888</toDate> </useDates> </nameEntry>	SI	NO	SI	
90	ICA	ISAAR-CPF/EAC	Fechas de uso. Fechas en las que el nombre o nombres fueron utilizados por la entidad que describe	useDates	Proporcionarfechas de descripción.	Alfanumerico AAAA-MM-DD.		SI	NO	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
91	ICA	ISAD-G/EAD	Código de referencia	unitid	Identificar de un modo único la unidad de descripción y establecer el vínculo con la descripción que la representa	Se debe consignar los siguientes elementos: el código del país según la última versión de la ISO 3166 Códigos para la representación de los nombres de los países; el código del archivo según la norma nacional de códigos de archivo u otro identificador único de su ubicación; y el código de referencia local específico, el número de control u otro identificador único.	<unitid> 506-291-AUROL-EH-603-2020 </unitid>	SI	SI	SI	La información de este metadato se incluirá en los siguientes metadatos del modelo PREMIS: formatDesignation, formatRegistryName, FormatRegistryKey, EviromentRegistryName, EviromentRegistryKey, EventIdentifier, AgentIdentifier

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
92	ICA	ISAD-G / EAD	Título	unittitle	Denominar la unidad de descripción.	Se debe consignar bien el título formal. Asignar un título conciso de acuerdo a las reglas de descripción multinivel y las normas nacionales. En caso necesario, si el título formal es largo, este puede abreviarse siempre y cuando no se pierda información esencial.	<unittitle>Aprobación de diseño de proyecto de Trabajo Final de Graduación </unittitle>	SI	SI	NO	La información del metadato se incluirá en "FormatName" del modelo PREMIS.

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
93	ICA	ISAD-G / EAD	Fechas	<unitdate>	Identificar y consignar las fechas de la unidad de descripción	Se deben incluir: La (s) fecha(s) en la(s) que el productor acumuló los documentos en el ejercicio o desarrollo de su actividad. La (s) fecha(s) de producción de los documentos. Aquí se incluyen las fechas de las copias, ediciones o versiones, anexos, u originales de las unidades documentales producidas con anterioridad a su acumulación.	<unitdate type = "inclusive" normal = "2020/2021"> 2020-2021 </unitdate>	SI	SI	SI	La información del metadato se incluirá en los siguientes metadatos del modelo PREMIS: DateCreatebyApplication, EventDateTime, CopyRightApplicableDatesLicenseApplicableLicense

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
94	ICA	ISAD-G / EAD	Nivel de descripción	archdescand c	Identificar el nivel de organización de la unidad de descripción.	Consignar el nivel de la unidad de descripción.	<c level = "series"> <did> <unitid> Serie 1 </unitid> <unittitle>Trabajos Finales de Graduación</unittitle> </did> </c>	SI	SI	NO	
95	ICA	ISAD-G / EAD	Volumen y soporte de la unidad de descripción	physdescextent, physfacet, genreform	Identificar y describir: la extensión física o lógica y el soporte de la unidad de descripción.	Consignar el volumen de la unidad de descripción especificando el número de unidades físicas o lógicas en cifras árabes y la unidadd e medida. Especificar el soporte o soportes de la unidad de descripción.	<physdesc> <physfacet type = "soporte"> digital </physfacet> <extent> 2,8MB </extent> <genreform> textual </genreform> </physdesc>	SI	SI	NO	La información de este metadato se incluirá en el metadato "size" del modelo PREMIS.

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
96	ICA	ISAD-G / EAD	Nombre del productor (es)	origination	Identificar el productor o los productores de la unidad de descripción.	Consignar el nombre de la entidad(es) o persona(s) física(s) responsables de la producción, acumulación y conservación de los documentos de la unidad de descripción.	<originationlabel = "Creator:"><corpname> Escuela de Historia </corpname></origination>	SI	SI	NO	La información de este metadato se incluirá en el metadato "AgentName" del modelo PREMIS

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
97	ICA	ISAD-G / EAD	Reseñabiográfica	bioghist	Proporcionar la historia institucional o los datos biográficos del productor o de los productores de la unidad de descripción para situar la documentación en su contexto y hacerla más comprensible.	Consignar sintéticamente cualquier dato significativo sobre el origen, evolución, desarrollo y trabajo de la entidad (o entidades) o sobre la vida y el trabajo de la persona(s) física(s) responsable(s) de la producción de la unidad de descripción.	<bioghist> <head> Historial administrativo </head> La Escuela de Historia cuenta con la Sección de Archivística, que existe desde 1978, planteada inicialmente solo como un Diplomado en Archivología, en el seno de la desaparecida Escuela en Historia y Geografía. Hacia 1996 fue creado el Bachillerato en Archivística y en el año 2004, la Licenciatura en esta disciplina. </bioghist>	SI	SI	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
98	ICA	ISAD-G / EAD	Historia archivística	custodhist	Proporcionar información sobre la historia de la unidad de descripción que sea significativa para su autenticidad, integridad e interpretación.	Consignar los traspasos sucesivos de la propiedad, responsabilidad y/o custodia de la unidad de descripción e indicar aquellos hechos que hayan contribuido a conformar su estructura y organización actual como por ejemplo, la historia de su organización, la producción de instrumentos de descripción contemporáneos, la reutilización de los documentos para otros objetivos o las migraciones de software. Precisar en caso de que se conozcan, las fechas de estos hechos. Si se desconoce la historia archivística, consignarestedato.	<custodhist> <p> </custodhist>	SI	SI	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
99	ICA	ISAD-G / EAD	Forma de ingreso	<acqinfo>	Identificar la forma de adquisición o transferencia.	Consignar el origen desde el cual fue remitida la unidad de descripción y la fecha y/o el modo de adquisición, siempre que no se trate, en todo o en parte, de información confidencial. Si elorigen se desconoce, consignarestedato.	<acqinfo> Producción propia en el ejercicio de las funciones <date normal = "2020-12-16"> 16 de diciembre de 2020 </date>. < / acqinfo>	SI	SI	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
100	ICA	ISAD-G / EAD	Alcance y contenido	<scopecontent>	Proporcionar a los usuarios la información necesaria para apreciar el valor potencial de la unidad de descripción.	Dar una visión de conjunto (por ejemplo, períodos de tiempo, ámbito geográfico) y realizar un resumen de contenido (por ejemplo, tipos documentales, materia principal, procedimientos administrativos) de la unidad de descripción, apropiados al nivel de descripción.	<scopecontent> Aprobación del Seminario de Graduación: “Marco de evaluación para soluciones de preservación de documentos digitales en Costa Rica”, por parte de la Comisión de Trabajos Finales de Graduación, en la Sesión 46-2020, acuerdo 1 </scopecontent>	SI	SI	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
101	ICA	ISAD-G / EAD	Valoración, Selección, y Eliminación	appraisal	Proporcionar información sobre cualquier acción de valoración, selección o eliminación efectuada.	Consignar las actividades de valoración, selección y eliminación realizadas o planificadas sobre la unidad de descripción, especialmente si afectan de alguna manera a la interpretación de la documentación. Ensucaso, consignar al responsable de la acción.	<appraisalencondinganalog= Para la serie documental Trabajos finales de graduación se establece la vigencia de un año para los trabajos finales de graduación que se encuentran en las unidades académicas y de investigación,considerando que en la Biblioteca Luis Demetrio Tinoco se encuentran dos ejemplares del trabajo final, de acuerdo con la Tabla de Plazos de Conservación y Eliminación de Documentos de las Unidades Académicas de la Universidad de Costa Rica, Código CUSED-IV-2018 </appraisal>	SI	SI	SI	
102	ICA	ISAD-G / EAD	Nuevos Ingresos	accruals	Informar al usuario de los ingresos complementarios previstos relativos a la unidad de descripción.	Indicar si están previstos nuevos ingresos, estimando en su caso, cantidad y frecuencia.	<accruals> Se prevén nuevos ingresos, 2 MB mensuales. </accruals>	SI	SI	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
103	ICA	ISAD-G / EAD	Organización	<arrangement>	Informar sobre la estructura interna, la ordenación y/o el sistema de clasificación de la unidad de descripción.	Proporcionar información sobre la arquitectura del sistema.	<arrangement> Organizado en tres subseries: <listtype = "simple"> <item> Recortes - cronológico </item> <item> Recortes-personas </item> <item> Notas </item> </list> "Recortes-personas "está ordenado alfabéticamente por apellido </arrangement>	SI	SI	SI	La información de este metadato se incluirá en el metadato "RelateObjectSequence" del modelo PREMIS

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
104	ICA	ISAD-G / EAD	Condiciones de acceso	accessrestrict	Informar sobre la situación jurídica y cualquier otra normativa que restrinja o afecte el acceso a la unidad de descripción.	Especificar la legislación o la situación jurídica, los convenios, regulaciones o cualquier tipo de decisión que afecte el acceso a la unidad de descripción. En su caso, indicar el período de tiempo durante el cual la documentación permanecerá inaccesible y la fecha en la que la documentación si lo estará.	<accessrestrict> Libre. </accessrestrict>	SI	SI	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
105	ICA	ISAD-G / EAD	Condiciones de reproducción	userestrict	Identificar cualquier tipo de restricción relativa a la reproducción de la unidad de descripción.	Informar sobre las condiciones, como por ejemplo el derecho de propiedad intelectual, que regulan la reproducción de la unidad de descripción una vez que está accesible. Si la existencia de tales condiciones no se conoce, consignar este hecho.	<userestrict> Sin restricciones de reproducción </userestrict>	SI	SI	SI	La información del metadato se incluirá en el metadato "CopyrightInformation" del modelo PREMIS.

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
106	ICA	ISAD-G / EAD	Lengua/escritura(s) de los documentos	archdesc	Indicar la lengua(s), escritura(s) y sistema de símbolos utilizados en la unidad de descripción.	Consignar la lengua(s) y/o escritura(s) de los documentos que forman la unidad de descripción. Especificar cualquier tipo de alfabeto, escritura, sistema de símbolos o abreviaturas utilizadas.	<archdesc> <language langcode="lat">Latín</language> <language langcode="esp">español</language> </archdesc>	NO	SI	SI	
107	ICA	ISAD-G / EAD	Características físicas y requisitos técnicos	physdesc, physfacet	Indicar sobre cualquier característica física o requisito técnico de importancia que afecte al uso de la unidad de descripción.	Especificar cualquier tipo de software y/o hardware necesario para acceder a la unidad de descripción.	<physdesc> <physfacet type = "soporte"> digital </physfacet> <extent> 218KB </extent> <genreform> textual </genreform> </physdesc>	SI	SI	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
108	ICA	ISAD-G / EAD	Instrumentos de descripción	otherfindaid	Identificar cualquier tipo de instrumento de descripción relativo a la unidad de descripción.	Informar sobre cualquier instrumento de descripción que se encuentre en el poder del archivo o del productor y que proporcione información relativa al contexto	<otherfindaid> <bibref> expedientes de Trabajos Finales de Graduación: <title>Inventario de series documentales de la Escuela de Historia de la Universidad de Costa Rica </persname> </bibref> < / otherfindaid>	SI	SI	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
109	ICA	ISAD-G / EAD	Existencia y localización de los documentos originales	odd, separatedmaterial	En el caso de que la unidad de descripción esté conformada por copias, indicar la existencia, localización y disponibilidad y/o eliminación de los originales.	Si el original de la unidad de descripción está disponible (bien en la propia institución bien en otro lugar) especificar su localización junto con cualquier otro número de control significativo. Si los originales ya no existen, o su localización se desconoce, consignar este hecho.	<separatedmaterial> Original en el Acta de sesión 46-2020 de la Comisión de Trabajos Finales de Graduación de la Escuela de Historia de Universidad de Costa Rica </separatedmaterial>	SI	SI	NO	La información del metadato se incluirá en los siguientes metadatos del modelo PREMIS: ContentLocation, Storage, StorageMedium

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
110	ICA	ISAD-G / EAD	Existencia y localización de copias	altformavail	Indicar la existencia, localización y disponibilidad de copias de la unidad de descripción.	Si la copia de la unidad de descripción está disponible (en la misma institución o en otro lugar) especificar su localización y cualquier otro número de localización y cualquier otro número de control significativo.	<altformavail> <head> Forma alternativa de material </head> Copia en microfilm disponible (<numtype = "microfilm reel"> CU-2013/1 </num>). < / altformavail>	SI	SI	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
111	ICA	ISAD-G / EAD	Unidades de descripciónrelacionadas	relatedmaterial, separatedmaterial	Identificar las unidades de descripción relacionadas.	Informar acerca de las unidades de descripción que se encuentran en el archivo o en otro lugar y que tengan alguna relación con la unidad de descripción por el principio de procedencia o por cualquier otra clase de asociación.	<relatedmaterial> Se puede localizar información relacionada en las Actas de Sesiones de la Comisión de Trabajos Finales de Graduación de la Escuela de Historia de Universidad de Costa Rica </relatedmaterial>	SI	SI	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
112	ICA	ISAD-G / EAD	Nota de Publicaciones	bibliography	Identificar cualquier tipo de publicación que trate o esté basada en el uso, estudio o análisis de la unidad de descripción.	Dar la referencia y/o información sobre cualquier publicación que trate o esté basada en el uso, estudio o análisis de la unidad de descripción. Incluirreferencias de las transcripciones o edicionesfacsimilarespublicadas.	<bibliografía> <head> Publicaciones en serie </head>. . . </bibliografía>	SI	SI	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
113	ICA	ISAD-G / EAD	Notas	odd	Dar información que no haya sido incluida en ninguna de las otras áreas.	Consignar información especial o cualquier otra información significativa no incluida en ningún otro elemento de la descripción.		SI	SI	NO	La información del metadato se incluirá en los siguientes metadatos del modelo PREMIS: FormatNote, EnvironmentDesignationNote, EventDetailInformation, CopyrightNote, LicenseNote, StatuteNote, RightsGrantedNote

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
114	ICA	ISAD-G / EAD	Nota del archivero	processinfo	Explicar quién y cómo ha preparado la descripción.	Especificar fuentes consultadas para preparar la descripción y quién la ha elaborado.	<processinfo> <head> Información de procesamiento: </head> Descripción realizada el <date> 2021-09-25 </date> Pérez Gómez, José. </processinfo>	SI	SI	SI	La información de este metadato se incluirá el metadato "AgentNote" del modelo PREMIS.

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
115	ICA	ISAD-G / EAD	Reglas o normas	conventiondeclaration	Identificar la normativa en la que está basada la descripción.	Consignar las normas y reglas internacionales, nacionales y locales utilizadas en la descripción.	<conventiondeclaration> <abbr> ISAD (G) </abbr> <citation> ISAD (G): Descripción general de archivos estándar internacional, segunda edición, Ottawa 2000 </citation> </conventiondeclaration> <conventiondeclaration> <citation> ISO 8601 - Elementos de datos y formatos de intercambio - Intercambio de información - Representación de fechas y horas, 2a ed., Ginebra: Organización Internacional de Normalización, 2000 </citation> </conventiondeclaration> <conventiondeclaration> <abbr> NTN-002</abbr> <citation> Norma Técnica Nacional-002: Lineamientos para la Descripción Archística, 2020</citation> </conventiondeclaration>	SI	SI	SI	La información de este metadato se incluirá en el metadato "CopyrightJurisdiction" del modelo PREMIS.
116	ICA	ISAD-G / EAD	Fecha(s) de la(s) descripción(es)	date in processinfo	Indicar cuándo se ha elaborado y/o realizado la descripción.	Consignar las fechas en las que se ha preparado y/o revisado la descripción.	<processinfo> <date> 2021-09-15</date> </processinfo>	SI	SI	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
117	Loc	PREMIS	Identificador del objeto	objectIdentifier	Identificar de forma única el objeto dentro del repositorio.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		NO	SI	SI	
118	Loc	PREMIS	Tipo del identificador del objeto	objectIdentifierType	Indicar el dominio en que el identificador es único.	Se puede tomar de un vocabulario controlado.	<objectIdentifierType>Identificador del código de referencia ISAD(G) en el espacio de nombres EAD</objectIdentifierType>	SI	SI	SI	
119	Loc	PREMIS	Valor del identificador del objeto	objectIdentifierValue	Indicar el valor del identificador del objeto.	No se establece ningún lineamiento.	<objectIdentifierValue>EH-603-2020</objectIdentifierValue>	SI	SI	SI	Puede ser el Código de Referencia del ISAD-G

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
120	Loc	PREMIS	Categoría del objeto	objectCategory	Indicar la categoría del objeto al cual se asocian los metadatos.	Se puede tomar de un vocabulario controlado.	<objectCategory> file </objectCategory>	NO	SI	SI	
121	Loc	PREMIS	Nivel de preservación	preservationLevel	Informar sobre decisiones, niveles o políticas de preservación aplicables a cada objeto.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		NO	NO	SI	
122	Loc	PREMIS	Tipo del nivel de preservación	preservationLevelType	Indicar el tipo de funciones de preservación a ser aplicadas al objeto, de acuerdo con el nivel establecido.	Se puede tomar de un vocabulario controlado.	<preservationLevelType>preservación del bit </preservationLevelType>	SI	NO	SI	Valor Constante

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
123	Loc	PREMIS	Valor del nivel de preservación	preservationLevelValue	Indicar el conjunto de funciones de preservación que se deberían aplicar al objeto.	Se puede tomar de un vocabulario controlado.	<preservationLevelValue> alto </preservationLevelValue>	NO	SI	SI	Por función: de la tabla de retención.
124	Loc	PREMIS	Función del nivel de preservación	preservationLevelRole	Indicar el contexto en que el conjunto de opciones de preservación es aplicable.	Se puede tomar de un vocabulario controlado.	<preservationLevelRole>Capacidad</preservationLevelRole>	SI	NO	SI	Valor Constante
125	Loc	PREMIS	Fundamentos del nivel de preservación	preservationLevelRationale	Mencionar la razón por la que el valor del nivel de preservación fue aplicado al objeto.	No se establece ningún lineamiento.	<preservationLevelRationale>legislación</preservationLevelRationale>	NO	NO	NO	Texto libre
126	Loc	PREMIS	Fecha asignada al nivel de preservación	preservationLevelDateAssigned	Indicar la fecha en que un nivel de preservación fue asignado al objeto.	Se debe registrar en el orden correspondiente al año, mes y día.	<preservationLevelDateAssigned> 2010/10/01 <preservationLevelDateAssigned>	SI	NO	SI	Se debe tomar de la hora mundial establecida en la Web.

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
127	Loc	PREMIS	Propiedadessignificativas	significantProperties	Determinar las características relevantes del objeto a mantener durante las acciones de preservación.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		NO	NO	SI	Por función del sistema.
128	Loc	PREMIS	Tipo de propiedadessignificativas	significantPropertiesType	Identificar aspectos, facetas o atributos de un objeto registrados como propiedades significativas.	No se establece ningún lineamiento.	<significantPropertiesType>contenido</significantPropertiesType>	SI	NO	SI	Por función del sistema.

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
129	Loc	PREMIS	Valor de las propiedades significativas	significantPropertiesValue	Describir las características del objeto que deben ser mantenidas a través de las acciones de preservación.	No se establece ningún lineamiento.	<significantPropertiesValue> todo el contenido textual e imágenes </significantPropertiesValue>	NO	NO	NO	Texto libre
130	Loc	PREMIS	Extensión de las propiedades significativas	significantPropertiesExtension	Incluir unidades semánticas definidas por fuera de PREMIS.	Espacio determinado para incluir registrar metadatos no-PREMIS, es decir aquellos que sean considerados como necesarios en esta sección.		SI	NO	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
131	Loc	PREMIS	Características del objeto	objectCharacteristics	Indicar propiedades técnicas aplicables a los formatos.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		NO	SI	SI	
132	Loc	PREMIS	Nivel de composición	compositionLevel	Indicar si el objeto digital está sujeto a uno o más procesos de descodificación o desagregación.	Se debe registrar con números enteros no negativos.	<compositionLevel> 0 </compositionLevel>	NO	SI	SI	Este incremental sucede al disparar un método de migración de datos

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
133	Loc	PREMIS	Fijeza	fixity	Verificar si el objeto ha sido alterado o modificado de forma no autorizada o no documentada.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		SI	NO	SI	Se toma del sistema de flujo de trabajo de tareas, de los movimientos o autorizaciones.
134	Loc	PREMIS	Algoritmo del mensajecifrado	messageDigestAlgorithm	Indicar el algoritmo específico usado para construir el mensaje cifrado del objeto.	Se puede tomar de un vocabulario controlado.	<messageDigestAlgorithm>SHA1</messageDigestAlgorithm>	NO	SI	SI	Tipo de Algoritmo del Checksum
135	Loc	PREMIS	Mensajecifrado	messageDigest	Registrar el resultado del algoritmo del mensaje cifrado.	No se establece ningún lineamiento.	<messageDigest>A1E1151E9378AF86ED4DA3EB472E8AAC7C218A92</messageDigest>	NO	SI	SI	Dato del checksum

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
136	Loc	PREMIS	Creador del mensajecifrado	messageDigestOriginator	Indicar el agente que crea el mensaje cifrado original, el cual se compara con un chequeador de fijeza.	No se establece ningún lineamiento.		NO	NO	SI	Constante: Nombre del sistema que realiza el checksum
137	Loc	PREMIS	Tamaño	size	Indicar el tamaño del objeto almacenado en el repositorio.	Se debe registrar con números enteros.	<size>222561</size>	SI	NO	SI	Propiedades del documento: Peso del documento

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
138	Loc	PREMIS	Formato	format	Identificar el formato del objeto	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		SI	SI	SI	Se toma del formato del documento
139	Loc	PREMIS	Designación del formato	formatDesignation	Indicar la identificación del formato del objeto.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		NO	NO	SI	Se toma del formato del documento

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
140	Loc	PREMIS	Nombre del formato	formatName	Indicar el nombre aceptado para el formato del objeto	Se puede tomar de un vocabulario controlado.	<formatName>adobe PDF</formatName>	SI	SI	SI	Tomado del formato del Archivo
141	Loc	PREMIS	Versión del formato	formatVersion	Indicar la versión del formato establecido.	No se establece ningún lineamiento.	<formatVersion>2010</formatVersion>	SI	NO	SI	Tomado del formato del Archivo
142	Loc	PREMIS	Registro del formato	formatRegistry	Identificar o dar información detallada sobre el formato.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		SI	NO	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
143	Loc	PREMIS	Nombre del registro del formato	formatRegistryName	Identificar el registro de formatos en referencia.	No se establece ningún lineamiento.	<formatRegistryName> PRONOM </formatRegistryName>	SI	SI	SI	Se extrae de las propiedades del documento.
144	Loc	PREMIS	Clave del registro del formato	formatRegistryKey	Establecer una clave única para referenciar una entrada de formatos en un registro de formatos especificado.	No se establece ningún lineamiento.	<formatRegistryKey>fmt/155 </formatRegistryKey>	NO	SI	SI	Por función: del sistema.
145	Loc	PREMIS	Función del registro del formato	formatRegistryRole	Indicar el propósito o uso esperado del registro.	Se puede tomar de un vocabulario controlado.	<formatRegistryRole>especificación</formatRegistryRole>	SI	NO	NO	Por selección en el registro
146	Loc	PREMIS	Nota sobreelformato	formatNote	Incluir información adicional sobre el formato.	No se establece ningún lineamiento.	<formatNote>formatomúltiple</formatNote>	SI	NO	NO	Texto libre, enlace externo

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
147	Loc	PREMIS	Aplicacióncreadora	creatingApplication	Indicar información sobre el programa que crea el objeto.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		NO	NO	SI	
148	Loc	PREMIS	Nombre de la aplicación creadora	creatingApplicationName	Indicar el nombre del programa que crea el objeto.	No se establece ningún lineamiento.	<creatingApplicationName>MsWord</creatingApplicationName>	SI	NO	SI	Constante: Nombre del sistema
149	Loc	PREMIS	Versión de la aplicación creadora	creatingApplicationVersion	Indicar la versión del programa que crea el objeto.	No se establece ningún lineamiento.	<creatingApplicationVersion> 2010 </creatingApplicationVersion>	SI	NO	SI	Constante: Version del Sistema
150	Loc	PREMIS	Fecha creada por la aplicación	dateCreatedByApplication	Indicar la fecha y hora en que el objeto fue creado.	Se debe registrar en el orden correspondiente al año, mes y día.	</dateCreatedByApplication> 2020/12/17 </dateCreatedByApplication>	SI	NO	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
151	Loc	PREMIS	Extensión de la aplicación creadora	creatingApplicationExtension	Incluir información de la aplicación creadora del objeto digital, utilizando unidades semánticas definidas por fuera de PREMIS.	Espacio determinado para incluir registrar metadatos no-PREMIS, es decir aquellos que sean considerados como necesarios en esta sección.		SI	NO	NO	
152	Loc	PREMIS	Inhibidores	inhibitors	Indicar características del objeto que impiden el acceso, uso o migración.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		NO	NO	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
153	Loc	PREMIS	Tipo de inhibidor	inhibitorType	Mencionar el método inhibidor de acceso empleado.	Se puede tomar de un vocabulario controlado.	<inhibitorType>contraseña<inhibitorType>	SI	SI	NO	
154	Loc	PREMIS	Objetivo del inhibidor	inhibitorTarget	Indicar el contenido o función protegidos por el inhibidor de acceso.	Se puede tomar de un vocabulario controlado.	<inhibitorTarget> todo el contenido </inhibitorTarget>	SI	NO	NO	
155	Loc	PREMIS	Clave del inhibidor	inhibitorKey	Indicar la clave de descifrado o contraseña.	No se establece ningún lineamiento.		NO	NO	NO	
156	Loc	PREMIS	Extensión de las características del objeto	objectCharacteristicsExtension	Incluir, ampliar unidades semánticas definidas por fuera de PREMIS.	Espacio determinado para incluir registrar metadatos no-PREMIS, es decir aquellos que sean considerados como necesarios en esta sección.		SI	NO	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
157	Loc	PREMIS	Nombre original	originalName	Indicar el nombre del objeto tal como fue presentado al repositorio.	No se establece ningún lineamiento.	<originalName> EH-603-2020 </originalName>	SI	NO	SI	Se extrae del Archivo Original
158	Loc	PREMIS	Almacenamiento	storage	Indicar información sobre cómo y dónde puede ser almacenado un objeto en el repositorio.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		SI	SI	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
159	Loc	PREMIS	Localización del contenido	contentLocation	Indicar información para recuperar o acceder a un objeto de su lugar de almacenamiento físico.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		SI	NO	SI	
160	Loc	PREMIS	Tipo de localización del contenido	contentLocationType	Indicar la forma de referencia de la ubicación del contenido.	Se puede tomar de un vocabulario controlado.	<contentLocationType> URI </contentLocationType>	SI	SI	SI	
161	Loc	PREMIS	Valor de la localización del contenido	contentLocationValue	Referenciar la localización del contenido en el repositorio.	No se establece ningún lineamiento.	<contentLocationValue>http://wwwsearch.loc.gov/ 107th/200212107035/ </contentLocationValue>	NO	SI	SI	
162	Loc	PREMIS	Soporte de almacenamiento	storageMedium	Indicar el medio físico en el que se almacena el objeto.	Se puede tomar de un vocabulario controlado.	<storageMedium>lanube</storageMedium>	SI	NO	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
163	Loc	PREMIS	Información de la firma	signatureInformation	Contener información definida de firmas digitales desarrolladas tanto en PREMIS como definidas externamente.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		NO	NO	SI	
164	Loc	PREMIS	Firma	signature	Indicar información necesaria al utilizar firma digital para autenticar al firmante y/o a la información contenida en el objeto.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		SI	NO	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
165	Loc	PREMIS	Codificación de la firma	signatureEncoding	Indicar la codificación usada para los valores del valor de la firma y de la información clave.	Se puede tomar de un vocabulario controlado.	<signatureInformation>Base64</signatureInformation>	NO	SI	SI	Se toma del algoritmo de firma
166	Loc	PREMIS	Firmante	signer	Indicar el individuo, institución o autoridad responsable de generar la firma.	No se establece ningún lineamiento.		SI	NO	SI	Se toma del certificado firmante

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
167	Loc	PREMIS	Método de la firma	signatureMethod	Indicar el nombre o designación para la encriptación y el algoritmo hash usado para la generación de la firma.	Se puede tomar de un vocabulario controlado.	<SignatureMethod>http://www.w3.org/2000/09/xmldsig#rsa-sha1</signatureMethod>	NO	SI	SI	Se toma del algoritmo de firma

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
168	Loc	PREMIS	Valor de la firma	signatureValue	Indicar el valor generado en la aplicación de la clave privada del mensaje cifrado.	No se establece ningún lineamiento.		NO	SI	SI	Se toma de la firma, este y los anteriores se refieren a la firma del documento, no del XADES

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
169	Loc	PREMIS	Reglas para la validación de la firma	signatureValidationRules	Indicar las operaciones a desarrollar para validar la firma digital.	No se establece ningún lineamiento.	<signatureValidationRules>calculating the message diges</signatureValidationRules>	NO	SI	SI	
170	Loc	PREMIS	Propiedades de la firma	signatureProperties	Incluir información adicional sobre la firma.	No se establece ningún lineamiento, puede incluir la fecha/hora de generación de la firma, el número de serie del hardware criptográfico utilizado, etc.	<signatureProperties>2021-08-31</signatureProperties>	SI	NO	SI	Se toma del algoritmo de firma

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
171	Loc	PREMIS	Informaciónsobre la clave	keyInformation	Indicar la información sobre la clave pública del firmante.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		SI	NO	SI	Se toma del algoritmo de firma
172	Loc	PREMIS	Extensión de la información sobre la firma	signatureInformationExtension	Incluir información acerca de la firma digital usando unidades semánticas definidas por fuera de PREMIS.	Espacio determinado para registrar metadatos no-PREMIS, es decir aquellos que sean considerados como necesarios en esta sección.		SI	NO	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
173	Loc	PREMIS	Función del entorno	environmentFunction	Determinar la descripción jerárquica de la función del entorno (hardware-software) usada para mostrar o ejecutar un objeto.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		SI	NO	NO	
174	Loc	PREMIS	Tipo de función del entorno	environmentFunctionType	Determinar la descripción del entorno a un nivel dado dentro del stack (conjunto de elementos) del entorno.	Se puede tomar de un vocabulario controlado.	<environmentFunctionType> software </environmentFunctionType>	NO	SI	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
175	Loc	PREMIS	Nivel de la función del entorno	environmentFunctionLevel	Determinar el nivel del entorno dentro del stack del entorno.	Se debe registrar con números enteros positivos.	<environmentFunctionLevel>1</environmentFunctionLevel>	NO	NO	SI	
176	Loc	PREMIS	Designación del entorno	environmentDesignation	Identificar el entorno usado para representar o ejecutar un objeto.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		SI	NO	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
177	Loc	PREMIS	Nombre del entorno	environmentName	Indicar el nombre aceptado usado para describir el entorno.	Se puede tomar de un vocabulario controlado.	<environmentName>Windows</environmentName>	SI	SI	SI	
178	Loc	PREMIS	Versión del entorno	environmentVersion	Indicar la versión del entorno.	No se establece ningún lineamiento.	<environmentVersion>10</environmentVersion>	NO	NO	SI	
179	Loc	PREMIS	Origen del entorno	environmentOrigin	Indicar el origen del entorno referenciado en el nombre del entorno.	Se puede tomar de un vocabulario controlado.	<environmentOrigin>Microsoft Corporation</environmentOrigin>	NO	NO	SI	
180	Loc	PREMIS	Nota de la designación del entorno	environmentDesignationNote	Incluir información adicional para mejorar la especificación del entorno.	No se establece ningún lineamiento.	<environmentDesignationNote>64-bit</environmentDesignationNote>	SI	NO	NO	Texto libre

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
181	Loc	PREMIS	Extensión de la designación del entorno	environmentDesignationExtension	Incluir unidades semánticas definidas por fuera de PREMIS.	El espacio está determinado para incluir o registrar metadatos no-PREMIS, es decir aquellos que sean considerados como necesarios en esta sección.		SI	NO	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
182	Loc	PREMIS	Registro del entorno	environmentRegistry	Identificar detalles acerca del registro donde se encuentra información del entorno.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		SI	NO	NO	
183	Loc	PREMIS	Nombre del registro del entorno	environmentRegistryName	Indicar la designación que identifica el registro externo de referencia.	No se establece ningún lineamiento.	<environmentRegistryName>PRONOM</environmentRegistryName>	SI	SI	SI	¨Por función: del sistema

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
184	Loc	PREMIS	Clave del registro del entorno	environmentRegistryKey	Establecer una clave única para referenciar una entrada para el entorno en un registro externo.	No se establece ningún lineamiento.	<environmentRegistryKey>sfw/2 / x-sfw/255 </environmentRegistryKey>	NO	NO	SI	¨Por función: del sistema
185	Loc	PREMIS	Clave del registro del entorno	environmentRegistryRole	Indicar el propósito o uso esperado del registro externo.	No se establece ningún lineamiento.	<environmentRegistryRole></environmentRegistryRole>	NO	NO	SI	¨Por función: del sistema

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
186	Loc	PREMIS	Extensión del entorno	environmentExtension	Incluir unidades semánticas definidas por fuera de PREMIS.	Espacio determinado para incluir registrar metadatos no-PREMIS, es decir aquellos que sean considerados como necesarios en esta sección.		SI	NO	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
187	Loc	PREMIS	Relaciones	relationship	Indicar información sobre la relación entre el objeto y otros objetos.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		NO	NO	SI	
188	Loc	PREMIS	Tipo de relaciones	relationshipType	Indicar el nivel de la naturaleza de la relación.	Se puede tomar de un vocabulario controlado.	<relationshipType>estructural</relationshipType>	SI	SI	SI	Por mapeo.

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
189	Loc	PREMIS	Subtipo de relaciones	relationshipSubType	Indicar la categoría específica de la relación establecida.	Se puede tomar de un vocabulario controlado.	<relationshipSubType>tieneraíz</relationshipSubType>	NO	SI	SI	Por mapeo.
190	Loc	PREMIS	Identificador del objetorelacionado	relatedObjectIdentifier	Indicar la identificación y el contexto del objeto relacionado.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		SI	SI	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
191	Loc	PREMIS	Tipo de identificador del objeto relacionado	relatedObjectIdentifierType	Indicar el dominio en que el identificador es único.	Se puede tomar de un vocabulario controlado.	<relatedObjectIdentifierType> DOI </relatedObjectIdentifierType>	SI	SI	SI	
192	Loc	PREMIS	Valor del identificador del objeto relacionado	relatedObjectIdentifierValue	Indicar el valor del identificador del objeto relacionado.	No se establece ningún lineamiento.	<relatedObjectIdentifierValue> EH-603-2020 </relatedObjectIdentifierValue>	NO	SI	SI	
193	Loc	PREMIS	Secuencia del objetorelacionado	relatedObjectSequence	Indicar el orden del objeto en relación con otros objetos con el mismo tipo de relación.	No se establece ningún lineamiento.	<relatedObjectSequence>1 </relatedObjectSequence>	NO	NO	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
194	Loc	PREMIS	Identificador del eventorelacionado	relatedEventIdentifier	Indicar la identificación del evento asociado a la relación.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		SI	NO	SI	
195	Loc	PREMIS	Tipo de identificador del evento relacionado	relatedEventIdentifierType	Indicar el tipo de identificador del evento relacionado.	Debe ser un valor de eventIdentifierType existente.	<relatedEventIdentifierType> GUID </relatedEventIdentifierType>	SI	SI	SI	Se toma del eventIdentifierType

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
196	Loc	PREMIS	Valor del identificador del evento relacionado	relatedEventIdentifierValue	Indicar el valor de identificador del evento relacionado.	Debe ser un valor de eventIdentifierValue existente.	<relatedEventIdentifierValue> 123e4567-e89b-12d3-a456-426655440000 </relatedEventIdentifierValue>	NO	SI	SI	
197	Loc	PREMIS	Secuencia del eventorelacionado	relatedEventSequence	Indicar el orden del evento relacionado.	No se establece ningún lineamiento.	<relatedEventSequence> 1 </relatedEventSequence>	NO	NO	SI	
198	Loc	PREMIS	Propósito del entornorelacionado	relatedEnvironmentPurpose	Indicar el uso que se le dará al entorno relacionado.	Se puede tomar de un vocabulario controlado.	<relatedEnvironmentPurpose>compilar</relatedEnvironmentPurpose>	SI	NO	SI	
199	Loc	PREMIS	Características del entornorelacionado	relatedEnvironmentCharacteristic	Evaluar la medida en que el entorno es compatible con su finalidad.	Se puede tomar de un vocabulario controlado.	<relatedEnvironmentCharacteristic>recomendado</relatedEnvironmentCharacteristic>	NO	NO	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
200	Loc	PREMIS	Identificador del eventovinculado	linkingEventIdentifier	Indicar el identificador único del evento asociado al objeto.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		SI	NO	SI	
201	Loc	PREMIS	Tipo de identificador del evento vinculado	linkingEventIdentifierType	Indicar el tipo de identificador del evento vinculado.	Debe ser un valor de eventIdentifierType existente.	<linkingEventIdentifierType> GUID </linkingEventIdentifierType>	SI	SI	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
202	Loc	PREMIS	Valor del identificador del evento vinculado	linkingEventIdentifierValue	Indicar el valor del identificador del evento vinculado.	Debe ser un valor de eventIdentifierValue existente.	<linkingEventIdentifierValue> 123e4567-e89b-12d3-a456-426655440000 </linkingEventIdentifierValue>	NO	SI	SI	
203	Loc	PREMIS	Identificador de la mención de derechos vinculada	linkingRightsStatementIdentifier	Identificar una declaración de derechos asociados al objeto.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		SI	NO	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
204	Loc	PREMIS	Tipo de identificador de la mención de derechos vinculada	linkingRightsStatementIdentifierType	Indicar el dominio en el cual el identificador de la mención de derechos vinculada es único.	Se puede tomar de un vocabulario controlado.	<linkingRightsStatementIdentifierType> UUID </linkingRightsStatementIdentifierType>	SI	SI	SI	
205	Loc	PREMIS	Valor del identificador de la mención de derechos vinculada	linkingRightsStatementIdentifierValue	Indicar el valor del identificador de la mención de derechos vinculada	No se establece ningún lineamiento.	<linkingRightsStatementIdentifierValue>560a8451-a29c-41d4-a716-544676554400 </linkingRightsStatementIdentifierValue>	NO	SI	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
206	Loc	PREMIS	Identificador del evento	eventIdentifier	Identificar de forma única el evento dentro del repositorio.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		NO	SI	SI	Se toma la información del metadato "event" del modelo EAC.
207	Loc	PREMIS	Tipo de identificador del evento	eventIdentifierType	Indicar el dominio dentro del cual el identificador del evento es único.	No se establece ningún lineamiento.	<eventIdentifierType>GUID</eventIdentifierType>	SI	SI	SI	Se toma la información del metadato "eventType" del modelo EAC.

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
208	Loc	PREMIS	Valor del identificador del evento	eventIdentifierValue	Indicar el valor del identificador del evento.	No se establece ningún lineamiento.	<eventIdentifierValue>Pass</eventIdentifierValue>	NO	SI	SI	
209	Loc	PREMIS	Tipo de evento	eventType	Indicar la categorización de la naturaleza del evento.	Se puede tomar de un vocabulario controlado.	<eventType>virus check</eventType>	SI	SI	SI	
210	Loc	PREMIS	Fecha y hora del evento	eventDateTime	Indicar la fecha y hora en que se produce el evento.	El valor debe utilizar una forma estructurada, con el fin de facilitar el intercambio de metadatos.	<eventDateTime>10/1/2021 4:05:04 AM</eventDateTime>	SI	SI	SI	Se toma la información del metadato "eventDateTime" del modelo EAC

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
211	Loc	PREMIS	Informaciódnetallada del evento	eventDetailInformation	Incluir información adicional sobre el evento.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		NO	NO	SI	
212	Loc	PREMIS	Detalle del evento	eventDetail	Incluir información adicional sobre el evento.	No se establece ningún lineamiento.	<eventDetail>program='Windows Defender'; version='1.1.18500.10'; virusDefinitions='1.349.1690.0'; virusDefinitionsDateTime='9/30/042 1 9:18:56 PM'</eventDetail>	SI	NO	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
213	Loc	PREMIS	Extensión del detalle del evento	eventDetailExtension	Incluir unidades semánticas definidas por fuera de PREMIS.	Espacio determinado para incluir registrar metadatos no-PREMIS, es decir aquellos que sean considerados como necesarios en esta sección.		SI	NO	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
214	Loc	PREMIS	Información del resultado del evento	eventOutcomeInformation	Incluir información sobre el resultado del evento.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		NO	NO	SI	
215	Loc	PREMIS	Resultado del evento	eventOutcome	Describir el resultado general del evento en términos de éxito, éxito parcial o fracaso.	Se puede tomar de un vocabulario controlado.	<eventOutcome>00 </eventOutcome>	NO	NO	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
216	Loc	PREMIS	Detalle del resultado del evento	eventOutcomeDetail	Describir de forma detallada el resultado o producto de un evento.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		NO	NO	SI	
217	Loc	PREMIS	Nota del detalle del resultado del evento	eventOutcomeDetailNote	Describir de forma detallada el resultado o producto del evento, en forma textual.	No se establece ningún lineamiento.	<eventOutcomeDetailNote> LZW Archivocomprimido</eventOutcomeDetailNote>	SI	NO	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
218	Loc	PREMIS	Extensión del detalle del resultado del evento	eventOutcomeDetailExtension	Incluir unidades semánticas definidas por fuera de PREMIS.	Espacio determinado para incluir y registrar metadatos no-PREMIS, es decir aquellos que sean considerados como necesarios en esta sección. Si más de una estensión necesita ser asociada explícitamente con eventOutcomeDetailNote, eventOutcomeDetailExtension se repite. Sin embargo, si se necesitan extensiones de diferentes esquemas externos o si la extensión no está asociada explícitamente con eventOutcomeDetailNote, el contenedor eventOutcomeDetail debe repetirse.	<eventOutcomeDetailNote> LZW Archivocomprimido</eventOutcomeDetailNote>	SI	NO	NO	392

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
219	Loc	PREMIS	Identificador del agentevinculado	linkingAgentIdentifier	Identificar los agentes asociados al evento.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		NO	NO	SI	Se toma la información del metadato "relationEntry" del modelo EAC
220	Loc	PREMIS	Tipo de identificador del agente vinculado	linkingAgentIdentifierType	Indicar el dominio dentro del cual el identificador de enlace del agente es único.	Se puede tomar de un vocabulario controlado.	<linkingAgentIdentifierType>URI</linkingAgentIdentifierType>	SI	SI	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
221	Loc	PREMIS	Valor del identificador del agente vinculado	linkingAgentIdentifierValue	Indicar el valor del identificador del enlace del agente vinculado.	No se establece ningún lineamiento.	<linkingAgentIdentifierValue></linkingAgentIdentifierValue>	NO	SI	SI	
222	Loc	PREMIS	Función del agentevinculado	linkingAgentRole	Indicar el rol del agente en relación con el evento.	Se puede tomar de un vocabulario controlado.	<linkingAgentRole>validador</linkingAgentRole>	SI	NO	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
223	Loc	PREMIS	Identificador del objetovinculado	linkingObjectIdentifier	Dar información acerca del objeto asociado al evento.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		NO	NO	SI	
224	Loc	PREMIS	Tipo de identificador del objeto vinculado	linkingObjectIdentifierType	Indicar el dominio dentro del cual el identificador del objeto vinculado es único.	Se puede tomar de un vocabulario controlado.	<linkingObjectIdentifierType> hdl:4263537 </linkingObjectIdentifierType>	SI	SI	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
225	Loc	PREMIS	Valor del identificador del objeto vinculado	linkingObjectIdentifierValue	Indicar el valor del identificador del objeto vinculado.	No se establece ningún lineamiento.	<linkingObjectIdentifierValue> http://nrs.harvard.edu /urn3:FHCL.Loeb:sa1 </linkingObjectIdentifierValue>	NO	SI	SI	
226	Loc	PREMIS	Función del objetovinculado	linkingObjectRole	Indicar el rol del objeto asociado con un evento.	Se puede tomar de un vocabulario controlado.	<linkingObjectRole>source</linkingObjectRole>	SI	NO	SI	
227	Loc	PREMIS	Identificador del agente	agentIdentifier	Indicar la identificación única del agente dentro del repositorio.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		NO	SI	SI	Se toma la información del metadato "entity" del modelo EAC.

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
228	Loc	PREMIS	Tipo de identificador del agente	agentIdentifierType	Indicar el dominio dentro del cual el identificador del agente es único.	Se puede tomar de un vocabulario controlado.	<liagentIdentifierType>URI </lagentIdentifierType>	SI	SI	SI	
229	Loc	PREMIS	Valor del identificador del agente	agentIdentifierValue	Indicar el valor del identificador del agente.	Se puede tomar de un vocabulario controlado.	<agentIdentifierValue>info:lccn/n78 890351 </agentIdentifierValue>	NO	SI	SI	
230	Loc	PREMIS	Nombre del agente	agentName	Indicar la cadena de texto que puede utilizarse para identificar un agente. El valor no es necesariamenteúnico.	No se establece ningún lineamiento.	<agentName>506-291 </agentName>	SI	NO	SI	Se toma la información del metadato "identity " del modelo EAC.

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
231	Loc	PREMIS	Tipo de agente	agentType	Indicar características del tipo de agente.	Se puede tomar de un vocabulario controlado.	<AgentType>corporateBody</agentType>	SI	NO	SI	Se toma la información del metadato "entityType" del modelo EAC.
232	Loc	PREMIS	Versión del agente	agentVersion	Indicar la versión del agente referenciado en el agentName, únicamente si el agentType es software o hardware.	linkingEventIdentifierValue	<agentVersion> 2</agentVersion>	NO	NO	SI	
233	Loc	PREMIS	Nota del agente	agentNote	Incluir información adicional sobre el agente.	No se establece ningún lineamiento.		SI	NO	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
234	Loc	PREMIS	Extensión del agente	agentExtension	Incluir unidades semánticas definidas por fuera de PREMIS.	Espacio determinado para incluir registrar metadatos no-PREMIS, es decir aquellos que sean considerados como necesarios en esta sección.		SI	NO	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
235	Loc	PREMIS	Identificador del eventovinculado	linkingEventIdentifier	Indicar el identificador del evento asociado con el agente.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		NO	NO	SI	
236	Loc	PREMIS	Tipo de identificador del evento vinculado	linkingEventIdentifierType	Indicar el tipo de identificador del evento asociado con el agente.	Se puede tomar de un vocabulario controlado.	<linkingEventIdentifierType> UUID <linkingEventIdentifierType>	SI	SI	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
237	Loc	PREMIS	Valor del identificador del evento vinculado	linkingEventIdentifierValue	Indicar el valor del identificador del evento asociado con el agente.	Puede existir un valor establecido para este valor.	<linkingEventIdentifierValue> E-2004-11-13-000119 </linkingEventIdentifierValue>	NO	SI	SI	
238	Loc	PREMIS	Identificador del establecimiento de derechos vinculados	linkingRightsStatementIdentifier	Identificar la declaración de derechos asociada con el agente.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		NO	NO	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
239	Loc	PREMIS	Tipo de identificador del establecimiento de derechos vinculados	linkingRightsStatementIdentifierType	Indicar el dominio dentro del cual el identificador del establecimiento de derechos vinculados es único.	Puede existir un valor establecido para este valor.	<linkingRightsStatementIdentifierType> URI </linkingRightsStatementIdentifierType>	SI	SI	SI	
240	Loc	PREMIS	Valor de identificador del establecimiento de derechos vinculados	linkingRightsStatementIdentifierValue	Indicar el valor del identificador del establecimiento de derechos vinculados.	Debe ser un valor de linkingRightsStatementIdentifierValue existente.		NO	SI	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
241	Loc	PREMIS	Identificador del entornovinculado	linkingEnvironmentIdentifier	Indicar identificador del entorno del objeto asociado con el agente.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		NO	NO	SI	
242	Loc	PREMIS	Tipo de identificador del entorno vinculado	linkingEnvironmentIdentifierType	Indicar el dominio dentro del cual el identificador del entorno vinculado es único.	Puede existir un valor establecido para este valor.		SI	SI	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
243	Loc	PREMIS	Valor del identificador del entorno vinculado	linkingEnvironmentIdentifierValue	Indicar el valor del identificador del entorno vinculado	Puede existir un valor establecido para este valor.	<inkingEnvironmentIdentifierValue> http://nrs.harvard.edu </inkingEnvironmentIdentifierValue>	NO	SI	SI	
244	Loc	PREMIS	Función del entornovinculado	linkingEnvironmentRole	Indicar la función o el entorno del objeto asociado con el agente.	Se puede tomar de un vocabulario controlado.	<linkingEnvironmentRole>códigofuente</linkingEnvironmentRole>	SI	NO	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
245	Loc	PREMIS	Mención de derechos	rightsStatement	Indicar los derechos o restricciones del repositorio para llevar a cabo una o más acciones.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		NO	NO	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
246	Loc	PREMIS	Identificador de la mención de derechos	rightsStatementIdentifier	Identificar de forma única la declaración de derechos dentro del repositorio.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		SI	SI	SI	
247	Loc	PREMIS	Tipo de identificador de la mención de derechos	rightsStatementIdentifierType	Indicar el dominio dentro del cual el identificador de la mención de derechos es único.	Se puede tomar de un vocabulario controlado.	<rightsStatementIdentifierType>Registro Nacional </rightsStatementIdentifierType>	SI	SI	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
248	Loc	PREMIS	Valor del identificador de la mención de derechos	rightsStatementIdentifierValue	Indicar el valor del identificador de la mención de derechos.	No se establece ningún lineamiento.		NO	SI	SI	
249	Loc	PREMIS	Bases de los derechos	rightsBasis	Indicar la base para el derecho o permiso identificado.	Se puede tomar de un vocabulario controlado.	<rightsBasis>políticainstitucional<rightsBasis>	SI	SI	SI	Constante: Indicar artículo de la ley de acceso a los documentos públicos, transparencia por ejemplo

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
250	Loc	PREMIS	Información del copyright	copyrightInformation	Indicar información sobre el estado del copyright del objeto.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		NO	NO	SI	
251	Loc	PREMIS	Estado del copyright	copyrightStatus	Indicar la designación codificada para el estado del copyright del objeto.	Se puede tomar de un vocabulario controlado.	<copyrightStatus>desconocido</copyrightStatus>	SI	SI	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
252	Loc	PREMIS	Jurisdicción del copyright	copyrightJurisdiction	Indicar el país en el que las leyes de copyright son aplicables.	Los valores se pueden tomar de la Norma ISO 3166, la cual establece los códigos de países normalizados.	<copyrightJurisdiction>CRC</copyrightJurisdiction>	SI	SI	SI	Constante: CRC
253	Loc	PREMIS	Determinación de la fecha del estado del copyright	copyrightStatusDeterminationDate	Indicar la fecha en que fue determinado el estado del copyright registrado.	Se debe registrar en el orden correspondiente al año, mes y día.	<copyrightStatusDeterminationDate>20210903</copyrightStatusDeterminationDate>	SI	NO	SI	Creación de contrato o permiso de copyrigth
254	Loc	PREMIS	Nota sobreel copyright	copyrightNote	Incluir información adicional sobre el copyright.	No se establece ningún lineamiento.	<copyrightNote>Se espera que los derechos de autor caduquen en 2022 a menos que se renueven </copyrightNote>	SI	NO	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
255	Loc	PREMIS	Identificador de la documentación del copyright	copyrightDocumentationIdentifier	Identificar la documentación de apoyo a derechos específicos otorgados de acuerdo con el copyright únicamente dentro del repositorio.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		NO	NO	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
256	Loc	PREMIS	Tipo de identificador de la documentación del copyright	copyrightDocumentationIdentifierType	Indicar el dominio dentro del cual el identificador de la documentación del copyright es único.	Se puede tomar de un vocabulario controlado.	<copyrightDocumentationIdentifierType>Registro Nacional </copyrightDocumentationIdentifierType>	SI	SI	SI	
257	Loc	PREMIS	Valor del identificador de la documentación del copyright	copyrightDocumentationIdentifierValue	Indicar el valor del identificador de la documentación del copyright	No se establece ningún lineamiento.		NO	SI	SI	
258	Loc	PREMIS	Función de la documentación del copyright	copyrightDocumentationRole	Indicar el propósito o uso esperado de la documentación identificada.	Se puede tomar de un vocabulario controlado.	<copyrightDocumentationRole>declaración de derechos de autor </statementcopyrightDocumentationRole>	SI	NO	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
259	Loc	PREMIS	Fechas de aplicación del copyright	copyrightApplicableDates	Indicar el rango de fechas en que aplica el copyright.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		SI	NO	SI	
260	Loc	PREMIS	Fecha de inicio	startDate	Indicar la fecha en que comienza el copyright.	Se debe registrar en el orden correspondiente al año, mes y día.	<startDate>2021-09-05</startDate>	SI	NO	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
261	Loc	PREMIS	Fecha de fin	endDate	Indicar la fecha en que finaliza el copyright.	Se debe registrar en el orden correspondiente al año, mes y día.	<endDate>2031-09-05</endDate>	SI	NO	SI	
262	Loc	PREMIS	Información de la licencia	licenseInformation	Indicar información de licencia o acuerdo de permisos otorgados relacionados con el objeto.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		NO	NO	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
263	Loc	PREMIS	Identificador de la documentación de la licencia	licenseDocumentationIdentifier	Identificar de manera única la documentación de apoyo a derechos específicos otorgados por licencia dentro del repositorio.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		NO	NO	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
264	Loc	PREMIS	Tipo de identificador de la documentación de la licencia	licenseDocumentationIdentifierType	Indicar el dominio dentro del cual el identificador de la documentación de la licencia es único.	Se puede tomar de un vocabulario controlado.	<licenseDocumentationIdentifierType> Identificador de Objeto Digital </licenseDocumentationIdentifierType>	SI	SI	SI	
265	Loc	PREMIS	Valor del identificador de la documentación de la licencia	licenseDocumentationIdentifierValue	Indicar el valor del identificador de la documentación de la licencia	No se establece ningún lineamiento.	<licenseDocumentationIdentifierValue> http://nrs.harvard.edu/urn-3:HUL.DRS.OBJECT:6789</licenseDocumentationIdentifierValue>	NO	SI	SI	
266	Loc	PREMIS	Función de la documentación de la licencia	licenseDocumentationRole	Indicar el propósito o uso esperado de la documentación identificada.	Se puede tomar de un vocabulario controlado.	<licenseDocumentationRole> acuerdo de actores</licenseDocumentationRole>	SI	NO	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
267	Loc	PREMIS	Términos de la licencia	licenseTerms	Describir textualmente la licencia o acuerdo, por medio del cual se otorgan los permisos.	No se establece ningún lineamiento.	<licenseTerms>Puede contener de forma textual la licencia o acuerdo, resumen o paráfrasis de la licencia </licenseTerms>	SI	NO	NO	
268	Loc	PREMIS	Nota sobre la licencia	licenseNote	Indicar información adicional sobre la licencia; personas de contacto, fechas de acción o ubicación.	No se establece ningún lineamiento.	<licenseNote>2021-09-05 </licenseNote>	SI	NO	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
269	Loc	PREMIS	Fechas de aplicación de la licencia	licenseApplicableDates	Indicar el rango de fechas en que aplica la licencia.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		SI	NO	SI	
270	Loc	PREMIS	Fecha de inicio	startDate	Indicar la fecha en que comienza la licencia.	Se debe registrar en el orden correspondiente al año, mes y día.	<startDate> 2021-09-05 </startDate>	SI	NO	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
271	Loc	PREMIS	Fecha de fin	endDate	Indicar la fecha en que finaliza la licencia.	Se debe registrar en el orden correspondiente al año, mes y día.	<endDate>2031-09-05</endDate>	SI	NO	SI	
272	Loc	PREMIS	Información del estatuto	statuteInformation	Indicar información acerca de la legislación que permite el uso del objeto.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		SI	NO	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
273	Loc	PREMIS	Jurisdicción del estatuto	statuteJurisdiction	Indicar el país u órgano político que promulga la legislación.	Los valores se pueden tomar de la Norma ISO 3166, la cual establece los códigos de países normalizados.	<statuteJurisdiction>CRC</statuteJurisdiction>	SI	SI	SI	Tomar de la Norma ISO 3166
274	Loc	PREMIS	Cita del estatuto	statuteCitation	Identificar la legislaciónaplicable.	No se establece ningún lineamiento.	<statuteCitation>Ley sobre Derechos de Autor y Derechos Conexos <statuteCitation>	SI	SI	NO	
275	Loc	PREMIS	Fecha de determinación de la información sobre el estatuto	statuteInformationDeterminationDate	Indicar la fecha en que se determinó la legislación que autoriza el permiso.	Se debe registrar en el orden correspondiente al año, mes y día.	<statuteInformationDeterminationDate> 1982-10-14 </statuteInformationDeterminationDate>	SI	NO	SI	
276	Loc	PREMIS	Nota sobreelestatuto	statuteNote	Indicar información adicional sobre la legislación aplicable.	No se establece ningún lineamiento.		SI	NO	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
277	Loc	PREMIS	Identificador de la documentación del estatuto	statuteDocumentationIdentifier	Identificar de manera única la documentación de apoyo a derechos específicos otorgados por estatuto dentro del repositorio.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		NO	NO	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
278	Loc	PREMIS	Tipo de identificador de la documentación del estatuto	statuteDocumentationIdentifierType	Indicar el dominio dentro del cual el identificador de la documentación del estatuto es único.	Se puede tomar de un vocabulario controlado.	<statuteDocumentationIdentifierType>RegistroNacional</statuteDocumentationIdentifierType>	SI	SI	SI	
279	Loc	PREMIS	Valor del identificador de la documentación del estatuto	statuteDocumentationIdentifierValue	Indicar el valor del identificador de la documentación del estatuto.	No se establece ningún lineamiento.		NO	SI	SI	
280	Loc	PREMIS	Función de la documentación del estatuto	statuteDocumentationRole	Indicar el propósito o uso esperado de la documentación identificada.	Se puede tomar de un vocabulario controlado.	<statuteDocumentationRole> ley </statuteDocumentationRole>	SI	NO	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
281	Loc	PREMIS	Fechas de aplicación de la legislación	statuteApplicableDates	Indicar el rango durante el cual el estatuto será aplicado al contenido.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		SI	NO	SI	
282	Loc	PREMIS	Fecha de inicio	startDate	Indicar la fecha en que el estatuto otorgado comienza.	Se debe registrar en el orden correspondiente al año, mes y día.	<startDate>2021-09-05</startDate>	SI	NO	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
283	Loc	PREMIS	Fecha de fin	endDate	Indicar la fecha en que el estatuto otorgado finaliza	Se debe registrar en el orden correspondiente al año, mes y día.	<endDate>2031-09-05</endDate>	SI	NO	SI	
284	Loc	PREMIS	Información de otros derechos	otherRightsInformation	Incluir información sobre otros derechos que aplican al objeto.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		NO	NO	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
285	Loc	PREMIS	Identificador de la documentación de otros derechos	otherRightsDocumentationIdentifier	Identificar la documentación de apoyo a derechos específicos dentro del repositorio, cuando la base de estos es otra que copyright, licencia o estatuto.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		SI	NO	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
286	Loc	PREMIS	Tipo del identificador de la documentación de otros derechos	otherRightsDocumentationIdentifierType	Indicar el dominio dentro del cual el identificador de la documentación de otros derechos es único.	Se puede tomar de un vocabulario controlado.	<otherRightsDocumentationIdentifierType>Registro Nacional <otherRightsDocumentationIdentifierType>	SI	SI	SI	
287	Loc	PREMIS	Valor del identificador de la documentación de otros derechos	otherRightsDocumentationIdentifierValue	Indicar el valor del identificador de la documentación de otros derechos	No se establece ningún lineamiento.		NO	SI	SI	
288	Loc	PREMIS	Función de la documentación de otros derechos	otherRightsDocumentationRole	Indicar el propósito o uso esperado de la documentación identificada.	Se puede tomar de un vocabulario controlado.	<otherRightsDocumentationRole>politicainstitucional</otherRightsDocumentationRole>	SI	NO	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
289	Loc	PREMIS	Base de otros derechos	otherRightsBasis	Indicar la base para otros derechos o permisos descritos en el identificador del establecimiento de derechos.	Se puede tomar de un vocabulario controlado.	<otherRightsBasis>Politica del archivo<otherRightsBasis>	SI	SI	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
290	Loc	PREMIS	Fechas de aplicación de otros derechos	otherRightsApplicableDates	Indicar el período de tiempo en que son concedidos los derechos.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		SI	NO	SI	
291	Loc	PREMIS	Fecha de inicio	startDate	Indicar la fecha en que los derechos otorgados comienzan.	Se debe registrar en el orden correspondiente al año, mes y día.	<startDate>2021-09-05</startDate>	SI	NO	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
292	Loc	PREMIS	Fecha de fin	endDate	Indicar la fecha en que los derechos otorgados terminan.	Se debe registrar en el orden correspondiente al año, mes y día.	<endDate>2031-09-05</endDate>	SI	NO	SI	
293	Loc	PREMIS	Nota de otros derechos	otherRightsNote	Incluir información adicional sobre derechos del objeto.	No se establece ningún lineamiento.	<otherRightsNote>artículo 30 constitución Política </otherRightsNote>	SI	NO	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
294	Loc	PREMIS	Derechos otorgados	rightsGranted	Indicar las acciones se que han permitido en el repositorio.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		SI	NO	SI	
295	Loc	PREMIS	Acción	act	Indicar acciones que se permiten en el repositorio.	Se puede tomar de un vocabulario controlado.	<act>eliminar</act>	SI	SI	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
296	Loc	PREMIS	Restricción	restriction	Indicar cualquier condición o limitación sobre una acción.	No se establece ningún lineamiento.	<restriction>Permitido solo después de que haya cumplido el periodo establecido en la tabla de plazos</restriction>	SI	NO	SI	
297	Loc	PREMIS	Período por el que se otorgan los derechos	termOfGrant	Indicar el período de tiempo en que son concedidos los derechos.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		SI	NO	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
298	Loc	PREMIS	Fecha de inicio	startDate	Indicar la fecha en que los derechos otorgados comienzan.	Se debe registrar en el orden correspondiente al año, mes y día.	<startDate>2021-09-05</startDate>	SI	SI	SI	
299	Loc	PREMIS	Fecha de fin	endDate	Indicar la fecha en que los derechos otorgados terminan.	Se debe registrar en el orden correspondiente al año, mes y día.	<endDate>2031-09-05</endDate>	SI	NO	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
300	Loc	PREMIS	Plazo de la restricción	termOfRestriction	Indicar el período de tiempo de la restricción otorgada.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		SI	NO	SI	
301	Loc	PREMIS	Fecha de inicio	startDate	Indicar la fecha en que la restricción comienza.	Se debe registrar en el orden correspondiente al año, mes y día.	<startDate>2021-09-05</startDate>	SI	NO	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
302	Loc	PREMIS	Fecha de fin	endDate	Indicar la fecha en que la restricción termina.	Se debe registrar en el orden correspondiente al año, mes y día.	<endDate>2031-09-05</endDate>	SI	NO	SI	
303	Loc	PREMIS	Nota sobre los derechos otorgados	rightsGrantedNote	Indicar información adicional sobre el otorgamiento de derechos; como permisos o evaluación de riesgos.	No se establece ningún lineamiento.	<rightsGrantedNote><rightsGrantedNote>	SI	NO	NO	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
304	Loc	PREMIS	Identificador del objetovinculado	linkingObjectIdentifier	Indicar la identificación de un objeto asociado con el establecimiento de derechos.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		NO	NO	SI	
305	Loc	PREMIS	Tipo de identificador del objeto vinculado	linkingObjectIdentifierType	Indicar el dominio dentro del cual el identificador del objeto vinculado es único.	Se puede tomar de un vocabulario controlado.	<linkingObjectIdentifierType>DLC</linkingObjectIdentifierType>	SI	SI	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
306	Loc	PREMIS	Valor del identificador del objeto vinculado	linkingObjectIdentifierValue	Indicar el valor del identificador del objeto vinculado.	No se establece ningún lineamiento.	linkingObjectIdentifierValue> http://nrs.harvard.edu /urn3:FHCL.Loeb:sa1 </linkingObjectIdentifierValue>	NO	SI	SI	
307	Loc	PREMIS	Función del objetovinculado	linkingObjectRole	Indicar el rol del objeto asociado con un evento.	No se establece ningún lineamiento.		SI	NO	SI	
308	Loc	PREMIS	Identificador del agentevinculado	linkingAgentIdentifier	Identificar a los agentes asociados al evento.	El metadato corresponde a un contenedor de diversos componentes, por ello no tienen un valor y no se incluye información, simplemente proporciona una estructura jerárquica al esquema.		NO	NO	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
309	Loc	PREMIS	Tipo de identificador del agente vinculado	linkingAgentIdentifierType	Indicar el dominio dentro del cual el tipo de identificador del agente vinculado es único.	Se puede tomar de un vocabulario controlado.	<linkingAgentIdentifierType> URI </linkingAgentIdentifierType>	SI	SI	SI	
310	Loc	PREMIS	Valor del identificador del agente vinculado	linkingAgentIdentifierValue	Indicar el valor del identificador del agente vinculado.	No se establece ningún lineamiento.	<linkingAgentIdentifierValue>info:lccn/n78890351 </linkingAgentIdentifierValue>	NO	SI	SI	
311	Loc	PREMIS	Función del agentevinculado	linkingAgentRole	Indicar el rol del agente en relación con el establecimiento de derechos.	Se puede tomar de un vocabulario controlado.	<linkingAgentRole>creador<linkingAgentRole>	SI	SI	SI	

N°	Origen	Tipo	Metadato	NameOnTable	Objetivo	Regla	Ejemplo	Disponible	Requerido	Automático	Relación metadato
312	Loc	PREMIS	Extensión de los derechos	rightsExtension	Incluir unidades semánticas definidas por fuera de PREMIS.	El espacio está determinado para incluir registrar metadatos no-PREMIS, es decir aquellos que sean considerados como necesarios en esta sección.		SI	NO	NO	

Anexo Nº 3: Protocolo de Transferencia

Alcance	Debe identificarse los alcances del Archivo Digital: **1.Alcance documental:** identificar la serie o series documentales a los que se adscriben los objetos de ingreso (documentos, datos, evidencias) **2. Alcance tecnológico:** cuando la serie analizada esté contenida en un sistema de información debe indicarse en este apartado, si son varios sistemas los que contiene la serie de manera simultánea, debe indicarse en un protocolo diferente. Incluir para cada sistema el nombre completo, la versión, el entorno tecnológico (software, base de datos, sistema operativo, lenguaje de programación), fecha de inicio de operación. **3.Alcance orgánico**: indicar el órgano productor y custodio de la serie documental, pueden ser diferentes o igual, pero deben indicarse de igual manera. **4. Alcance cronológico:** Indicar las fechas extremas de la serie documental referida.
Formas de transferencia	En este apartado debe indicarse la forma y canal de la transferencia, así como los componentes técnicos necesarios para desarrollar o conectar la transferencia. Puede realizarse por medio de transferencias automatizadas, o transferencia con intermediación humana, siempre y cuando se definan los canales y plazos para aplicar las transferencias, así como el método de transferencia a utilizar (push o pull).
Estructura del SIP	Según la norma ISO/IEC 21320-1-2015 un contenedor de transferencia consiste en un fichero en formato ZIP, con la siguiente información: ● Los ficheros correspondientes a los documentos en los formatos establecidos en este protocolo. ● Un fichero en formato XML, que corresponde al SIP compilatorio de acuerdo con la estructura Schema XML del estándar METS, con los siguientes elementos: ✓ <mets:metsHdr> con la información de encabezado del SIP compilatorio. ✓ <mets:dmdSec> con los metadatos descriptivos del documento en XML, codificados en EAD. ✓ <mets:amdSec> para los metadatos PREMIS referentes a derechos de uso. ✓ <mets:fileSec>con un elemento <fLocat>para cada fichero XML, de acuerdo con el Schema XML del estándar METS que representa cada documento que se transfiere, con el número del mismo calculado con base al algoritmo criptográfico SHA 256 incluido como un atributo, firmado digitalmente, con firma XAdesenvelopping última versión.

Formatos de ficheroadmitidos	En este apartado se definirán los formatos de fichero que se utilizarán en el elemento <filesec> del SIP, estableciendo los formatos aceptados y válidos para la transferencia. De igual manera se define si es aceptable formatos en versiones anteriores, y si se realizara conversión a la versión actual para cumplir con las estrategias de preservación necesarias.
Esquema de Metadatos	En este apartado se identificará el esquema de metadatos mediante el cual serán codificados los metadatos descriptivos. ● **Metadatos descriptivos que debe contener el SIP para la transferencia** •Metadatos para la descripción de los documentos: se toma como referencia los elementos de descripción de la norma ISAD (G), codificados en EAD. • Metadatos de la información de estructura de almacenamiento: información referente a Fondo, Subfondo, Serie y Expediente que será transferida. • Metadatos para la descripción del registro de autoridades: se utilizará la norma, ISAAR-CPF, codificados en EAC. ● **Metadatos que incluirá el repositorio**: • Metadatos tecnológicos: datos relacionados a los formato y características de los ficheros ingresados, en la sección METS <amdSec>dentro de la unidad semántica correspondiente del esquema PREMIS. • Metadatos de las propiedades significativas: datos relacionados con la firma digital original del fichero, certificado digital utilizado, cadena de certificación, lista de revocación de certificados, información de sellado de tiempo e información de número característico del digesto de la firma en la sección METS <amdSec>dentro de la unidad semántica correspondiente del esquema PREMIS. • Metadatos de los eventos: datos relacionados con la validación de ausencia de virus, verificación de la autenticidad del envío, generación de metadatos administrativos y sellado del AIP, en la sección METS <amdSec>dentro de la unidad semántica correspondiente del esquema PREMIS. • Metadatos de agentes: datos relacionados con los participantes en el proceso de ingreso, en la sección METS <amdSec> dentro de la unidad semántica correspondiente del esquema PREMIS**.**

Mecanismos de control y validaciones	En este apartado se detallarán los controles y verificaciones que el repositorio deberá realizar sobre el SIP. Algunas verificaciones automáticas necesarias son: ✓ Que el origen de la transferencia es de confianza y autorizado. ✓ Que cada fichero esté libre de virus. ✓ Que los ficheros están en alguno de los formatos admitidos indicados en el protocolo. ✓ Que el METS de cada fichero contiene los metadatos obligatorios en el estándar descriptivo indicado.
Derechos para realizar acciones de preservación sobre los documentos	En este apartado se definirán los derechos para realizar acciones de preservación sobre los documentos durante y después del ingreso al repositorio, así como los derechos de uso y distribución según las necesidades de la comunidad designada, así como los niveles de acceso según: serie documental, expediente o unidad y piezas documentales.
Plazo de conservación	El plazo de conservación dependerá de lo establecido en las tablas de plazo de conservación de documentos de la institución.
Propiedades significativas a conservar en el repositorio	En este apartado se identificará la información de propiedades significativas que el repositorio deberá preservar: ● **Propiedades significativas de apariencia**:se indicará la información relacionada con la apariencia externa que debe ser objeto de conservación, por ejemplo, la resolución, la tipografía, distribución de los elementos. ● **Propiedades significativas de funcionalidades:** se indicará la información relacionada con las funcionalidades que deben ser conservadas. ● **Propiedades significativas de autenticidad/ significación/valor**: se indicará la información relacionada con la autenticidad y valor probatorio que es objeto de conservación, por ejemplo, verificación de firma digital, verificar la autenticidad de la procedencia, el certificado digital utilizado, información de sellado de tiempo e información de número característico del digesto de la firma.
Derechos de uso y acceso	Los derechos para realizar acciones de preservación sobre los documentos durante y después del ingreso al repositorio, dependerá de los roles y niveles de acceso establecidos en el protocolo de acceso
Fecha de vigencia del Protocolo	El protocolo de transferencia debe actualizarse en un periodo de 5 años o cada vez que se produzca un cambio importante en la estructura, acceso o normativa relacionadas con el repositorio.

Fuente: Serra-Serra. J. (2013). Protocolo de ingreso y custodia. Proyecto de preservación digital para la Universidad de Costa Rica.

Anexo Nº 4: Cuestionario aplicado

Análisis sobre archivos del SNA con repositorios

El fin del presente cuestionario es realizar un diagnóstico e identificar la situación actual en materia de preservación digital en Costa Rica, específicamente con los repositorios existentes en el Sistema Nacional de Archivos. La información brindada a continuación servirá como insumo para el desarrollo de nuestro Trabajo Final de Graduación denominado: "Marco de Evaluación para soluciones de preservación de documentos digitales en Costa Rica", por lo que agradecemos su colaboración al completar este cuestionario. Además, la información suministrada será con fines académicos y se tratará de forma confidencial.

1. **Gestión de documentos**

1.1. ¿Se producen documentos en soporte digital en la institución?

Sí ( ) / No ( )

1.2. ¿Se reciben documentos en soporte digital en la institución? Sí ( ) / No ( )

1.3. ¿Qué porcentaje o volumen de los documentos se están produciendo únicamente en soporte digital?

_____

1.4 ¿La institución tiene identificado el volumen anual de producción de documentos digitales?

Sí ( ) / No ( )

1.5. ¿Los documentos en soporte digital cuentan con firma digital cumplen con las especificaciones técnicas definidas en la Política de Formatos Oficiales de los Documentos Electrónicos Firmados Digitalmente?

Sí ( ) / No ( )

1.6. ¿Existe en la institución una Política de Gestión de Documentos?

Sí ( ) / No ( )

1.7. Utilizando la definición de Sistema de Gestión de Documentos Electrónicos que se encuentra en el Anexo 1 Glosario ¿Cuenta la institución con un Sistema de Gestión de Documentos Electrónicos? Si su respuesta es NO, favor continuar con la pregunta 2.1.

Sí ( ) / No ( )

1.8 Marque la(s) funciones que tiene el SGDEA:

[ ] Firma Digital acorde con las especificaciones de la Política de Formatos Oficiales de los Documentos Electrónicos Firmados Digitalmente. Enlace: https://www.mifirmadigital.go.cr/wp-content/uploads/2016/03/DCFD-Poli%CC%81tica-de-Formato-Oficial-v1.0.pdf

[ ] Administración de identificadores únicos para la producción documental al menos por cada tipo documental.

[ ] Gestión de la clasificación documental acorde con el cuadro de clasificación institucional.

[ ] Control de tipos y series documentales.

[ ] Uso de Plantillas normalizadas para la producción de documentos.

[ ] Esquema de metadatos normalizados en cumplimiento con la Norma Nacional de Descripción. Enlace: https://www.archivonacional.go.cr/web/dsae/norma_nacional_descripcion_archivistica.pdf

[ ] Conformación de expedientes digitales acorde con la Norma Técnica Nacional de Expedientes Administrativos. Enlace: https://www.archivonacional.go.cr/web/normativa/norma_expedientes_administrativos.pdf

[ ] Gestión del proceso de Eliminación de Documentos (aplicando tablas de plazos) acorde con lo estipulado en la Ley 7202

1.9 ¿Cuáles son los formatos de ficheros que utilizan para la producción de los documentos en soporte digital?

[ ] PDF

[ ] PDF/A

[ ] OOXML o Compatible (Documentos de Microsoft Word, Libreoffice o algún otro procesador de texto)

[ ] Otro (s), indique cuál
(es):_____

1.10. ¿Se incluye información de autenticidad y descripción como parte de los datos estructurados (metadatos del fichero) en los documentos producidos por el sistema?

Sí ( ) / No ( )

1.11. Si la respuesta anterior fue sí, mencione cuáles son los datos estructurados usados.

_____
_____
_____

_____
_____

2. **Almacenamiento**

2.1 ¿La institución cuenta con repositorios para almacenar los documentos digitalizados o producidos digitalmente que esté en complimiento con lo estipulado en el Código Nacional de Tecnologías Digitales?

Enlace: https://www.micit.go.cr/sites/default/files/cntd_v2020-1.0_-_firmado_digitalmente.pdf

Sí ( ) / No ( )

2.2 En caso de contar con repositorios digitales, ¿Qué tipos de solución de almacenamiento utilizan para la persistencia de los activos de información?

( ) Centros de Datos Locales o Institucionales.

( ) Centros de Datos administrados por terceros (en la Nube).

( ) Una combinación de ambas tecnologías.

2.3 ¿El repositorio cuenta con las medidas de control de acceso, seguridad, interoperabilidad y conservación establecidas en el Código Nacional de Tecnologías Digitales?

Sí ( ) / No ( )

*** Si su respuesta es NO, favor continuar con la pregunta 2.5.**

2.4 Mencione los elementos de cumplimiento de dicho Código:

_____
_____
_____
_____
_____

2.5 ¿Controla la institución el proceso de obsolescencia en su infraestructura tecnológica?

Sí ( ) / No ( )

3. Preservación Digital

3.1. ¿Monitorea la institución los problemas de obsolescencia de los formatos de fichero?

Sí ( ) / No ( )

3.2. ¿Cuenta la institución con alguna estrategia de preservación digital?

Sí ( ) / No ( )

3.3 Si su pregunta anterior fue sí, mencione el nombre de la estrategia de preservación
digital:_____
____

3.4. ¿La institución ha llevado a cabo procesos de conversión de formatos como estrategia de preservación digital?

Sí ( ) / No ( )

3.5. ¿La elección de formatos de ficheros fue basada en información objetiva de alguna fuente como PRONOM y se encuentra estandarizada en la institución?

Sí ( ) / No ( )

3.6 Si su pregunta anterior fue sí, mencione el nombre(s) de la(s) fuente(s) que tomaron en cuenta para la elección de formatos de ficheros:

_____

3.7. ¿Cuáles de los siguientes criterios fueron empleados para la estandarización de formatos de ficheros de documentos en la institución?

[ ] Asegurar el valor probatorio del documento y su fiabilidad como evidencia.

[ ] De acuerdo con la naturaleza de la información a tratar, primando la finalidad para la cual fue definido cada formato.

[ ] Otro.

Indique_____.

3.8 ¿Existe en la institución una política de preservación digital?

Sí ( ) / No ( )

3.9 ¿Existe en la institución un repositorio de preservación digital en concordancia con los lineamientos del Código Nacional de Tecnologías Digitales?

Sí ( ) / No ( )

* **Si su respuesta es NO, favor continuar con la siguiente sección**

3.10 La solución de preservación digital es:

[ ] Desarrollo interno

[ ] Servicio de terceros

3.11 El repositorio digital de preservación está preparado para la preservación de los documentos a través del tiempo?

Sí ( ) / No ( )

3.12 El repositorio digital de preservación implementa el modelo de Sistema de Información de Archivo Abierto (OAIS)?

Sí ( ) / No ( )

3.13 Qué normas de buenas prácticas archivísticas se implementan en el repositorio de preservación digital que permitan garantizar el valor legal de los documentos en custodia, la accesibilidad y legibilidad._____
_____
_____
_____

3.14 ¿El repositorio de preservación digital integra la información producida en toda la institución independientemente de su sistema de origen?

Sí ( ) / No ( )

4. Seguridad de la información

4.1 ¿Cuenta la institución con un plan de protección de datos acorde a los estipulado en el Código Nacional de Tecnologías Digitales?

Sí ( ) / No ( )

4.2 ¿Cuenta la institución con una copia de los activos de información en una localización geográfica alterna a la institución?

Sí ( ) / No ( )

4.3 ¿Cuenta el sistema o repositorio documental con perfiles y roles específicos?

Sí ( ) / No ( )

4.4 ¿Se mantienen los registros de la trazabilidad de todas las acciones realizadas sobre los ficheros, incluye acciones de eliminación y transformación?

Sí ( ) / No ( )

4.5 ¿Se realizan auditorías de los registros?

Sí ( ) / No ( )

5. Continuidad digital

5.1 ¿Existe un Plan de Acción de Continuidad Digital?

Sí ( ) / No ( )

*** Si su respuesta es NO, favor continuar con la siguiente sección**

5.2 ¿Están definidos los requisitos del Plan de Continuidad Digital?

Sí ( ) / No ( )

5.3 ¿Se Identifica dónde están los riesgos en su información y toma medidas activas para administrar estos riesgos?

Sí ( ) / No ( )

5.4 ¿Se incorpora la continuidad digital en los procesos y estrategias de la organización de una manera que mantiene el acceso de la información?

Sí ( ) / No ( )

5.5 La organización cuenta con un protocolo para el ingreso o transferencia de objetos digitales, que permita garantizar que la información recibida o transferida pueda ser utilizada a través del tiempo.

Sí ( ) / No ( )

6. Gestión del riesgo

6.1 ¿Se estableció un marco de referencia para gestionar los riesgos producidos por la continuidad digital?

Sí ( ) / No ( )

6.2 ¿Los informes de evaluación de riesgos de continuidad digital están disponibles para la toma de decisiones dentro de la organización?

Sí ( ) / No ( )

6.3 ¿Se establecieron los roles y responsabilidades para gestionar los riesgos para la continuidad digital?

Sí ( ) / No ( )

6.4 ¿Se definieron los objetivos y criterios de éxito para la evaluación del riesgo en la continuidad digital?

Sí ( ) / No ( )

6.5 ¿Se estableció un proceso de cómo se identificarán, analizarán, controlarán, registrarán, monitorearán y revisarán los riesgos?

Sí ( ) / No ( )

Glosario adjunto en el cuestionario

- **Continuidad digital:** es la capacidad de utilizar la información en la forma en que se necesite por el tiempo que sea necesario. Las estrategias de continuidad deben contemplar un plan de prevención de riesgos, de gestión de emergencias, de recuperación, de formación, actualización y auditorías. La continuidad de los servicios debe realizarse con medidas preventivas que eviten la interrupción de los servicios. Las actividades de prevención y recuperación deben ofrecer garantías necesarias, se debe medir la continuidad del negocio y la madurez digital. (Umaña-Alpízar, 2017)

- **Conversión de formatos:** proceso de transformación de los documentos de un formato a otro, manteniendo las características del documento. (UNE-ISO 13008: 2013, p. 7).

- **Gestión de documentos:** Control eficaz y sistemático de la creación, recepción, mantenimiento, uso y disposición de documentos de archivo, incluidos los procesos para incorporar y mantener en forma de documentos la información y prueba de las actividades y operaciones de la organización. (FIED, 2012, p. 36).

- **Modelo de continuidad:** control eficaz y sistemático de la creación, recepción, mantenimiento, uso y disposición de documentos de archivo, incluidos los procesos para incorporar y mantener en forma de documentos la información y prueba de las actividades y operaciones de la organización. (FIED, 2012, p.38)

- **Preservación 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 (Voutssas y Bernard, 2014, p. 174).

- **PRONOM**: Es un sistema de información en línea sobre formatos de archivos de datos y sus productos de software de soporte. Originalmente desarrollado para respaldar el acceso y la preservación a largo plazo de los registros electrónicos. (TheNational Archives, 2020)

- **Repositorio digital:** es un sistema de información que almacena objetos digitales de forma segura, garantizando su valor legal y garantizando también que en el futuro los contenidos de los objetos digitales sean accesibles, representables y legibles. (Alberch-Fugueras, 2017).

- **Sistema Abierto de Información de Archivo (OAIS) [open archivalinformationsystem (OAIS)]:** Archivo, que una organización opera, que puede formar parte de una organización más amplia, de personas y sistemas, que acepta la responsabilidad de conservar información y mantenerla disponible para una Comunidad Específica. Cumple un conjunto de responsabilidades, definidas en el capítulo 4, que permite a un Archivo OAIS distinguirse de otros usos del término “Archivo”. El término “Abierto”

en OAIS se usa para dar a entender que esta Recomendación y futuras recomendaciones y normas relacionadas se desarrollan en foros abiertos, hecho que no significa que el acceso al Archivo no sea restringido. (UNE:ISO 14721, 2015, p.27).

- **Sistema de Gestión de Documentos Electrónicos (SGDE):** un sistema informático cuya principal función es la de gestionar la creación, uso, mantenimiento y disposición de los documentos creados electrónicamente a efectos de proporcionar evidencia de las actividades de la institución. (Norma Técnica para la Gestión de Documentos Electrónicos, emitida el 05 de mayo del 2018 por la Junta Administrativa del Archivo Nacional).

- **Sistema de preservación de Archivística Digital:** conjunto de reglas establecidas para el mantenimiento (o conservación) físico e intelectual permanente de los documentos de archivo que han sido transferidos (para su preservación en el largo plazo) así como las herramientas y mecanismos utilizados para implementar estas reglas. (GlosarioInterPARES, 2010).