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

PROYECTO DE GRADUACIÓN PARA OPTAR POR EL GRADO DE LICENCIATURA EN ARCHIVÍSTICA

MODELO DE PRESERVACIÓN DIGITAL SISTÉMICA PARA EL DESARROLLO DE UN ARCHIVO DIGITAL EN LA UNIVERSIDAD DE COSTA RICA

ESTUDIANTES:
JÉSSICA MARÍA BARAHONA CHAVARRÍA, B30812
JORGE LUIS MORA CERDAS, A74254

CIUDAD UNIVERSITARIA RODRIGO FACIO

I 2023

Trabajo Final de Graduación aprobado con distinción, para optar por el grado de Licenciatura en Archivística, presentado el martes 08 de agosto de 2023, en la Facultad de Ciencias Sociales de la Universidad de Costa Rica:

Tribunal Examinador:

M.Sc. Claudio Vargas Arias
Director de la Escuela de Historia
Presidente del Tribunal Examinador

M.Sc. Raquel Umana Alpízar
Directora del Proyecto de Graduación

M.Ls. María Teresa Bermúdez Muñoz
Profesora Invitada

M.Sc. María Gabriela Castillo Solano
Miembro del Comité Asesor: Lectora

M.Sc. Sergio Blanco Zeledón
Miembro del Comité Asesor: Lector

Sustentantes:

Jéssica María Barahona Chavarría
Licenciada

Jorge Luis Mora Cerdas
Licenciado

Dedicatoria

A **Dios**, por el don de la vida, la inteligencia y el amor.

A **Jorge**, el mejor compañero, esposo y colega.
Todos los días doy gracias por tenerte en mi vida, por ser mi apoyo e impulso.
Gracias por ser incondicional, por motivarme, por sacar lo mejor de mí.
Este es el inicio de un gran camino que quiero recorrer junto a ti.

A mi padre **Roger Barahona** hasta el cielo, y a mi madre **Grace Chavarría**,
porque ambos lo han dado todo por mis hermanos, hermanas y por mí,
son mis pilares y mi ejemplo.

A mis hermanos y hermanas, que siempre creyeron en mí.

Jéssica María Barahona Chavarría.

Dios, quién nos lleva de la mano todos los días. Gracias por tu amor.

A **Jéssica**, mi amada esposa, quién alegra mi alma todos los días.
Eres mi equipo ideal en la vida y la mejor compañera en la academia.
Te admiro por tu dulce corazón y tu gran inteligencia.
Gracias por impulsarme a soñar y a cumplir esos sueños.

A mi madre, **Olga Cerdas**, por darme su amor y apoyarme sin condiciones.
Te agradezco, porque me enseñaste a no desfallecer cuando las situaciones son difíciles
y a luchar por ser feliz ante cualquier circunstancia.

Jorge Luis Mora Cerdas.

Agradecimientos

A **Dios**, por darnos las fuerzas y el entendimiento para llevar a buen término este proyecto.

A la **Universidad de Costa Rica**, *Alma Máter*, quien nos abrió sus puertas; ha sido nuestra casa por años y lo seguirá siendo. Nos dio techo, alimento y educación, gracias a una beca en los años de desarrollo como estudiantes. Nos formó en conocimiento, pensamiento y crítica, encaminándonos al vasto mundo del saber, del cual ya no queremos salir.

A los profesores del Comité Asesor, **M.Sc. Raquel Umana Alpízar**, directora del Proyecto de Graduación, **M.Sc. María Gabriela Castillo Solano** y **M.Sc. Sergio Blanco Zeledón**, lectores del proyecto, quienes nos dieron su apoyo constante y compartieron sin limitaciones su conocimiento con nosotros para lograr este resultado.

Al profesor **Dr. Daniel Flores**, de la *Universidade Federal Fluminense* de Brasil, pionero en temas de preservación digital en Latinoamérica, por su disposición para atender nuestras consultas.

Al **AUROL,** al **Comité Técnico de SAU** y la **CIADi**, por la confianza en nuestra capacidad para elaborar un insumo de investigación tan importante, para el desarrollo del Archivo Digital de la Universidad de Costa Rica.

Resumen Ejecutivo

La Universidad de Costa Rica es una de las instituciones de educación superior más importantes del país y de la región, cuya estructura organizativa es de alta complejidad y, por consiguiente, la gestión documental también lo es. Dentro de la Universidad, la mayor parte de la información institucional es creada por medios digitales, lo cual implica riesgos tecnológicos, el más claro de ellos: la obsolescencia tecnológica.

El uso de las Tecnologías de la Información y Comunicación representa desafíos para la preservación digital de la información, por lo cual la Universidad requiere implementar acciones que le permitan preservar adecuadamente la información digital, esto con el fin de apoyar y mejorar la gestión administrativa, asegurar la transparencia y la rendición de cuentas, al tiempo que se promueve la investigación y la cultura.

El presente trabajo de investigación propone un modelo de preservación digital sistémica para el desarrollo de un Archivo Digital, que permita la conservación a mediano y largo plazo de la información producida y recibida por la Universidad de Costa Rica.

Para el establecimiento de este modelo, se llevó a cabo una evaluación del estado actual de la preservación digital de la información generada y recibida por la Universidad de Costa Rica, mediante un diagnóstico de la situación archivística, normativa y tecnológica de la institución. Así también, se definieron las estrategias de preservación digital, y los requisitos del modelo funcional y modelo tecnológico para el desarrollo del Archivo Digital.

El Archivo Digital de la Universidad de Costa Rica, o ADiUCR, es el ente encargado de aplicar las políticas de preservación digital y es donde se transfiere la información institucional. No se puede comprender el Archivo Digital únicamente como una herramienta informática, sino que es la unión de la normativa, las personas y las herramientas tecnológicas que permiten llevar a cabo la preservación digital.

La Preservación Digital Sistémica (PSD), por su parte, se refiere a las acciones y estrategias implementadas para asegurar la conservación de la información y su acceso y uso a través del tiempo, y se encuentra basada en Normas, Modelos y estrategias probados ampliamente. La PSD, debe estar regulada por una Política de Preservación Digital.

Por medio de la Preservación Digital Sistémica, se busca asegurar la Cadena de Custodia Digital Archivística, proceso que implica un monitoreo ininterrumpido en la gestión de la información, para asegurar que la información no ha sido alterada, desde su creación hasta que llega al Archivo Digital, donde será conservada o eliminada según corresponda; garantizando así, la autenticidad, fiabilidad, integridad y usabilidad a lo largo del tiempo.

Tomando en cuenta estos aspectos, la propuesta del modelo de preservación digital sistémica, presenta dos aristas principales. La primera, es la necesidad imperativa de la creación de una política institucional y la normativa conexa requerida: de manera que se abarquen aspectos como la inclusión de los términos de Preservación Digital Sistémica y Cadena de Custodia Digital Archivística; y que, además, abarque la preservación digital a largo plazo de toda la información institucional, incluyendo la que tiene solo valor administrativo y también la de valor secundario: científico-cultural.

La segunda, es el Modelo de Requisitos para el Archivo Digital, que abarca el *Marco Estratégico* de Preservación Digital en el cual se define el funcionamiento administrativo del Archivo Digital; el *Modelo Funcional*, el cual identifica los requisitos clave que caracterizan los elementos que se deben incluir en el repositorio digital; y el *Modelo Tecnológico*, que permite determinar cuáles son las especificaciones de la plataforma y las herramientas tecnológicas requeridas para el desarrollo e implementación del Archivo Digital.

Finalmente, se trabajaron dos casos de estudio particulares para transferir la información al ADiUCR. El primero es el del Sistema de Gestión de Documentos Institucional (SiGeDI), para abordar el caso de un sistema de información; y el segundo, el de la colección fotográfica de la Unidad de Programas Deportivos Recreativos y Artísticos (UPDRA), para la transferencia de un grupo de documentos digitalizados o escaneados, que se encuentran fuera de un sistema informático.

Tabla de contenido

Índice de figuras

Índice de Tablas

Introducción

El rápido avance en el desarrollo de las Tecnologías de la Información y la Comunicación y su uso extendido a nivel mundial presenta nuevos retos para la ciencia Archivística, la cual debe especializarse cada vez más en el tema de la preservación digital de la información, para poder abordar los problemas inherentes que se presentan, como la obsolescencia tecnológica.

De esta forma, es necesario que la Universidad de Costa Rica pueda asegurar la integridad, fiabilidad, autenticidad y disponibilidad de la información que produce y recibe al ejecutar sus funciones. Para lograrlo, debe implementar soluciones integrales, que se aborden desde la perspectiva archivística, jurídica y tecnológica, mejorando la toma de decisiones estratégicas y el uso adecuado de los recursos públicos, para garantizar la transparencia institucional, la rendición de cuentas y el cumplimiento de los derechos de las personas.

Esta investigación se estructura en dos partes: en primer lugar, se realizó un diagnóstico del estado de la preservación digital en la Universidad de Costa Rica, partiendo del año 2013, cuando se presentó la primera propuesta de un Archivo Digital, hasta el año 2022. En segundo lugar, se propuso un modelo de preservación digital sistémica, compuesto por un modelo funcional y un modelo tecnológico que sirvan como base para el desarrollo e implementación de un Archivo Digital, en el cual se pueda resguardar a largo plazo la información producida y recibida.

Finalmente, se abordaron los dos casos específicos del Sistema de Gestión de Documentos Institucional (SiGeDI) y la Colección Fotográfica de la Unidad de Programas Deportivos, Recreativos y Artísticos (UPDRA), por medio de los cuales se busca obtener resultados y soluciones escalables a la totalidad de la institución.

1. Objeto de la investigación

1.1. Tema

1.1.1 Título

Modelo de preservación digital sistémica para el desarrollo de un Archivo Digital en la Universidad de Costa Rica.

1.1.2. Justificación

La Universidad de Costa Rica (UCR), se constituye como una de las instituciones de educación superior más importantes del país y de la región. Está conformada por unidades académicas, administrativas y de investigación, por medio de las cuales logra desarrollar sus tres ejes fundamentales: la docencia, la investigación y la acción social.

La estructura organizativa de la UCR (refiriéndose a la cantidad de unidades académicas, administrativas y de investigación) es de alta complejidad, y por consiguiente, la gestión documental también lo es.

Para abordar este aspecto, la Institución dispone del Sistema de Archivos Universitarios (SAU), conformado por el Archivo Universitario Rafael Obregón Loría (AUROL), el Comité Técnico del SAU y la Comisión Universitaria de Selección y Eliminación de Documentos (CUSED), ya que los documentos de archivo, deben ser gestionados adecuadamente para ser preservados a mediano y largo plazo, conservando sus características de autenticidad, integridad, fiabilidad y disponibilidad, sirviendo como pruebas legales y administrativas de la ejecución de sus funciones y preservando la memoria institucional y nacional.

Sin embargo, aún no se dispone de un Archivo Digital que asegure la preservación y uso de los documentos en soporte electrónico, que se generan a raíz de las actividades sustantivas y facilitativas de la UCR.

También, debido al desarrollo acelerado y uso constante de las Tecnologías de la Información y la Comunicación (TIC), existe un creciente número de esos documentos que nacen en soporte electrónico. También existen múltiples procesos de digitalización, que transforman información fijada en soportes analógicos (papel, cintas de carrete abierto, discos de acetato, fotografías, etc.)

hacia medios digitales. En ambos casos, se genera un amplio volumen documental que debe ser gestionado mediante procesos de preservación digital, asegurando su almacenamiento y uso a través del tiempo.

Esta situación plantea tres niveles de desafíos en la gestión de los documentos. En primer lugar, implica que se generen distintas clases documentales de acuerdo con las necesidades de información que se deben suplir. Por ejemplo, se pueden encontrar las clases: textuales, audio, video, imagen fija, imagen dinámica, entre otros.

En segundo lugar, para cada clase documental, existe una gran variedad de formatos de archivos en los que pueden ser generados los distintos objetos digitales, lo cual complejiza el tema de la preservación digital. De esta forma, por ejemplo, para la clase textual se pueden encontrar ficheros en formato .txt, . docx, .pdf, entre otros. Para imágenes existen varios formatos como .jpg, .png o .tif.

Y en tercer lugar, en la Universidad de Costa Rica existen sistemas informáticos especializados, con la capacidad de generar y procesar una variada gama de clases documentales representadas mediante distintos formatos.

La implementación de estos sistemas de manera individualizada por parte de las distintas instancias universitarias, sin considerar aspectos como la interoperabilidad, ha provocado que se generen "islas" de información, donde no existe una interconexión, lo cual dificulta la gestión de la información archivística y la preservación a largo plazo de la información que en ellos se produce.

Por consiguiente, para abordar estos desafíos, es necesario establecer mecanismos normativos, archivísticos y tecnológicos, que en conjunto permitan llevar a cabo una gestión de documentos que asegure que los documentos sean auténticos, íntegros, disponibles y usables, durante todo el tiempo en que se requiera su preservación.

Se considera que el establecimiento de un Archivo Digital en la Universidad de Costa Rica vendría a

> (...) garantizar las mejores posibilidades de conservar el acceso a la información de un documento electrónico, dando fe de su integridad y autenticidad y de su información

> contextual o metadatos, gestionando el riesgo de la obsolescencia tecnológica que es inherente al continuo proceso de la evolución de la industria informática y la tecnología. (Castillo-Solano y Umaña-Alpízar, 2019, p.73)

Para establecer un Archivo Digital, se requiere de un trabajo previo institucional, mediante un compromiso oficial por parte de la administración: desde las altas jerarquías, hasta el personal operativo al que se le asigne la responsabilidad de mantenimiento y funcionamiento de dicho archivo.

Es importante destacar que, dentro de las razones para preservar por medio de un Archivo Digital la información que se produce, es que los archivos son responsables de proteger la memoria, promover la investigación y la cultura, y también "deben ser soporte de transparencia administrativa y de una gestión pública democrática, capaz de garantizar los derechos" (Rivas-Fernández, 2012, p.53).

Por lo tanto, la propuesta que se realiza a partir de esta investigación representa una alternativa enfocada en la preservación digital de información en la Universidad de Costa Rica, pero también tendrá la capacidad de generar bases que sean replicables en otras instituciones públicas y privadas a nivel nacional.

1.1.3. Delimitación

Temporal

Esta investigación se delimita entre el año 2013, momento en el que se plantea la primera propuesta para el desarrollo de un Archivo Digital en la Universidad de Costa Rica y el año 2023, con la presente propuesta de modelo para la preservación digital sistémica en la institución.

Espacial

Se delimita espacialmente a la Universidad de Costa Rica, ya que se realiza el análisis específico y propuesta metodológica para esta institución, basado en su situación en cuanto a la preservación digital.

1.2. Problema

En Costa Rica, las instituciones públicas avanzan con gran rapidez en la implementación de las TIC, con el fin de ofrecer servicios y productos de manera cada vez más ágil. Actualmente, existe una mayor exigencia por parte de los ciudadanos para satisfacer sus necesidades de información, por lo cual se comprende que las universidades públicas del país no pueden quedarse rezagadas en cuanto la utilización de tecnologías de la información y la alfabetización informacional.

El cambio acelerado en el desarrollo de las herramientas informáticas presenta una problemática inherente de obsolescencia tecnológica, que puede conllevar a la pérdida de información por la imposibilidad de recuperarla y utilizarla, razón por la cual, toda "organización productora de documentos digitales debe diseñar una estrategia para asegurar su conservación y disponibilidad, en función de afrontar los riesgos de la obsolescencia tecnológica" (Giménez-Chornet, 2014, p.148).

Desde esta perspectiva, se debe tomar en cuenta que gran parte de los documentos producto de las funciones y decisiones que se realizan en las instituciones, son producidos o transformados a medios electrónicos, de manera que deben ser controlados y conservados por el tiempo que sean requeridos.

Esta tarea, debe ser asumida por los archivos, ya que "la preservación es la razón de ser de los mismos, aunque sin perder de vista que el objetivo no es simplemente conservar sino estar preparados para dar acceso a los contenidos en el momento que sea preciso" (Térmens-Graell, 2009, p.117).

Para esto, los archivos deben estar preparados con apoyo de la administración, infraestructura tecnológica y procedimientos archivísticos capaces de proteger y asegurar la autenticidad, fiabilidad, integridad y disponibilidad de la información, características que en los documentos electrónicos "viene asegurado por técnicas como la firma electrónica y el sellado de tiempo, entre otras, unas medidas de seguridad informática que se aplican como instrumento para fijar el valor jurídico de los documentos" (Térmens-Graell, 2009, p.118).

En el caso específico de la UCR, la explosión documental que se da a partir del uso extendido de las TIC, ha provocado el problema principal que se intentará tratar mediante esta investigación:

la imposibilidad de asegurar la preservación a mediano y largo plazo de la información electrónica generada y recibida a partir de la ejecución de sus funciones sustantivas y facilitativas.

Esa imposibilidad de preservar la información digital tiene como punto de partida la ausencia de un Archivo Digital, necesario para que se promueva una cultura institucional de transparencia, rendición de cuentas y aseguramiento de los derechos de las personas.

Esta problemática tiene sus raíces en tres tipos de causas principales que intervienen a la hora de gestionar correctamente la información electrónica: legales, archivísticas y tecnológicas.

En primera instancia, desde el punto de vista legal, la UCR no cuenta con normativa específica en cuanto a preservación digital, para asignar responsabilidades, funciones, recursos, especificaciones técnicas, entre otros, que permitan asegurar la validez jurídica de la información.

Considerando que la información de archivo es la base para conformar las pruebas legales y administrativas en cuanto al cumplimiento de las funciones institucionales y para probar los derechos de las personas (tanto de la comunidad universitaria, como de personas externas que se relacionan con la UCR), la ausencia de normativa, pueden derivar consecuencias de tipo legal.

La pérdida de información, o bien, la dificultad para localizarla o comprobar su autenticidad e integridad, puede llegar a afectar a la Universidad en pérdidas económicas y sanciones legales para la institución.

En segundo lugar, en cuanto a las causas archivísticas, se debe mencionar que existe una ausencia de controles eficientes para la creación, uso y disposición de la información en soporte electrónico. Las series documentales que se producen y gestionan en la UCR no cuentan con la aplicación de procesos técnicos archivísticos de manera completa, puesto que instrumentos como el cuadro de clasificación documental y las tablas de plazos de conservación, no se encuentran desarrollados para todas las unidades administrativas, académicas y de investigación.

La inexistencia de un Archivo Digital que asegure la preservación de la información, así como la cadena de custodia ininterrumpida, tiene como consecuencia que se vea limitada la capacidad de asegurar las 4 características de los documentos electrónicos (autenticidad, integridad, fiabilidad

y usabilidad). También se seguirá generando información desorganizada y sin base en estándares internacionales, que faciliten el intercambio de conocimiento.

Otra consecuencia en el contexto archivístico, es la pérdida de credibilidad en las acciones de los archivistas, por lo cual los proyectos de preservación digital han sido históricamente delegados al liderazgo de profesionales de otras áreas, por ejemplo: TI, administradores, bibliotecólogos, entre otros. Esto también puede desencadenar en que no se asignen recursos institucionales para la capacitación continua de los archivistas en el campo de la preservación digital. Como indica Térmens-Graells (2009, p.120):

> Si las oportunidades son grandes, los peligros también: más de un responsable de archivos ha dicho que se encuentran ante la última oportunidad para que los archiveros y los archivos sean algo más que simples depósitos a ojos de sus respectivas instituciones; si no lo logran significará que buena parte de las funciones del archivo digital habrán sido directamente asumidas por las áreas de informática.

Además de esto, el desarrollo e implementación de las TIC en la UCR ha ido a un paso más acelerado que los procesos para llevar a cabo la gestión de los documentos electrónicos que se generan y se reciben, porque se ha dado prioridad al rescate y gestión de la información en soporte físico.

Esta última afirmación, muestra estrecha relación con el tercer tipo de causas, las tecnológicas: existe una falta de planificación de los recursos tecnológicos enfocados hacia la preservación digital, pues, por ejemplo, no se ha asignado formalmente personal, ni existe una plataforma tecnológica adecuada para este fin.

Así, cuando se habla del tema tecnológico, se puede volver al concepto de "islas de información", ya que debido a la diversidad de productos y servicios que ofrece la UCR, distintas unidades han buscado la forma de satisfacer sus requerimientos de producción y manejo de la información, dando paso al uso de múltiples sistemas, con poca o nula interrelación entre sí.

Por su parte, esta cantidad de sistemas informáticos que funcionan dentro de la UCR para suplir las necesidades de las distintas unidades, producen múltiples formatos de fichero para almacenar

la información electrónica, lo cual dificulta garantizar la autenticidad, perdurabilidad y acceso a la información a largo plazo.

En la parte tecnológica, se pueden derivar consecuencias relacionadas con el uso de los recursos, en cuanto a la designación de espacio de almacenamiento no planificado. Este aspecto, unido a los retos que se generan para combatir la obsolescencia tecnológica tanto de los objetos digitales como de los *hardware* que se utilizan, implicaría mayores costos y más dificultad para implementar planes de preservación con acciones de migración de información a soportes o sistemas óptimos.

También existen consecuencias que traslapan a los ámbitos archivístico y tecnológico, relacionadas con la sobreproducción de objetos digitales, que no están almacenados en un ambiente controlado, como lo es un Archivo Digital. La falta de control al gestionar la información dificulta la aplicación de instrumentos archivísticos para su disposición, por lo cual se puede tender a realizar respaldos y copias innecesarias de los objetos digitales, manteniendo una falsa expectativa que así los documentos y datos se encuentran siempre resguardados y disponibles.

Sumado a ello, la ausencia de controles provoca que la información y los documentos producidos, se mantengan en el almacenamiento local de las computadoras que utilizan los funcionarios, o dentro de correos electrónicos, con el riesgo de que se puedan eliminar de forma indiscriminada.

El conjunto de consecuencias legales, archivísticas y tecnológicas, pueden implicar amplios inconvenientes a nivel estratégico en la UCR, como la dificultad para la toma de decisiones documentadas, inadecuado control de la información, pérdida de información institucional, inadecuado uso de los recursos públicos e ineficiencia en el desarrollo de las funciones y actividades.

Si bien, desde el enfoque archivístico de esta investigación, no es su finalidad el indicar cuántos ni cuáles sistemas informáticos puede o debe utilizar la institución, se resalta la necesidad de que exista comunicación e integración de dichos sistemas con los procedimientos y las aplicaciones informáticas que se utilizarán para la preservación a largo plazo de la información (Térmens-Graell, 2009).

A raíz de la problemática presentada, surgen las siguientes interrogantes:

¿De qué manera se organiza el ámbito archivístico en la Universidad de Costa Rica? ¿Qué instrumentos archivísticos se han desarrollado y con cual personal cuenta la institución para atender las necesidades de preservación a largo plazo de la información?

¿Con cuáles sistemas informáticos cuenta la Universidad de Costa Rica para producir, gestionar y preservar la información electrónica? ¿Qué características tienen a nivel tecnológico?

¿Cuál sería el efecto del desarrollo e implementación de un Archivo Digital en la preservación digital de los documentos e información producidos en la Universidad de Costa Rica que deben conservarse a largo plazo?

¿Cuáles han sido las acciones tomadas por la Universidad de Costa Rica, desde el primer planteamiento de un Archivo Digital en 2013, para asegurar a largo plazo las características de autenticidad, fiabilidad, integridad y usabilidad de los documentos que produce?

¿Cuáles son los requisitos necesarios para proponer un modelo funcional y un modelo tecnológico para desarrollar un Archivo Digital en la Universidad de Costa Rica?

1.3. Estado de la cuestión

El tema de la preservación digital, el cual está ligado con el establecimiento de un Archivo Digital, ha sido abordado desde la perspectiva de las distintas ciencias de la información, entre la que destaca la Archivística.

De esta manera, se presentan algunas iniciativas relevantes, a nivel internacional y nacional que se refieren al conocimiento teórico desarrollado en torno a la preservación digital y cómo este conocimiento se ha logrado llevar a casos aplicados.

1.3.1. Ámbito Internacional

A continuación, se presentan las propuestas desarrolladas a nivel internacional, con el objetivo de contextualizar el tema de la preservación digital. Se hará por medio del estudio de algunos de los casos de países que comparten entre sí características similares en cuanto a ubicación geográfica y/o idioma. También se toman en cuenta los países que tienen una mayor influencia en el aporte a la Archivística costarricense.

1.3.1.1. Europa

En Europa se han realizado múltiples iniciativas para la preservación de objetos digitales a mediano y largo plazo.

Así, el Gobierno de España ha desarrollado el proyecto PAE (Portal de Administración Electrónica) el cual tiene como objetivo gestionar la administración pública de forma electrónica, con base en normativa nacional, principalmente en las Leyes *39/2015 Procedimiento Administrativo Común de las Administraciones Públicas* y *40/2015 Régimen Jurídico del Sector Público*, normas técnicas y tecnologías de la información y la comunicación. Este proyecto tiene una gran importancia para el desarrollo de dos iniciativas mayores: el Plan de Recuperación, Transformación y Resiliencia de la Economía y la iniciativa España Digital 2025 (Portal Administración Electrónica, s.f.-b).

El PAE está compuesto de varios ejes que lo sustentan, entre los que se encuentran la Estrategia de Identidad y Firma Electrónica, Estrategia TIC, Estrategia de Gobierno Abierto, Estrategia de Seguridad, la Estrategia de Interoperabilidad y la Estrategia de Archivo Electrónico.

De esta forma, destaca la Estrategia de Archivo Electrónico, la cual "permite almacenar por medios electrónicos todos los documentos utilizados en las actuaciones administrativas. Estos archivos electrónicos, destinados a cubrir el conjunto del ciclo de vida de los documentos electrónicos vienen a ser complementarios y equivalentes a los archivos convencionales" (Portal Administración Electrónica, s.f.-a párr.1).

Está sustentada por la Norma Técnica de Interoperabilidad de Política de Gestión de Documentos Electrónicos y en Modelos de Políticas de Gestión de Documentos Electrónicos, orientativos de política de gestión documental, el cuadro de clasificación funcional y el índice de series documentales que permiten llevar a cabo la gestión de los documentos electrónicos (Portal Administración Electrónica, s.f.-c.).

Otro proyecto destacado en España es el proyecto PARES (Portal de Archivos Españoles [PARES], s.f.), con énfasis en documentos digitalizados para promover la difusión del Patrimonio Histórico Documental Español, compuesto por cada uno de los Archivos Estatales y centros administrados por el Ministerio de Cultura y Deporte, dando acceso libre, gratuito e

ilimitado a los ciudadanos. Cada uno de los fondos administrados y los documentos que se han cargado dentro de repositorios han sido descritos mediante la norma archivística ISAD (G), con la posibilidad de exportar los datos al formato XML.

Otro importante caso es el del Reino Unido, al crear los Archivos Nacionales en 2003, a partir de la unión de 4 organizaciones gubernamentales: La Oficina de Registro Público, la Comisión Real de Manuscritos Históricos, La Oficina de Papelería de Su Majestad y la Oficina de Información del Sector Público (The National Archives. s.f.-c), lo que ha dado como resultado el mantener bajo custodia cerca de 1000 años de documentos nacionales icónicos, convirtiendo a los Archivos Nacionales en una institución cultural, académica y de herencia histórica (The National Archives. s.f.-d).

Por consiguiente, y debido a los rápidos avances tecnológicos, los Archivos Nacionales han desarrollado una estrategia digital que busca "*to understand the past and make sense of the present, while offering guidance for the future. Our ability to preserve and make available digital records will decide what evidence people in the future will have of today* (The National Archives. s.f.-b, párr.1)".

Dicha estrategia permite la instauración de un Archivo Digital Disruptivo, que entre otras características busca preservar todos los tipos de registros digitales creados por el gobierno y no solo de formatos de archivo comunes; desarrollar nuevas formas de proporcionar contexto, gestionar el riesgo y garantizar que los documentos de archivo no han sido modificados; el uso del internet para llegar a nuevas audiencias y permitir la disponibilidad de toda su colección; además, compartir herramientas, experiencia y trabajo con otros para desarrollar nuevas prácticas archivísticas y nuevos estándares (The National Archives, 2017a).

De esta forma, han desarrollado herramientas que permiten a las personas e instituciones ahondar en la investigación de la preservación digital. Una de estas herramientas es DROID (*Digital Record Object Identification*). Es un programa informático que perfila una gran variedad de formatos de ficheros, determinando características como la versión, antigüedad, cambios realizados y tamaño (The National Archives, 2017b). Otra ejemplo de herramienta es PRONOM; es un servicio en línea que brinda información sobre una gran variedad de formatos, estableciéndose como una fuente de información autorizada sobre productos de *software*, sus

ciclos de vida de soporte y requisitos técnicos, y sobre los formatos de archivo que admiten (The National Archives, s.f.-a).

Estas iniciativas de preservación digital están orientadas hacia las organizaciones públicas y privadas para que puedan iniciar con el aseguramiento a largo plazo de sus objetos digitales, promoviendo su participación en la preparación del material y la transferencia de los objetos digitales a los Archivos Nacionales.

1.3.1.2. Australia

Australia ha sido históricamente un referente en la gestión de documentos electrónicos. Es por ello que se ha desarrollado una Política de Preservación Digital aplicada en los Archivos Nacionales de Australia, con el objetivo de contrarrestar los riesgos que corre la información digital, como por ejemplo, la inaccesibilidad por obsolescencia de los *software* o *hardware*; pérdida por la alteración accidental o maliciosa de la información; captura incompleta o inadecuada de los datos, lo cual implica la generación de información no auténtica o no fiable (National Archives of Australia, s.f.).

Dicha política está dirigida a personal de archivos, agencias del gobierno de la *Commonwealth*, grupos de expertos en la comunidad de archivos digitales y clientes públicos. Además, se extiende a los documentos que han nacido digitalmente (*born-digital records*) y documentos que se crearon originalmente en soportes analógicos y que por razones de trámites, preservación o acceso han sido digitalizados (*digitised records*).

Esta estrategia de preservación digital se ha desarrollado por medio del uso de estándares para que haya interoperabilidad entre los sistemas actuales y los futuros, con la posibilidad de definir requisitos y medir los resultados. Entre estos estándares destacan la ISO 14721 Sistema abierto de información de archivo (OAIS), la ISO-IEC 26300: Formato de documento abierto para aplicaciones de oficina, la ISO-IEC 15948: Gráficos de red portátiles, entre otras; se usa el diccionario PREMIS para gestionar metadatos de preservación. Además, estándares internos para digitalización, conservación de formatos, transferencia y almacenamiento y recuperación (National Archives of Australia, s.f.).

Por último, es importante mencionar que la Política de Preservación está relacionada con otras políticas y estrategias importantes como el Plan Corporativo de los Archivos Nacionales de Australia 2017-18 a 2020-21, la Estrategia Nacional de Digitalización, la Política Nacional de Transferencia, entre otras.

1.3.1.3. Canadá y Estados Unidos

En el caso de Norteamérica, se pueden encontrar distintas iniciativas relacionadas con la creación y gestión de archivos digitales.

Por un lado, en Canadá nace el *The International Research on Permanent Authentic Records in Electronic Systems (InterPARES)*, proyecto que tiene su sede en la *School of Library, Archival and Information Studies* en *The University of British Columbia*, en la ciudad de Vancouver, Columbia Británica, y cuya directora desde sus inicios en 1999 es la Dra. Luciana Duranti (InterPARES Project, s.f.-b).

La Dra. Duranti, señala en la página web del proyecto que (InterPARES Project, s.f.-a, párr. 1):

> *Digital technology had profoundly challenged the traditional methods by which records were identified, recognized as accurate, reliable and authentic, appraised and preserved. The InterPARES Project chose to rely on an intellectual framework based on archival science and diplomatics, but committed to an inter-disciplinary process involving a wide spectrum of academic and professional fields, from geography and musicology to computer engineering and law. Its researchers included individuals, organizations and institutions from five continents, working in the public and private sectors.*

El proyecto de InterPARES se desarrolló inicialmente en tres fases:

***InterPARES 1 Project (1999-2001)*:** estuvo enfocado en preservar la autenticidad de los registros que han pasado su etapa administrativa y son seleccionados para su conservación permanente; dentro de sus principales hallazgos se encuentran los requisitos conceptuales de autenticidad y los métodos para la selección y preservación de registros electrónicos auténticos (InterPARES 1 Project, s.f.).

InterPARES 2 Project: *Experiential, Interactive, Dynamic Records. (2002-2007)*: dentro de sus objetivos principales estaban (InterPARES 2 Project, s.f.-b, párr.2):

> *to develop and articulate the concepts, principles, criteria and methods that can ensure the creation and maintenance of accurate and reliable records and the long-term preservation of authentic records in the context of artistic, scientific and government activities that are conducted using experiential, interactive and dynamic computer technology.*

Las partes interesadas incluyeron: creadores de registros individuales, organizaciones, Gobiernos, archivistas, investigadores de todas las disciplinas científicas, la ciudadanía en general y el sector de las tecnologías de la información (InterPARES 2 Project, s.f.-b).

Este proyecto se trató de una colaboración internacional y multidisciplinaria, por medio de la cual se buscó la aplicación de un enfoque de múltiples métodos que permitieran desarrollar conceptos, procesos y herramientas para ayudar a asegurar un entorno protegido y duradero para los registros digitales producidos en sistemas interactivos, dinámicos y experienciales (InterPARES 2 Project, s.f.-a).

InterPARES 3 Theoretical Elaborations into Archival Management (TEAM): Implementing the theory of preservation of authentic records in digital systems in small and medium-sized archival organizations. (2007-2012): esta tercera fase permitió traducir la teoría y los métodos de preservación digital desarrollados por InterPARES, así como de otros esfuerzos en planes de acción concretos para las masas de registros existentes que se mantendrán a largo plazo por archivos o unidades de archivo dentro de organizaciones con recursos limitados (InterPARES 3, s.f.).

Durante este proceso, se desarrolló conocimiento detallado acerca de:

- Cómo la teoría y los métodos generales pueden implementarse en archivos y unidades pequeñas y medianas y convertirse en prácticas efectivas.
- Qué factores determinan el tipo de implementación que es apropiada para cada cuerpo de registros en cada contexto.
- Qué habilidades necesitarán los profesionales para realizar tales operaciones.

Una vez concluyeron estas tres fases, inició una cuarta fase, relacionada con el tema de confianza y confiabilidad de registros y datos en entornos en línea (InterPARES Trust, 2018):

InterPARES Trust (ITrust; 2012-2019): el objetivo principal de este proyecto es el de "*to generate the theoretical and methodological frameworks to develop local, national and international policies, procedures, regulations, standards and legislation, in order to ensure public trust grounded on evidence of good governance, a strong digital economy, and a persistent digital memory*" (InterPARES Trust, 2018, párr.1).

Se considera que *ITrust* es una asociación de investigación, en la que trabajan más de cincuenta universidades y organizaciones, nacionales y multinacionales, públicas y privadas en distintos países de todo el mundo. Además, los investigadores de este proyecto son expertos en: archivística, gestión de registros, diplomática, derecho, tecnología de la información, comunicación y medios, periodismo, comercio electrónico, informática de la salud, ciberseguridad, gobernanza y garantía de la información, análisis forense digital, ingeniería informática y política de la información (InterPARES Trust, 2018).

Por otro lado, se tiene el caso de Estados Unidos, donde se pueden encontrar varias iniciativas enfocadas en la preservación digital. Algunos ejemplos de estas iniciativas son:

a. *National Archives and Records Administration* (NARA)

La Administración Nacional de Archivos y Registros NARA, es la entidad encargada de gestionar los documentos y materiales que se generan por el gobierno federal de los Estados Unidos (National Archives and Records Administration [NARA], s.f.-e).

Los Archivos Nacionales fueron establecidos en 1934, por el presidente Franklin Roosevelt, pero sus principales posesiones se remontan a 1775. En el NARA se conservan sólo los documentos que se consideran con valor secundario, lo que representa entre el 2% y el 5% de la producción documental. Esto significa que (NARA, s.f.-a, párr.6)

> *By now, they add up to a formidable number, diverse in form as well as in content. There are approximately 13.28 billion pages of textual records; 10 million maps, charts, and architectural and engineering drawings; 44.4 million still photographs, digital images, filmstrips, and graphics; 40 million aerial photographs; 563,000 reels of motion picture film; 992,000 video and sound recordings; and 1,323 terabytes of electronic data.*

Debido a la gran cantidad de documentos electrónicos que se generan por el gobierno, NARA desarrolló la estrategia de *Electronic Records Archives* (ERA), la cual está enfocada en enfrentar el reto de la preservación, administración y el acceso de los documentos electrónicos y se espera que ERA mantenga los registros federales electrónicos por el tiempo que sean requeridos (NARA, s.f.-a).

Sin embargo, se debe tener en cuenta que ya se está trabajando en el proyecto ERA 2.0. Si bien desde 2008 se ha estado utilizando ERA para recibir y almacenar todo tipo de registros electrónicos gubernamentales, ERA 2.0 representa una modernización del sistema ya existente (NARA, s.f.-b).

Dentro de las principales mejoras que se trabajan en ERA 2.0 se incluyen (NARA, s.f.-b, párr.3): "*provide end-to-end lifecycle coverage for electronic records, from scheduling, obtaining approvals for transfers, uploading into the system by a producing Federal agency, processing of uploaded records, preservation of the records, to, finally, production of access versions for the National Archives Catalog*", además se explica que ERA 2.0 consta de tres componentes principales: un entorno de procesamiento, el repositorio digital y formularios/flujos de trabajo para respaldar la programación de registros federales, así como la transferencia de registros federales permanentes a la custodia de NARA.

El proyecto ERA 2.0 ofrece un almacenamiento apropiado a largo plazo, esto en estrecha relación con la Estrategia de Preservación Digital (*Digital Preservation Strategy*) de NARA. La primera publicación de la Estrategia se realizó en 2017, para guiar sus operaciones internas (NARA, s.f.-c):

> *It outlines the specific strategies that NARA will use in its digital preservation efforts and specifically addresses Infrastructure, Format & Media Sustainability and Standards, Data Integrity, and Information Security. It applies to born-digital agency electronic records, digitized records from agencies, and NARA digitization for access and preservation reformatting.*

Dentro de un gran marco como lo es la *Digital Preservation Strategy*, se aplican distintas estrategias clave para lograr una preservación efectiva de los contenidos digitales, y que también

están pensadas para ser flexibles, es decir, que permita una adaptación a los cambios constantes (NARA, s.f.-d).

Dentro de dichas estrategias clave se encuentran (NARA, s.f.-d):

- Documentación de estándares y procedimientos: proporciona orientación sobre la creación de agencias de sustitutos digitales y proporciona orientación sobre metadatos mínimos y formatos de archivo preferidos para que los registros electrónicos se transfieran a NARA.
- Priorización: un enfoque basado en el riesgo para establecer prioridades de preservación digital, establecimiento de cronogramas y evaluaciones periódicas.
- Gestión de archivos: NARA almacenará el contenido digital en el Repositorio de Objetos Digitales (*Digital Object Repository*) de confianza y proporcionará administración y acceso continuos al contenido a lo largo de su ciclo de vida. El repositorio de NARA se basará en los conceptos incorporados en el Modelo de referencia para sistemas abiertos de información de archivo OAIS (*Open Archival Information Systems*), ISO 14721: 2012 para repositorios digitales fiables.
- Autenticidad: se refiere a la confiabilidad del registro como una representación precisa del original. Aquí también se garantizará la autenticidad según OAIS.
- Metadatos de preservación: identificadores digitales persistentes y metadatos de preservación de registros sobre cada objeto digital. Los metadatos de preservación, garantizan que la información contextual, administrativa, descriptiva y técnica esencial se conserve junto con el objeto digital.
- Relaciones organizacionales: NARA participará activamente con las comunidades de preservación digital locales, nacionales e internacionales para compartir información y experiencias, buscar orientación y colaborar para abordar los desafíos de la preservación digital.

Finalmente, señalar que NARA ofrece una guía de preservación digital llamada *Digital Preservation Guidance Electronic Records Management and Transfer Guidance and Digital Preservation,* así como un marco de preservación digital llamado *Digital Preservation Framework for Risk Assessment and Preservation Planning*; ambos cuentan con una serie de recursos disponibles en línea para su reutilización y adaptación.

b. *Library of Congress*

La Biblioteca del Congreso o *Library of Congress*, contó con el programa *National Digital Information Infrastructure and Preservation Program* (NDIIPP), el cual actualmente no se encuentra activo, pero tuvo un gran éxito y se ha constituído como un precedente en la creciente comunidad de preservación digital de Estados Unidos (Library of Congress, s.f.-a).

Además de esto (Library of Congress, s.f.-b, párr.a)

> *The Library of Congress is actively committed to developing, following and promoting effective methods for digital content management, organization, preservation, and access; conducting and encouraging research in digital preservation sciences and technologies; and building relationships with stakeholder communities to share digital collections management information, practices, and resources.*

Dentro de la Biblioteca del Congreso, los esfuerzos de preservación digital se encuentran distribuidos en diversas unidades, e incluyen "*programs related to digital content packaging and ingest, monitoring and reporting of digital storage, sustainable digital file formats, metadata and more*" (Library of Congress, s.f.-b).

Al igual que NARA, la Biblioteca del Congreso ofrece una serie de recursos en línea, disponibles para ser consultados y utilizados, dentro de los que se incluyen:

- Informes y eventos.
- El sitio web *Sustainability of Digital Formats.*
- Iniciativa de Directrices Digitales de Agencias Federales (*Federal Agencies Digital Guidelines Initiative* FADGI).
- La Declaración de formatos recomendados.
- Herramientas y *software* de código abierto (BagIt File Packaging Format, Bagger, BagIt-Python, BWF MetaEdit, PREMIS).

c. *Federal Agencies Digital Guidelines Initiative* (FADGI)

Se trata de un sitio creado como esfuerzo colaborativo de agencias federales desde 2007, con el fin de articular un conjunto sostenible común de pautas técnicas, métodos y prácticas para contenido histórico, archivístico y cultural digitalizado y nacido en formato digital (Federal Agencies Digital Guidelines Initiative [FADGI], 2017).

Debido a la especialización en conocimientos requerida, se crearon dos grupos de trabajo (FADGI, 2017): por un lado, el Grupo de Trabajo de Imágenes Fijas (*Still Image Working Group*) enfocado en el contenido de imágenes como libros, manuscritos, mapas e impresiones fotográficas y negativos, mientras que, por el otro lado, está el Grupo de Trabajo Audiovisual (*Audio-Visual Working Group*) el cual centra su trabajo en películas de sonido, video e imágenes en movimiento.

Cabe resaltar que (FADGI, 2017, párr.4)

> *The participating agencies share the belief that common guidelines will enhance the exchange of research results and developments, encourage collaborative practices and projects for digital material among federal agencies and institutions and provide the public with a product of uniform quality. They will also serve to set common benchmarks for service providers and manufacturers.*

Esta iniciativa cuenta con un cuadro de resumen que actualizan constantemente, en el cual se puede consultar información acerca del impacto de los esfuerzos y el trabajo realizado por FADGI (FADGI, 2021).

Finalmente, indicar que cada uno de los dos grupos de trabajo cuentan con una página web en la que se pueden observar resultados obtenidos y más información sobre el funcionamiento de los mismos.

1.3.1.4. América Latina

En América Latina, existen diferentes casos para analizar el abordaje que ha tenido la preservación digital a largo plazo de información y documentos de archivo. A continuación se destacan las experiencias de México y Brasil, donde gracias a los esfuerzos realizados por el

programa InterPARES, y en particular a partir de InterPARES 3 (2007-2012), se iniciaron las investigaciones correspondientes al tema de preservación digital en ambos países.

Así también, se incluye el abordaje de la temática del Archivo digital en el país de Colombia con el Proyecto ADN Archivo Digital Nacional y los Fundamentos de Preservación a Largo Plazo.

México, por su parte, desarrolló la investigación basada en dos iniciativas:

a) **Políticas de preservación del Banco de México (Junio 2008 - diciembre 2009)**

En el estudio que se llevó a cabo en este banco mexicano, el principal objetivo fue "establecer criterios generales para la preservación de archivos con valor histórico del Banco, mediante el desarrollo de políticas y lineamientos para la gestión y preservación, en el largo plazo, de documentos de archivo dentro del Banco" (Barnard-Amozorrutia, 2020, p.83-84).

Cabe resaltar que el Banco de México ya contaba con políticas y lineamientos; un esquema lógico de metadatos, cuadro de clasificación documental y un catálogo de disposición documental; así como con un sistema tecnológico para llenado de metadatos, un sistema de control de archivos físicos y electrónicos, y un sistema de gestión documental automatizado para la producción y conservación de documentos de archivo en su etapa administrativa (AD) (Barnard-Amozorrutia, 2020).

Sin embargo, a pesar de la infraestructura tecnológica adelantada con la cual contaban y los esfuerzos realizados para "regular la preservación de documentos de archivo digitales que serían conservados en el largo plazo" (Barnard-Amozorrutia, 2020, p.88), la autora señala que "hasta donde se conoce, las políticas de preservación no fueron instrumentadas. No obstante, es posible apuntar que, con ciertas actualizaciones, las políticas aún son vigentes" (2020, p.90).

b) **Políticas y lineamientos para la gestión documental y preservación de archivos digitales del Tribunal Electoral del Poder Judicial de la Federación (Junio 2010 - diciembre 2010)**

Para este caso específico, el objetivo perseguido fue "desarrollar las políticas y lineamientos para la gestión documental y preservación de archivos digitales en el Tribunal"

(Barnard-Amozorrutia, 2020, p.91), esto conforme a la metodología propuesta por el proyecto InterPARES 3.

Así como en el caso anterior, esta entidad ya contaba con un marco normativo en materia de archivos y de gestión documental, dentro de los que destacan: Lineamientos para la organización, descripción y conservación del Archivo Institucional, cuadro de clasificación documental y catálogo de disposición documental; a los que se pueden sumar normativas relacionadas con seguridad informática, acceso a la información y transparencia (Barnard-Amozorrutia, 2020, p.91).

Dentro de la normativa en materia archivística, si bien se trataba el tema de los documentos electrónicos, no se contaba con lineamientos específicos en cuanto a la preservación documental (Barnard-Amozorrutia, 2020, p.91).

Este proyecto, tenía como propuesta la creación de políticas y otras normas que permitieran (Barnard-Amozorrutia, 2020, p.91):

> (...) la producción, conservación y preservación en el largo plazo. Esta incluiría requisitos y funcionalidades para una herramienta tecnológica para archivos en cualquier formato durante su vida administrativa, así como los correspondientes del Archivo Histórico para preservación en el largo plazo. Se pretendía que el Tribunal contara con políticas y lineamientos para mantener archivos auténticos, fiables, precisos y accesibles.

Asimismo, se pretendía llevar a cabo el proceso de preservación digital de forma que los documentos se pudieran mantener a lo largo del tiempo, independientemente de los cambios económicos presentados en el tiempo. Sin embargo, la misma autora Barnard-Amozorrutia (2020), señala que finalmente, no se tuvo la información para corroborar la instrumentación, tanto de la política como de los lineamientos.

Ambos casos, son una muestra de la existencia de las iniciativas mexicanas para hacer frente a la preservación digital de la información y de los documentos de diversas organizaciones, así como también la cantidad de esfuerzos necesarios, principalmente en cuanto a la implantación de políticas, que requieren de la voluntad de los principales actores y autoridades, para ser implementados con éxito.

Como parte del contexto de aplicación de InterPARES 3, Brasil desarrolló 10 estudios de los cuáles la autora Lacombe-Rocha (2020) destaca tres:

a) ***BRCS01 – Procedimentos para a gestão e a preservação da Autorização de Internação Hospitalar (AIH) produzida no Sistema de Informação Hospitalar Descentralizado (SIHD)***

Este estudio fue dirigido a la *Autorização para Internação Hospitalar* (AIH), ya que los documentos que utiliza demuestran (en materia financiera) el derecho de recibir los servicios que ofrece el *Sistema Único de Saúde* (SUS) (Lacombe-Rocha, 2020, p.58).

La autora Lacombe-Rocha (2020, p.60), señala que a pesar de que se conocen las responsabilidades de la custodia legal de los documentos de este sistema, tanto en soporte físico como electrónico, no existen disposiciones para llevar a cabo procesos de transferencias de documentación al archivo institucional; el mecanismo que se ha utilizado para garantizar la precisión, fiabilidad y autenticidad del AIH, es la realización de copias de seguridad semanales, quincenales y mensuales, almacenadas en tres servidores diferentes.

Así mismo, se señala que la problemática es provocada a raíz de que el sistema permite realizar cambios -en caso de necesidad-, ya que estos cambios provocan la modificación de contenido del documento original, puesto que hay una superposición de la información, provocando la pérdida de información inicial y el documento que se guarda en la base de datos se convierte en uno diferente (Lacombe-Rocha, 2020, p.60-61).

Para esta situación, se planteó un plan de acción en dos etapas (Lacombe-Rocha, 2020):

- La primera etapa: incluyó tres acciones principales: definir estrategias con las máximas autoridades responsables, para evitar la sobreescritura de información en casos de reprocesamiento; definir los plazos y el destino final de los documentos en conjunto con las autoridades competentes; y presentar al Archivo Nacional la propuesta del plan de Clasificación y la Tabla de Plazos de los documentos del Ministerio de Salud.
- La segunda etapa: de acuerdo con los plazos y el destino definido, adoptar procedimientos de almacenamiento. Para esto se proponen algunas opciones: preservar el AIH en su forma manifiesta, ya sea generar un documento en formato PDF o XML y

almacenar en una base de datos o generar un formulario en XML y almacenarlo en una base de datos; la segunda opción sería evaluar el plazo del formulario almacenado y considerar la preservación digital señalada en InterPARES 1.

b) BRCS02 – *Procedimentos para produção, gestão e preservação de fotografias digitais produzidas pela Assessoria de Comunicação da Unicamp*

El segundo caso estudiado en Brasil, se dirigió a registros fotográficos de coberturas periodísticas; así lo explica Lacombre-Rocha (2020, p.66):

> *A entidade digital estudada trata-se dos registros fotográficos de coberturas jornalísticas, produzidos pela ASCOM da UNICAMP, também chamados de reportagens fotográficas. Esses registros fotográficos são produzidos em decorrência da produção de artigos, notas e reportagens sobre pesquisas, cursos, projetos de extensão, convênios de cooperação, transferência de tecnologia e demais realizações promovidas pela UNICAMP, além da produção de material de divulgação institucional e da edição das publicações da universidade.*

Estas fotografías, son clasificadas y agrupadas en colecciones temáticas, son transferidas al repositorio digital del *Sistema Arquivo Digital da ASCOM*, donde se archivan en alta resolución en el servidor del *Arquivo Central do SIARQ*. Una vez que han sido almacenadas, se lleva a cabo la descripción e indexación de los registros fotográficos de acuerdo al *Manual de Organização de Arquivos da ASCOM* en el sistema SIARQ/PESQUISA, así también, los metadatos se ingresan a la base de datos de manera manual, basados en la ISAD(G) (Lacombe-Rocha, 2020, p.66-67).

Después de los análisis realizados a esta serie documental, se detectó la necesidad de mejorar procedimientos de producción y mantenimiento, para apoyar la preservación digital a largo plazo, garantizando así la autenticidad y accesibilidad a través del tiempo, para lo cual se incluyeron aspectos como: monitoreo del formato de archivo, para implementar acciones necesarias para su preservación; definición de un formato más adecuado para la preservación a largo plazo; y evaluar aspectos de seguridad del repositorio (Lacombe-Rocha, 2020, p.68).

El plan de acción propuesto para este caso presentado en Brasil incluyó (Lacombe-Rocha, 2020, p.72-73): el cambio en el formato digital de las fotografías, eligiendo el CAMERA-RAW

-formato propietario de cada cámara digital, variando según el Modelo y el fabricante-, y finalmente será almacenado en TIFF; además, se propuso implementar mayor seguridad en la solución de almacenamiento, incluyendo estrategias como: pistas de auditoría, metadatos de uso y seguimiento, política de seguridad y acceso, respaldos de seguridad.

c) BRCS05 – Procedimentos para gestão e preservação dos relatórios de notas e frequência dos alunos produzidos no sistema de informação acadêmica da Unicamp

Para el tercer y último caso, se estudia la entidad digital del documento *boletim de notas e frequência dos alunos de graduação*, por medio del cual se lleva a cabo el registro del control de frecuencia y evaluación del desempeño académico de los estudiantes de pregrado de la UNICAMP (Lacombe-Rocha, 2020, p.73).

Además de contener la información de las condiciones para determinar la aprobación de cursos, la importancia de esta serie documental recae en que es utilizada para crear otros documentos relacionados con estudiantes y con profesores, por ejemplo: expedientes académicos, informes de finalización del plan de estudios e informes de carga de trabajo didáctico del profesor (Lacombe-Rocha, 2020, p.74).

Lacombe-Rocha (2020, p.74) explica que el *boletim de notas e frequência dos alunos de graduação,* se muestra por medio de un documento HTML a partir de la consulta de una base de datos; y cabe resaltar que el acceso es controlado: las consultas pueden ser realizadas por profesores o funcionarios de DAC, quienes pueden ver la información y en el sistema quedan registradas las fechas de acceso, entrada de datos y control de contraseñas. Sin embargo, la creación o alteración de datos está limitado a técnicos autorizados por la *Diretoria de Serviço de Registro e Gerenciamento Acadêmico* así como del *Centro de Computação* de la universidad, lo cual permite la inspección y seguimiento de las acciones que se realicen.

La problemática que se presenta con estos documentos, es que al realizar modificaciones (solicitadas de manera formal), se sobreescribe el documento digital. Si bien la versión original se encuentra impresa en papel y se archiva de manera física, añadiendo una copia de los cambios realizados, dentro del sistema no se pueden observar estos cambios, puesto que como se mencionó anteriormente, los datos se sobreescriben y en el sistema solo queda la versión más actualizada.

De esta forma "*O documento digital não atende a todos os elementos e atributos necessários a um documento arquivístico, tais como as características de forma fixa e de conteúdo estável (as notas podem ser alteradas), não tem explícita a relação orgânica com os outros documentos que participam da ação*" (Lacombe-Rocha, 2020, p.75).

Dentro del plan de acción tomado para este caso, se reconoce la necesidad de realizar cambios en el sistema, de manera que "*se assegure a forma fixa e o conteúdo estável, bem como que a relação com os demais documentos que participam da ação fique explícita na forma de metadados*"; para lo cual se propone: conservar los componentes digitales del documento emitido por el maestro y conservar el documento en su forma manifiesta (PDF, XML u otro formato similar) (Lacombe-Rocha, 2020, p.80).

Al finalizar la presentación de estos casos específicos de Brasil, los autores hacen énfasis en algunas conclusiones de gran relevancia para el tema de preservación de documentos de archivo digital, entre las que destacan (Lacombe-Rocha, 2020, pp.80-81):

- La preservación de los documentos de archivo digitales debe garantizar las características básicas del documento de archivo, lo cual muchas veces no es tan evidente como lo es en los documentos en soporte papel. Así, por ejemplo, se debe asegurar la integridad del documento (la forma fija, el contenido estable), así como la relación con la entidad productora.
- Existe dificultad en reconocer a las entidades digitales como documentos de archivo, sino que se consideran solo como información de consulta.
- Se refuerza la importancia de la alianza entre los productores y archivos en la construcción de soluciones de preservación digital, reforzando la necesidad de formación de equipos multidisciplinarios que involucren a profesionales de las áreas de Archivo, Administración, Tecnologías de la Información y Comunicación.
- Resulta fundamental formalizar una política institucional de gestión documental y preservación digital, esto debido a que las políticas, los programas y los procedimientos relacionados con la preservación digital deben estar bien registrados y establecidos para garantizar que los documentos conservados sigan siendo auténticos y accesibles durante el tiempo que sea necesario.

En el caso particular de Colombia, se presentan dos iniciativas importantes, la primera relacionada con el tema del archivo digital, por medio del Proyecto ADN Archivo Digital Nacional y la segunda, con la presentación del instrumento emitido por el Archivo General de la Nación de Colombia titulado Fundamentos de Preservación a Largo Plazo.

En el caso del *Proyecto ADN Archivo Digital Nacional*, se establece como prioridad estratégica en el año 2015, como parte del Plan Nacional de Desarrollo 2014-2018 del Estado colombiano, indicando como una de las primeras acciones dotar de infraestructura tecnológica para la entrada en labores del ADN. Para 2016, se crea el marco de referencia y el modelo de preservación digital, esto con el acompañamiento de expertos internacionales. Un año después, en 2017, se lleva a cabo la adquisición de la infraestructura tecnológica parametrizada, incluyendo también un módulo de acceso abierto de las imágenes digitalizadas de fondos históricos y, para 2018, se implementa el sistema de preservación digital (Archivo General de la Nación de Colombia, s.f.).

El Proyecto del ADN de Colombia, se encuentra basado en el modelo OAIS, propuesto en la norma ISO 14721:2015 e incluye "la definición de políticas, lineamientos, directrices, estándares y la proyección de la infraestructura tecnológica necesaria para recibir las transferencias de los archivos de valor histórico en formato digital o electrónico de entidades públicas (...) para asegurar su protección, conservación y acceso a los ciudadanos" (Archivo General de la Nación de Colombia, s.f., p.2).

En cuanto al instrumento llamado *Fundamentos de Preservación a Largo Plazo*, nace a partir de la necesidad que observa el Estado colombiano para "garantizar la perdurabilidad y accesibilidad de la información digital que se está produciendo en el desarrollo de las funciones de cada una de las entidades" (Archivo General de la Nación de Colombia, 2018, p.5)

Dentro del documento publicado, se encuentra un apartado de conceptualización que permite conocer los fundamentos de preservación digital, y además, ofrece información de apoyo para el establecimiento de la política, las acciones, estrategias y técnicas necesarias para llevar a cabo la preservación digital a largo plazo.

Finalmente, cabe resaltar que existen otras iniciativas dentro del territorio Latinoamericano, que se han autodenominado como "Archivos Digitales" pero que en realidad no cumplen con las

características básicas para considerarse como tales desde el punto de vista archivístico. Algunos ejemplos de estas iniciativas son:

- **Archivo Digital de Efímera de América Latina y el Caribe**

Si bien esta es una iniciativa de la *Princeton University Library*, se trata de una colección de archivo (con documentos provenientes principalmente de Argentina, Bolivia, Chile y Cuba), el cual se encuentra en línea y accesible desde el año 2015. El objetivo de la Universidad y sus socios es "continuar agregando cientos de nuevos materiales efímeros digitalizados cada mes y convertir esta vasta y excepcional colección de un archivo oculto a un recurso dinámico que sirva de apoyo a presentes y futuras actividades académicas" (Princeton University Library, 2021, párr1).

Con la creación de la plataforma, a la que llamaron "archivo digital", se ofrece acceso abierto y en línea a la colección de más de 12 mil documentos que "en su gran mayoría son fuentes primarias raras y difíciles de hallar que no se encuentran disponibles en otros archivos" las cuales antes eran inaccesibles (Princeton University Library, 2021).

- **Archivo Digital del Archivo Histórico de la Policía Nacional de Guatemala**

Mediante la plataforma en línea de esta iniciativa, a la que también llamaron "archivo digital", se facilitan los documentos históricos digitalizados por el Archivo Histórico de la Policía Nacional de Guatemala (AHPN), dentro de su acervo se encuentran "más de 10 millones de imágenes escaneadas de documentos que se encuentran en el Archivo Histórico de la Policía Nacional" (Archivo Digital del Archivo Histórico de la Policía Nacional de Guatemala, s.f.).

Los documentos dentro del archivo digital "están ordenados según el orden original de la organización administrativa de la propia Policía Nacional" y se aclara que las descripciones archivísticas de AHPN, se elaboraron basadas en la Norma ISAD(G) (Archivo Digital del Archivo Histórico de la Policía Nacional de Guatemala, s.f.).

Estos dos últimos casos presentados, son reflejo de un esfuerzo importante que han realizado distintos países y organizaciones para rescatar parte de la memoria documental que conservan, y así colocarla al servicio de la sociedad. Sin embargo, se ha utilizado de manera errónea el

concepto de archivo digital con base en la rigurosidad archivística, y podrían considerarse simplemente repositorios de consulta con acceso abierto.

Se realiza esta acotación, ya que no todas las iniciativas que se declaran como "archivos digitales" lo son, pues no se trata únicamente de una plataforma tecnológica, sino que deben tener la capacidad de preservar las características de integridad, fiabilidad, autenticidad y usabilidad de los documentos de archivo a largo plazo, y además estar basados en políticas que respalden su creación y mantenimiento.

1.3.2. Ámbito Nacional

En el presente apartado, se realiza un recorrido por las principales iniciativas y proyectos teóricos desarrollados a nivel nacional en Costa Rica, relacionados con la temática de Archivo Digital y Preservación Digital.

1.3.2.1. Proyecto para la definición del archivo digital de la Universidad de Costa Rica

Este proyecto se trató de la primera iniciativa a nivel país sobre preservación digital. Se llevó a cabo en el año 2013, para la implementación de un archivo digital en la Universidad de Costa Rica. Fue desarrollada por diferentes actores, dentro de los que destacan: el Archivo Universitario Rafael Obregón Loría (AUROL), el profesor español Jordi Serra Serra de la Universitat de Barcelona (como colaborador externo), la Sección de Archivística, el Centro de Informática y la Unidad de Gestión de Proyectos, estos tres últimos de la Universidad de Costa Rica.

Este grupo de trabajo enfocó sus esfuerzos en resolver las necesidades de preservación digital presentes en la UCR, ante lo cual se planteó la necesidad de establecer una política institucional de preservación digital, la definición de requisitos funcionales para la implementación de un archivo digital y un protocolo de ingreso y custodia para la conservación de documentos electrónicos (Serra-Serra, 2013a).

La metodología propuesta para este proyecto se basó en (Serra-Serra, 2013a, p.6):

- *Digital Preservation Europe. DPE Repository Planning Checklist and Guidance DPED 3.2. April, 2008.*

- *Consultative Committee for Space Data Systems. Audit and certification of trustworthy digital repositories (CCSDS 652.0-M-1). Recommended Practice, Issue 1. Washington, DC: CCSDS, September 2011.*
- *Risk Assessment Handbook. Kew: The National Archives, 2011.*

Para esto, se plantearon dos fases principales (Serra-Serra, 2013a):

- **Nivel estratégico: Política de preservación digital**

En esta fase se plantea una evaluación de los riesgos para la continuidad digital, el análisis del contexto y la definición del tipo de archivo, la definición funcional y técnica del archivo digital, así como la elaboración de una política institucional de preservación.

- **Nivel Operativo: Reglas de preservación**

Aquí, se esperaba llevar a cabo la implementación y análisis de resultados obtenidos en un plan piloto. Sin embargo, esta etapa no fue puesta en marcha.

A pesar de que no se llevó a cabo la implementación del proyecto, sí se pueden destacar algunos de los resultados teóricos obtenidos durante la primera fase, que se detallan a continuación.

- Informe de evaluación de riesgos y de contexto

Para realizar la evaluación de riesgos, se utilizó un cuestionario desarrollado por los Archivos Nacionales de Reino Unido del año 2011, en el marco del *Digital Continuity Project* ("*Stage 3: Assess and manage risks to digital continuity*") (Serra-Serra, 2013b).

Este instrumento (Serra-Serra, 2013b), fue aplicado a 5 participantes de la UCR que formaban parte del proyecto, específicamente al AUROL, al Centro de Informática, a dos responsables de la Unidad de Gestión de Proyectos y a una profesora de la Sección de Archivística. Por medio de sus respuestas se identificaron riesgos medios y altos relacionados con los siguientes temas: identificación de la continuidad digital como reto y responsabilidades; requisitos de información y dependencias tecnológicas; y gestión de la información.

Por su parte, para la evaluación del contexto, se completó otro cuestionario basado en el apartado 3 ("*Repository classification*") del modelo PLATTER. Los resultados de este instrumento ofrecieron las siguientes conclusiones (Serra-Serra, 2013b):

a) La Universidad de Costa Rica debe disponer de un archivo digital operativo.
b) La Universidad de Costa Rica debe disponer de un archivo dimensionado para 1.500 usuarios totales en el primer año, con crecimiento progresivo.
c) El archivo deberá gestionar restricciones de acceso a la documentación que reciba mediante transferencias que se realizarán a iniciativa de las unidades.
d) La infraestructura tecnológica del archivo digital debe ser interna.

Este último cuestionario, fue completado por el AUROL.

- Modelo funcional y técnico del Archivo Digital

En primera instancia, se llevó a cabo un análisis de escenarios tecnológicos para "la implantación de la solución tecnológica que debe dar respuesta a las necesidades del ADUCR, de acuerdo con las obligaciones expresadas en la política de preservación digital" (Serra-Serra, 2013, p.5c).

Este análisis contempló los sistemas existentes en la UCR y la previsión de crecimiento a corto y mediano plazo. Además se plantearon los siguientes servicios para ser integrados en el *software* del Archivo Digital UCR (ADUCR): Servicio web para la recepción de SIP (transferencias), Interfaz para la creación manual de SIP, detección de virus, reconocimiento de formatos y extracción de sus propiedades significativas, conversión de formatos de fichero, firma digital y sellado de tiempo, gestión de identidades externas, interfaz para la búsqueda, visualización y petición de copias de documentos, así como servicio web para la recepción y remisión de peticiones de DIP (Serra-Serra, 2013c).

Además, se contemplaron tres escenarios para el ingreso de documentos, datos y evidencias al ADUCR: transferencia automatizada, transferencia con intermediación humana y transferencia con tratamiento previo de la documentación (Serra-Serra, 2013c).

En segundo lugar, se definieron los requisitos funcionales, que incluyen los requisitos para los procesos de ingreso, preservación y acceso requeridos por la solución tecnológica para el

ADUCR. Además de esto, se establecieron los requisitos técnicos e integraciones y los requisitos de interoperabilidad y normalización. (Serra-Serra, 2013c).

Finalmente, como un anexo en este modelo, se ofrece un listado de soluciones tecnológicas disponibles a la fecha de 2013, para los servicios e interfaces requeridas por el ADUCR.

- Política de preservación digital

Se definen dos partes en esta propuesta de política de preservación digital: la declaración de la política y la política de preservación digital. Dentro de la declaración (Serra-Serra, 2013d), se establecen la misión, los objetivos, los principios y la periodicidad de actualización de la política.

En la sección de la política como tal se definen al ADUCR como "responsable de conservar y dar 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, formará parte del Sistema de Archivos de la Universidad de Costa Rica, y estará a cargo del Archivo Universitario Rafael Obregón Loría " (Serra-Serra, 2013, p.7d).

Además de esto, se incluye la delimitación del tipo de información que se conservará, la creación de la Comisión Institucional del Archivo Digital de la Universidad de Costa Rica (CIAD), los recursos humanos requeridos para garantizar el funcionamiento del ADUCR, los requisitos de los sistemas de información, la asignación de un presupuesto para la sostenibilidad financiera y por último la prevención de pérdidas y actuación en caso de desastre (Serra-Serra, 2013d).

- Estrategia de preservación digital

Como un derivado de la política de preservación digital, se segrega la estrategia de preservación digital con el fin de complementarla. Esta estrategia incluye (Serra-Serra, 2013e):

a) **Plan de datos**: constituído por la información a conservar (documento, dato, evidencia de información) y los contenedores de información (SIP, AIP y DIP).
b) **Plan de ingreso**: este incluye: documentos, datos y evidencias susceptibles de ingreso, otras fuentes de ingresos, preceptividad del protocolo de ingreso y custodia, elaboración del protocolo de ingreso y custodia, sincronía en proyectos de desarrollo tecnológico,

escenarios funcionales de la transferencia, realización de la transferencia y responsabilidad sobre la conservación de los documentos, datos y evidencias.

c) **Plan de conservación**: en este plan se contemplan las condiciones de conservación de los documentos, datos y evidencias, la detección del riesgo de obsolescencia tecnológica, la ejecución del proceso de migración y la obsolescencia tecnológica del plan de datos.
d) **Plan de acceso**: aquí se lleva a cabo la identificación de las comunidades designadas de usuarios, los canales de acceso, la obtención de los documentos, datos y evidencias, los límites al acceso y el monitoreo de la base de conocimiento de cada comunidad designada.
e) **Plan de tecnología**: en este se incluye la seguridad y protección de la integridad, la disponibilidad y continuidad del servicio, así como la escalabilidad y actualización de la infraestructura.
f) **Plan de continuidad**: incorpora la continuidad de la capacidad financiera del archivo digital, de la base de conocimiento del archivo digital, del archivo digital y la continuidad en caso de desastre.

Esta estrategia, adjunta como anexos un calendario de obligaciones periódicas, en el que se determinan acciones y plazos por cumplir, una relación de registros de actividad del ADUCR y una relación de formatos de fichero para los distintos tipos de contenido.

- Modelo para el Protocolo de ingreso y custodia

Se trata de una plantilla en el cual se definen cada uno de los campos requeridos para el protocolo de ingreso y custodia. Esta plantilla incluye los siguientes apartados (Serra-Serra, 2013f):

a) *Datos identificativos*: identificador, órgano productor o custodio.
b) *Alcance*: documental, tecnológico, orgánico, cronológico y duración del protocolo y fecha de revisión.
c) *Parámetros de ingreso*: canal de transferencia, formatos de fichero admitidos, metadatos descriptivos obligatorios, características del contenedor de información de ingreso (SIP), verificaciones y normalización.

d) *Propiedades significativas que conservar por el ADUCR*: tipo documental, propiedades a conservar relacionadas con: la apariencia, las funcionalidades, la autenticidad y el valor evidencial.
e) *Plazos de conservación*: plazo total de conservación, de las propiedades significativas de: apariencia, funcionalidades y autenticidad.
f) *Derechos que se ceden*: derechos de difusión y acceso, de uso, de modificación para preservación.

Finalmente, se indican las responsabilidades adquiridas por las partes al firmar el protocolo propuesto.

1.3.2.1. Archivo Nacional Digital (ADN)

Esta es la iniciativa presentada por el Archivo Nacional de Costa Rica, con el fin de lograr la preservación de documentos digitales a largo plazo, y que como ente rector del Sistema Nacional de Archivos (SNA), pretende ofrecer a las instituciones que forman parte de dicho sistema.

El principal objetivo del ADN es "desarrollar un servicio de preservación y custodia de documentos" (Cantillano-Mora, Rojas-Mora, Otárola-Saénz, Valerín-Alvarado & Irola-Rojas, 2019, p.69). Por medio de este servicio, el ADN busca ofrecer (Cantillano-Mora et al, 2019, pp.69-70):

- Un punto único de resguardo de documentos electrónicos en el Estado costarricense.
- Un punto centralizado de acceso a los documentos electrónicos de la administración pública.
- Una solución nacional para la interoperabilidad de sistemas de documentos electrónicos.
- Estandarización de la preservación de documentos electrónicos.
- Seguridad informática y mejora continua.
- Normalización de la descripción archivística.
- Herramientas básicas de producción y recepción de documentos electrónicos, para instituciones que aún no cuentan con este tipo de soluciones informáticas.
- Asesoría y soporte técnico.
- Capacitación y acompañamiento durante su implementación.

Se señala que uno de los factores clave para alcanzar el éxito de un proyecto de esta índole es el nivel de compromiso de la institución, debido a que "significará en algunos casos la normalización en la ejecución de las tareas archivísticas en soporte electrónico y, en muchos otros, conllevará un cambio en las prácticas administrativas que se desarrollan en las diferentes unidades de las instituciones públicas" (Cantillano-Mora et al, 2019, p.71).

El proyecto de ADN, se compone de una serie de elementos que son requeridos para su debida implementación. Estos elementos son (Cantillano-Mora et al, 2019, p.73):

a) Implementación, Normativa y Capacitación: se brinda acompañamiento a las instituciones en temas como diagnósticos de producción de documentos, sello electrónico, interconexión, análisis de instrumentos archivísticos, parametrización de repositorio digital, carga de documentos electrónicos, evaluación de resultados, entre otros.
b) Mantenimiento y soporte: cuyo servicio contempla: actualización constante, soporte técnico, así como documentación y manuales de uso.
c) Herramienta de preservación: en la que se ofrece un repositorio digital basado en el Modelo de referencia OAIS, descripción multinivel y uso de metadatos con estándares como EAD, EAC y EAG, almacenamiento de todo tipo de documentos electrónicos y en distintos formatos, creación de paquetes de información archivística, compuestos por el documento, firmas digitales, estampas de tiempo, sello electrónico y metadatos incorporados asociados, protección y conservación de dichos paquetes, creación de índices electrónicos, entre otras características. Además de esto, permitiría a una institución que carezca de una solución para la gestión de documentos electrónicos, incluir interfaces relacionadas con la producción y recepción de documentos.
d) Enlaces y continuidad del negocio: se procura la instauración de un plan de continuidad del negocio, así como enlaces punto a punto e interoperabilidad con otros sistemas, entre otros.
e) Almacenamiento y seguridad: el ADN proporciona almacenamiento en plataformas seguras, respaldos de información, planes de contingencia, cifrado de bases de datos, entre otros.

El proyecto ADN se encuentra basado en el modelo de preservación OAIS, un modelo de gran popularidad alrededor del mundo ya que "garantiza que un documento sea auténtico, veraz e íntegro a través del tiempo, y que, a su vez faculta su accesibilidad, fiabilidad y utilización" (Cantillano-Mora et al, 2019, p.76).

Según Cantillano-Mora et al. (2019, p.81) dentro de la metodología de implementación del ADN, el apoyo y compromiso de parte de las altas jerarquías fue un factor clave en cada una de las fases. Además, uno de los primeros pasos fue la conformación de un equipo interdisciplinario, en el que se involucraron profesionales de áreas como archivística, informática, financiero/contable/proveeduría.

A continuación, se señalan las etapas de implementación del ADN (Cantillano-Mora et al, 2019):

Etapa 1: Identificación y diagnóstico: incluyó la revisión de instrumentos archivísticos, un diagnóstico del estado de gestión de documentos y el número de funcionarios con firma digital. En esta primera etapa se pudieron definir las unidades participantes, basado en el mayor volumen de documentos electrónicos y la mayor cantidad de funcionarios con firma digital.

Etapa 2: Configuración del Repositorio Digital: basado en el cuadro de clasificación y las tablas de plazos de conservación de documentos, se aplicó la parametrización de la Norma Nacional de Descripción para definir los metadatos obligatorios, así como la definición de los roles y permisos de los usuarios a nivel del sistema.

Etapa 3: Recopilación y carga de documentos electrónicos: la recopilación de los documentos electrónicos se llevó a cabo mediante un sitio colaborativo en línea, y la carga de dichos documentos fue realizada por medio de la herramienta ADN-Captura. Finalmente, se generó un informe de carga de documentos, el cual fue entregado a cada unidad productora.

Etapa 4: Capacitación y acompañamiento en la implementación: la capacitación se realizó mediante una presentación general de la solución y se efectuaron prácticas y demostraciones individuales con las personas participantes de cada unidad administrativa.

Etapa 5: Actualización de normativa archivística institucional: se elaboraron y actualizaron procedimientos, manuales, planes y lineamientos relacionados con la gestión de documentos y prácticas administrativas de las unidades parte del plan piloto.

Etapa 6: Documentación del proceso: esta etapa resulta de gran importancia debido a que permite contar con un control de tareas, ejecuciones y pendientes; así como también, facilita la transmisión de la información y el conocimiento a las personas que se vayan involucrando en cada etapa del proyecto.

Cabe resaltar que el proyecto ADN se ha desarrollado con base en una aplicación informática recibida como donación en el año 2016, para la preservación digital a través de un módulo de repositorio. El plan piloto comenzó a implementarse en el año 2019, en dos unidades administrativas y se propuso extender hacia una segunda etapa, en el Ministerio de Cultura y Juventud (MCJ) (Cantillano-Mora et al, 2019).

En el caso del MCJ, en 2019 se hizo el contrato para la implementación del plan piloto, sin embargo, a finales del 2020 se firmó un finiquito para terminar con el proceso de implementación por dificultades administrativas (S. Irola-Rojas, comunicación personal, 4 de febrero de 2022).

El plan piloto en el Archivo Nacional, se comenzó con algunas oficinas internas. No obstante, la falta de personal disponible y la necesidad de realizar mejoras, ralentizó el avance de los resultados (*Idem*).

S. Irola-Rojas (*Idem*), señala que el plan piloto en el Archivo Nacional terminó a inicios del 2020, con la presentación de un informe final que incluyó la metodología, resultados, conclusiones y recomendaciones. De esta manera, se recomienda que el proyecto se siga implementando a nivel institucional porque responde a la solución de una necesidad identificada de actualización en tecnología para la gestión de documentos.

Finalmente, la Dirección General del Archivo Nacional indica que se implemente el proyecto en toda la institución, de forma gradual. Por lo cual, en agosto del 2021, se toma la decisión de seguir con la implementación únicamente con algunas de las oficinas del Archivo y utilizando solo el módulo de repositorio (*Idem*).

1.3.2.3. Modelo para la preservación de documentos digitales

Se trata de un modelo enfocado en la administración y conservación de documentos digitales, basado en la experiencia y los resultados obtenidos a partir de un "Trabajo Final de

Investigación aplicada de la Maestría Profesional en Administración Universitaria de la Universidad de Costa Rica, denominado *Modelo de Preservación de Documentos Digitales en la Administración Universitaria. Estudio de caso: Universidad Nacional*" (Castillo-Solano & Umaña-Alpízar, 2019, p.131).

Uno de los grandes retos a los que responde esta investigación, es el de "garantizar la autenticidad, perdurabilidad y acceso a la información contenida en los documentos digitales a través del tiempo" (Castillo-Solano & Umaña-Alpízar, 2019, p.131).

Debido al rápido y constante cambio que supone el uso extendido de las TIC en las organizaciones, surgen las necesidades organizacionales de enfrentarse a la gestión de la información producida en el ejercicio de las funciones propias.

De esta forma, las autoras Castillo-Solano y Umaña-Alpízar (2019, p.132) señalan que "al ser los documentos de archivo, el origen institucional de la información fidedigna, la base de la transparencia, y el elemento que habilita a la ciudadanía a reclamar y mantener sus derechos, es imperativo garantizar su acceso, integridad y autenticidad, en el presente y en el futuro".

La preservación digital, por su parte "pretende asegurar el acceso a la información digital a largo plazo, manteniendo la capacidad de consultar y revisar el documento, sin importar su formato" (Castillo-Solano & Umaña-Alpízar, 2019, p.137), lo cual representa un reto para las actuales instituciones y organizaciones, quienes producen documentos, información y datos sin la claridad de su disponibilidad a futuro.

De manera previa al modelo de preservación digital propuesto (Castillo-Solano & Umaña-Alpízar, 2019), se debaten algunos aspectos de vital importancia para la conservación a largo plazo, dentro de los cuáles se destacan: el formato de preservación, el proceso de migración de la información, la conversión de formatos, las propiedades significativas de los documentos y el Modelo de la Cadena de Preservación.

Además de esto, se señala como marco de referencia el Modelo OAIS, en el cual se establece el uso de paquetes de información señalados en la norma ISO 14721: Paquete de Información de

Transferencia (SIP), Paquete de Información de Archivo (AIP) y Paquete de Información de Consulta (DIP) (Castillo-Solano & Umaña-Alpízar, 2019).

También, se considera de vital importancia la existencia de un repositorio digital que permita el almacenamiento consciente y planificado de los documentos, información y datos que se generan en las organizaciones, de manera que dichas organizaciones deben "aplicar políticas y estrategias de preservación, de acceso, de metadatos y protocolos de transferencia, con el fin de garantizar que los documentos, y la información, este disponible en el presente y para futuras generaciones" (Castillo-Solano & Umaña-Alpízar, 2019, p.145)

Las autoras de este modelo (Castillo-Solano & Umaña-Alpízar, 2019), hacen énfasis en la diferencia entre el Archivo Digital/Electrónico y un sistema de gestión de documentos electrónicos de archivo o SGDEA, ya que aunque ambos poseen una estrecha relación en cuanto a su objeto de trabajo común, por un lado el SGDEA "es un sistema que captura, gestiona y provee acceso a los documentos" (p.146), mientras que, por el otro lado, el Archivo Digital "apunta a la gestión y garantía de acceso por un largo plazo, que puede extenderse de forma indefinida" (p.146).

Ya dentro del Modelo de Preservación de Documentos Digitales, Castillo-Solano y Umaña-Alpízar (2019, p.153) indican que este:

> pretende proporcionar una solución metodológica para el desarrollo e implementación de un Archivo Digital, que permita garantizar el acceso, autenticidad, integridad y fiabilidad a la información archivística, como parte de una gestión de calidad en las instituciones públicas, facilitando nuevos servicios y la preservación de la herencia en soporte digital

Dentro de las estrategias de preservación se proponen (Castillo-Solano & Umaña-Alpízar, 2019):

- **Política de Preservación Digital**: con el propósito de "conservar y dar acceso a los documentos digitales" (p.153).
- **Definición del Archivo Digital**: será el "responsable de preservar y garantizar el acceso, autenticidad e integridad de los documentos digitales" (p.154).
- **Plan de Datos**: "consiste en definir las características de los documentos y la información a preservar en el Archivo Digital" (p.154).

- **Plan de Ingreso**: se trata del "proceso de transferencias de los documentos digitales" (p.156).
- **Plan de Conservación**: "proporciona los servicios y funciones de control del entorno del Archivo Digital e incluye las estrategias técnicas con el objetivo de mantener, a través del tiempo, las características de integridad, autenticidad y acceso a la información que se encuentra en custodia" (p.157).
- **Plan de acceso**: "se establecen los servicios de cara a las necesidades de los usuarios finales" (p.159).
- **Plan de Tecnología**: implica la infraestructura del Archivo Digital, debiendo cumplir con "las necesidades de almacenamiento, procesamiento, seguridad y comunicaciones, ser escalable y redundante, utilizando *software* y equipo con tecnología de vanguardia, pero confiable" (p.159).
- **Plan de Continuidad**: el cual debe "garantizar la disponibilidad y la operación ininterrumpida del Archivo Digital" (p.161).

Por último, se proponen el Modelo Funcional del Archivo Digital, el cual define los requisitos funcionales que deben incluirse en el repositorio digital: ingreso, almacenamiento de archivo, gestión de datos, administración, planificación de la conservación y acceso; y el Modelo Tecnológico del Archivo Digital, donde se plantean los servicios y funcionalidades del Archivo Digital en cuanto a: requerimientos de arquitectura tecnológica, almacenamiento y asignación de presupuesto (Castillo-Solano & Umaña-Alpízar, 2019).

1.4. Marco teórico

1.4.1. Gobernanza digital

El Estado costarricense ha promovido el uso de las tecnologías de la información y la comunicación para la mejoría de sus servicios desde principios del siglo XXI. Para ello, ha acatado normativa internacional y ha desarrollado normativa nacional, de manera que existan bases legales que posibiliten cambios positivos en la administración.

Así, se han considerado reuniones internacionales como la Carta Iberoamericana de Gobierno Electrónico (2007), la Segunda Conferencia Ministerial sobre la Sociedad de la Información en

América Latina y del Caribe (2008) y la Carta Iberoamericana de Calidad de la Gestión Pública (2008).

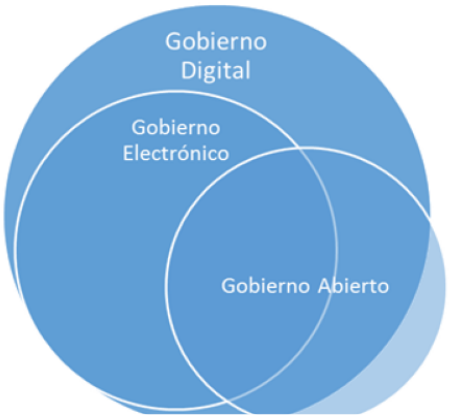
A nivel nacional, se han desarrollado varias leyes como la Ley 8454 Certificados, firmas digitales y documentos electrónicos, del 30 agosto 2005 y la más actual la Ley 9943 Creación de la Agencia Nacional de Gobierno Digital.

La gobernanza digital se refiere al conjunto normativo y políticas que interrelacionan a los distintos actores sociales (Instituciones públicas, sector privado y personas) para optimizar los trámites y recursos, por medio del uso de las TIC.

De ahí, se desprenden otros conceptos que se deben considerar: *gobierno electrónico, gobierno digital* y *datos abiertos*, los cuales en algunas ocasiones han sido considerados como sinónimos, al tener como constante el uso de las TIC para la planificación, la gestión y la administración pública. No obstante, estos términos contienen diferencias en cuanto al alcance de su aplicación.

Al respecto, se presenta la figura 1, en la cual se presenta la relación entre estos conceptos:

Figura 1. *Esquema conceptual de la gobernanza digital.*



Fuente: Cruz-Romero, 2018.

De esta forma, Cruz-Romero (2018), indica que el gobierno electrónico se planteó anteriormente al gobierno digital, donde el primero brinda a los usuarios un conjunto de aplicaciones unilaterales y estáticas en la prestación de servicios, como páginas web y aplicaciones para dispositivos móviles, mientras que el segundo, el gobierno digital, abarca al gobierno

electrónico, al tener un visión integral para la promoción de una cultura institucional más abierta, dinámica y tecnológicamente solvente. Esto ayuda a mejorar la calidad de los servicios, agilizar los trámites de los ciudadanos y a aumentar la transparencia de las organizaciones.

Según la Comisión de las Naciones Europeas (2003, p.3), la administración electrónica es entendida como la utilización combinada de las Tecnologías de la Información y la Comunicación con:

> los cambios organizativos y con nuevas aptitudes encaminadas a mejorar los servicios públicos, los procesos democráticos y las políticas públicas. (...) representa un potente medio de prestar servicios públicos de mejor calidad, reducir los tiempos de espera y mejorar la eficacia en el uso de los fondos, aumentar la productividad y mejorar la transparencia y la rendición de cuentas.

Según la Red de Transparencia y Acceso a la Información (RTA) (2014), la administración electrónica se basa en la utilización de TIC para aumentar la participación ciudadana en la toma de decisiones y la transparencia administrativa, al mejorar los servicios y la información brindada. Con ello se busca promocionar la inclusión e igualdad de oportunidades, independientemente de la situación territorial o social de las personas.

Además, García-Morales (2013) plantea que, por medio de este tipo de administración electrónica, las administraciones se ven obligadas a relacionarse con los ciudadanos por medios electrónicos, mediante el uso de distintos sistemas. Así, por ejemplo, en la Universidad de Costa Rica se brindan servicios por medio de programas informáticos como eMatrícula (plataforma para que los estudiantes realicen los procesos de matrícula y consulta de sus resultados académicos), Portal UCR (para mediar los asuntos laborales con los funcionarios universitarios) o el SiGeDI (Sistema de Gestión de Documentos Institucional) entre otros.

De esta manera, el acercamiento de la Universidad de Costa Rica hacia la comunidad universitaria y demás ciudadanos, debe estar cada vez más mediada por el uso de las TIC para mejorar sus servicios, sin embargo, es preponderante que la información que se gestiona debe ser conservada adecuadamente mediante un Archivo Digital que asegure su uso y conservación durante el plazo correspondiente.

1.4.2. Gestión de documentos de archivo

Los Archivos, tienen dentro de las organizaciones el papel indispensable de "reunir, clasificar, ordenar, describir, valorar, seleccionar, eliminar, conservar, administrar y facilitar los documentos producidos o recibidos en cualquier soporte" (Poder Ejecutivo de la República de Costa Rica, 2017, p.17). Es decir, las acciones archivísticas se tornan fundamentales para asegurar la correcta gestión de la información institucional.

- **Documento de Archivo**

Para el desarrollo de la presente investigación, se debe definir qué es un documento de archivo, independientemente de su soporte. Así, según la Norma UNE-ISO 15489:2016 Información y documentación. Gestión de documentos. Parte 1: Conceptos y Principios, el documento de archivo es la "información creada, recibida y conservada como evidencia (...) y como activo por una organización o individuo en el desarrollo de sus actividades o en virtud de sus obligaciones legales" (Asociación Española de Normalización y Certificación [AENOR], 2016, p.9). Todos los documentos de archivo que se custodian por una organización, en el ejercicio de sus funciones, se conocen como el fondo documental institucional (Poder Ejecutivo de la República de Costa Rica, 2017, p.4).

Los documentos de archivo, independientemente de su forma y estructura, deben contar con las siguientes cuatro características (AENOR, 2016, pp.10-11):

a) Autenticidad: el documento "es lo que afirma ser", "ha sido creado o enviado por el agente del cual se afirma que lo ha creado o enviado" y que "ha sido creado o enviado en el momento en que se afirma".
b) Fiabilidad: aquel documento que "es confiable porque su contenido es completo, exacto y es fiel representación de las operaciones, actividades, o hechos que evidencia" y "del que se puede depender en el transcurso de las subsiguientes operaciones o actividades".
c) Integridad: el documento "está completo e inalterado".
d) Usabilidad: el documento "puede ser localizado, recuperado, presentado e interpretado en un período de tiempo considerado razonable por las partes interesadas".

- **Documento electrónico de Archivo**

La aplicación de la Ciencia Archivística para la gestión de los documentos, logra abarcar tanto documentos en soporte físico como documentos electrónicos. Sumado a ello, para implementar un Archivo Digital y mantener su funcionamiento a largo plazo, es fundamental que la información independientemente de su tipo o clase documental, sea resguardada y mantenida útil y disponible, durante el tiempo en que deba ser conservada.

De esta forma, el término de documento electrónico de archivo, ha sido desarrollado por diversas normativas y autores. En este sentido, Cruz-Mundet lo plantea como: "el documento generado, gestionado, conservado y transmitido por medios electrónicos, informáticos o telemáticos, siempre que incorporen datos firmados electrónicamente." (Cruz-Mundet, 2011, p.32)

Además, la autora García-Morales (2013, p.12), define los documentos electrónicos como "entidades lógicas o virtuales cuya fiabilidad y autenticidad es necesario garantizar a los productores y usuarios". A esta definición se le suman algunas características propias de este tipo de documentos como el hecho que se consignan en soportes magnéticos u ópticos y su información se representa por códigos binarios, los cuales deben ser descodificados para ser comprensibles a los sentidos.

En Costa Rica, de forma oficial, el Ministerio de Ciencia Tecnología y Telecomunicaciones [MICITT] (2013, p.3) ha definido al documento electrónico como "cualquier manifestación con carácter representativo o declarativo, expresada o transmitida por un medio electrónico o informático. En otras palabras, cualquier conjunto de datos creado, preservado, transmitido o visualizado por medios electrónicos puede ser considerado un documento electrónico".

Además, en el artículo 1 del Reglamento a la Ley del Sistema Nacional de Archivos, se indica que un documento que se encuentra en soporte electrónico será (Poder Ejecutivo, 2017, p.3):

> Cualquier manifestación con carácter representativo o declarativo, expresada o transmitida por un medio electrónico o informático, se tendrá por jurídicamente equivalente a los documentos que se otorguen, residan o transmitan por medios físicos.
>
> En cualquier norma del ordenamiento jurídico en la que se haga referencia a un documento o comunicación, se entenderán de igual manera tanto los electrónicos como los físicos. No

> obstante, el empleo del soporte electrónico para un documento determinado no dispensa, en ningún caso, el cumplimiento de los requisitos y las formalidades que la ley exija para cada acto o negocio jurídico en particular.

Como se aprecia, existe un común denominador en cuanto al abordaje del documento electrónico de archivo: el uso indispensable de las TIC para poder realizar la gestión archivística de la información contenida en estos documentos y la necesidad de transformar la información electrónica a mensajes comprensibles para el ser humano, a través de equipos informáticos.

A esto se le debe sumar, el uso de la firma digital como elemento probatorio para establecer la autenticidad de los documentos electrónicos de archivo. Para esto, Costa Rica cuenta con legislación en la materia desde el año 2005, con la entrada en vigor de la ley Nº 8454 Ley de Certificados, Firmas Digitales y Documentos Electrónicos.

En el artículo 8 de la ley 8454 (2005), se define la firma digital como

> 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. Una firma digital se considerará certificada cuando sea emitida al amparo de un certificado digital vigente, expedido por un certificador registrado.

Además, "la validez de la firma implica que el documento no ha tenido alteraciones y que todos los elementos en el momento de la firma eran válidos (protocolos, algoritmos, formatos, certificados y el contenido firmado)" razón por la cual, resulta de un gran importancia desde el punto de vista de la preservación digital.

- **Gestión de documentos**

Como se ha observado anteriormente, en la definición de "documento" brindada por la Norma UNE-ISO 15489:2016, no se realiza una división o diferenciación entre los documentos en soporte electrónico o en soporte analógico, sino que se observa una generalidad de cómo debería concebirse un documento de archivo y la importancia que reviste para las organizaciones.

Todas las organizaciones, independientemente del sector al que pertenezcan (público o privado), generan documentos de archivo que son la prueba de las actividades que se desempeñan en el ejercicio de sus funciones, para brindar un servicio u ofrecer un producto al público.

La autora Russo-Gallo, define la gestión de documentos como el "conjunto de actividades que permiten coordinar y controlar los aspectos relacionados con la creación, recepción, organización, almacenamiento, preservación, acceso y difusión de documentos" (2009, p.10).

También es posible encontrar a otros autores, como es el caso de José Ramón Cruz Mundet (2012, p.85), quien indica que la gestión de documentos es:

> entendida como el conjunto de normas, técnicas y conocimientos aplicados al tratamiento de los documentos desde su diseño hasta su conservación permanente (...) bajo este rubro se agrupa el núcleo de nuestra ciencia, con aspectos tales como la clasificación, la ordenación la instalación, la descripción, la transferencia, la identificación, la valoración la selección y la eliminación, sin ánimo exhaustivo.

En esta definición, se denotan con más claridad los procesos técnicos archivísticos que se llevan a cabo en los archivos de las organizaciones: identificación, clasificación, ordenación, descripción, evaluación de documentos (valoración, selección y disposición final) y difusión.

Una vez comprendido esto, se determina que desde la Ciencia Archivística se debe llevar a cabo la gestión documental independientemente del soporte en el cual se plasmen las evidencias y la información que se encuentra en los documentos de archivo.

En la norma UNE-ISO 15489-1:2016, se encuentran conceptos y principios para llevar a cabo la gestión documental en las organizaciones, al tiempo que facilita un abanico de buenas prácticas para lograr que esa gestión sea exitosa (AENOR, 2016).

Dentro de esta norma se define la gestión de documentos como el "área de gestión responsable de un control eficaz y sistemático de la creación, recepción, el mantenimiento, el uso y la disposición de los documentos, incluidos los procesos para capturar, mantener, en forma de documentos, la información y evidencia de las actividades y operaciones de la organización" (AENOR, 2016, p.9). A este concepto se le suma el de sistema de gestión documental,

reconocido como un "sistema de información que captura, gestiona y facilita el acceso a los documentos a lo largo del tiempo" (AENOR, 2016, p.9).

Además, se debe considerar el *sistema de gestión para los documentos*, planteado en la familia de Normas ISO 30300, y que puede ser definido como un conjunto de elementos relativos a los documentos de una organización, que se interrelacionan con el fin de establecer políticas y objetivos, y procesos para alcanzarlos (Bustelo-Ruesta, 2011, p.7).

A nivel costarricense, en el año 2014 se desarrolla la *Propuesta de un Modelo de Requisitos Archivísticos para un Sistema de Gestión de Documentos Electrónicos de Archivo (SGDEA) en Costa Rica*, en el cual se presenta a la gestión de documentos como aquellas actividades que permiten la regulación de las prácticas que se llevan a cabo por las personas al utilizar los documentos como parte de sus funciones, y que implica la regulación por medio de políticas y normas (Cedeño-Molina, Granados-Peraza, Guevara-Acon y Montero-Paniagua, 2014).

Aquí, se indica que la gestión de documentos está precedida por uno de los Principios Archivísticos fundamentales: el Ciclo de Vida de los Documentos, a través del cual se establecen las diferentes etapas por las que transcurren los documentos y que da como resultado el surgimiento del *Records Management* (Cedeño-Molina, et al, 2014).

En la teoría del Ciclo de Vida de los Documentos (Cruz-Mundet, 2011), que tuvo su origen en Estados Unidos de Norte América, se señala que los documentos tienen una vida similar a la de un organismo vivo: nace, es decir, es creado; vive: se mantiene y utiliza; y muere, al llegar a una fase de eliminación.

Por su parte, el *Records Management*, se definió como "un conjunto de técnicas y de procedimientos orientados a resolver la organización de los documentos mientras son necesarios para la conducción de las actividades y de los asuntos propios de las organizaciones, concluyendo su actividad una vez que son seleccionados para su conservación perpetua" (Cruz-Mundet, 2011, p.21).

Sin embargo, cabe destacar que existen otras propuestas teóricas o paradigmas relacionados con la gestión documental. Así, una de las propuestas más fuertes, con origen en Australia, es la del *Recordkeeping*, la cual "establece cuatro niveles de actividad archivística (captura del

documento, gestión de documentos, gestión del sistema y garantiza las evidencias esenciales) que se desarrollan en cuatro ámbitos (individual, grupo de trabajo, organización o entidad y sociedad)" (Hernández-Olivera et al., 2011, p.7).

Dentro del *Recordkeeping,* se plantea el *Records Continuum*, el cual propone abandonar la tradicional gestión de los documentos, en la que se diferenciaba en el caso de ser documentos administrativos o documentos históricos (Hernández-Olivera, Martín-González, Ríos-Hilario y Travieso-Rodríguez, 2011).

El *Records Continuum*, o continuidad de los documentos (Cruz-Mundet, 2011), puede verse como un modelo más inclusivo, en el que se señala que no deben existir etapas separadas en la vida de los documentos, sino que se trata de una continuidad, en la cual la gestión de los documentos no debería de dividirse, sino más bien debe ser aplicada como un proceso continuado.

Desde de la perspectiva de este modelo de continuidad, el autor Cruz-Mundet (2011, p.23), señala que:

> (...) la capacidad de los documentos para funcionar como instrumentos de gobernanza y responsabilidad, formar memoria, identidad y proporcionar fuentes de información de valor añadido está estrechamente relacionado con sus cualidades probatorias, su transaccionalidad y contextualidad. En esta perspectiva, los documentos no pueden ser categorizados como prueba o como memoria. Son ambas cosas. Es su naturaleza probatoria la que los distingue de otras formas de información documental, y les permite jugar su particular papel en la formación de la memoria y de la identidad.

De esta forma, se indica que es posible encontrar cuatro dimensiones en el Records Continuum, las cuáles son (Hernández-Olivera et al., 2011, p.7):

1. Los documentos se crean como parte de una actividad o transacción.
2. Los documentos se capturan en un sistema, con contexto, contenido y estructura documentados en metadatos.
3. Los documentos se organizan y se gestionan como memoria y pruebas empresariales o personales.
4. Los documentos se gestionan y pluralizan como parte de la memoria social o colectiva.

De esta forma, se evidencia que a través del tiempo la gestión de los documentos ha ido evolucionando y ajustándose a las necesidades de una realidad en constante cambio, lo cual también se debería ver reflejado a nivel costarricense.

Así por ejemplo, en el caso de la Ley 7202, Ley del Sistema Nacional de Archivos, para el año 2017 se realiza una reforma del Reglamento a la Ley del Sistema Nacional de Archivos, en el cual se establece en su artículo 1 un glosario de términos, el cual permite un mayor grado de normalización a nivel nacional en cuanto a los conceptos referentes a la materia archivística.

En dicho artículo, se indica que en Costa Rica, la gestión de documentos se refiere a "todas las funciones, actividades y procesos que en una organización se aplican a los documentos **a lo largo de su vida**[1] para garantizar su producción, su autenticad [sic], su integridad, su conservación, su fiabilidad y su disponibilidad para su mayor uso y servicio" (Poder Ejecutivo de la República de Costa Rica, 2017, p.4).

Como se puede observar en el texto anterior, en la normativa costarricense, a pesar de que se han hecho modificaciones para abordar de forma más integral la gestión de documentos, todavía existe un arraigo conceptual hacia el modelo del *Records Management*.

1.4.3. Sistemas de información electrónica

Para lograr el acercamiento necesario entre las instituciones y los usuarios, desde los archivos se trabaja para colocar a disposición de manera ágil, eficiente y eficaz, la información contenida en los documentos de archivo.

Se plantea la necesidad de utilizar mecanismos o herramientas que incorporen las TIC, de manera que el acceso a la información por parte de las personas se lleve a cabo oportunamente, por medio de sistemas de información, los cuales consisten en sistemas computacionales que facilitan el éxito de la organización a través de distintas formas de gestión de la información, incluyendo la recopilación, el procesamiento y la difusión (Mohd Zuhan & Ab Razak, 2019, p. 213).

Uno de los conceptos más utilizados es el de los Sistemas de Gestión de Documentos Electrónicos de Archivo (SGDEA), señalandolos como sistemas que permiten que se lleve a

[1] La negrita no pertenece al original

cabo la gestión de los documentos que se producen en soporte electrónico en las organizaciones (Cedeño-Molina, et al, 2014).

Castillo-Solano y Umaña-Alpízar (2018), señalan que un SGDEA:

> (...) es un sistema que captura, gestiona y provee acceso a los documentos. Su principal objetivo consiste en llevar a cabo el proceso archivístico desde la creación misma de un documento, con funcionalidades como la homologación de la apariencia y características para tipos documentales a través del empleo de plantillas predefinidas, así como el control del flujo de trabajo de un determinado proceso, tipificado para una organización, la descripción y la clasificación de documentos.

La Norma UNE-ISO 15489:2016, por su parte, también propone el concepto de sistemas o aplicaciones de gestión documental, que definen como "sistemas de información que capturan, gestionan y facilitan el acceso a los documentos a lo largo del tiempo" (AENOR, 2016, p.9).

Estos sistemas deberían aplicar los instrumentos de gestión de documentos, como por ejemplo: esquemas de metadatos, cuadros de clasificación, reglas y permisos de acceso y calendarios de conservación; llevar a cabo procesos para la creación, captura, clasificación, indización, control de acceso, almacenamiento, uso, migración y disposición de los documentos (AENOR, 2016, p.24). Así también "sustentar la creación y mantenimiento de relaciones lógicas entre el contenido de los documentos y los metadatos para la gestión de documentos" (AENOR, 2016, p.12).

Para alcanzar objetivos como la interoperabilidad con otras aplicaciones, la utilización y reutilización de documentos, la preparación ante posibles cambios tecnológicos o administrativos en las organizaciones, así como la capacidad de respuesta ante la interrupción de las actividades, los sistemas o aplicaciones de gestión documental, deben ser diseñados e implementados tomando en consideración el contexto organizacional y los requisitos de gestión de documentos que se hayan identificado (AENOR, 2016, pp.12-13).

Además de esto, se indica que los sistemas o aplicaciones de gestión documental deben contar con las siguientes características (AENOR, 2016, pp.13-14):

- Fiable: “debería funcionar de modo regular y continuado en concordancia con la política y procedimientos autorizados”. La fiabilidad se debería documentar mediante documentos con las rutinas operacionales, procedimentales y tecnológicas, así como por medio de los metadatos.
- Segura: aplicando medidas como “controles de acceso, supervisión, validación de los agentes y destrucción autorizada con la finalidad de evitar el acceso no autorizado, la modificación, el ocultamiento o la destrucción de documentos”. Demostrable mediante metadatos.
- Conforme: “deberían cumplir los requisitos derivados de la organización, de las expectativas sociales o de la comunidad y de su marco legal y regulatorio”. Requiere de evaluaciones periódicas y su respectiva documentación.
- Exhaustiva: “deberían tener la capacidad de gestionar todos los documentos requeridos para todas las actividades de la organización con las que están relacionados”.
- Sistemático: “La creación, captura y gestión de los documentos se debería sistematizar a través del diseño y el funcionamiento habitual del sistema de gestión documental, y por su adhesión a las políticas y procedimientos autorizados”.

Por su parte, los sistemas de información electrónicos se definen en la norma UNE-ISO 14641-1:2015 como el “sistema designado para recibir, preservar, acceder y transferir archivos en un formato electrónico”; y además, indica que “los sistemas de información capturarán documentos electrónicos que se han enviado para su almacenamiento y utilización a largo plazo” (AENOR, 2015-a, p. 9).

Un sistema de información electrónica debe implementar una política de archivo predefinida y las características con las que debe contar son: 1-viabilidad de la preservación a largo plazo, 2-integridad, 3-seguridad y 4-trazabilidad (AENOR, 2015-a, p. 11).

1.4.4. Gestión de la información

Existe una relación lógica entre lo que se entiende como datos, documentos e información. Por un lado, los datos se definen como “un conjunto discreto de factores objetivos sobre un hecho u objeto. Un dato no dice nada sobre el porqué de las cosas, y por sí mismo tiene poca o ninguna relevancia o propósito” (Comisión Económica para América Latina y el Caribe [CEPAL], 2020a,

párr.5). Los datos pueden ser recopilados y almacenados de forma individual o en conjunto y al ser procesados e interrelacionados, serán la base para interpretaciones más complejas de estos hechos u objetos.

Por otro lado, de forma sintética, los documentos de archivo pueden ser definidos como "el subproducto documental de las actividades que desarrolla el hombre y son conservados (...) por su valor testimonial. Un documento de archivo es un instrumento de carácter contemporáneo que es creado por individuos y organizaciones en el desarrollo de sus actividades" (International Council on Archives [ICA], 2016, párr. 1-2).

A partir de estos dos conceptos, podemos definir un elemento más amplio que los abarca como partes constituyentes: la información. Por lo tanto, la información es la interpretación de un conjunto de datos, con los cuales es posible establecer relaciones, patrones y tendencias, lo cual sirve para tomar decisiones (Rodríguez y Lamarca, 2012, p.10).

Es importante resaltar que ese conjunto de datos que constituyen la información, normalmente (aunque no siempre) se presentan en forma de documentos o algún tipo de comunicación audible o visible, entre un emisor y un receptor (CEPAL, 2020a).

De manera que, para la presente investigación, se entenderá la información como el objeto de estudio al cual se le aplicarán metodologías archivísticas y tecnológicas para su preservación a largo plazo, por medio de la puesta en marcha del Archivo Digital de la Universidad de Costa Rica, incluyendo tanto datos como documentos de archivo.

Teniendo claros estos conceptos, se puede indicar que el objetivo principal de la gestión de la información es satisfacer la demanda de información y proporcionar valor a las entidades. Este valor adquirido permite tomar decisiones adecuadas; mejorar la efectividad de los procesos; proveer información a tiempo sobre resultados; mejorar la eficacia de la institución; y preservar la memoria de la organización (Rodríguez y Lamarca, 2012, p.16).

Así, el enfoque de la gestión de la información se ajusta a la necesidad de instaurar un Archivo Digital pues (CEPAL, 2020a):

- Se orienta a la generación, coordinación, almacenamiento o preservación, búsqueda y recuperación de la información.

- Optimiza la utilidad y contribución de los recursos de información a los objetivos de la organización a través de la creación de canales y medios para transmitir y acceder a la información.
- Se dirige hacia los procesos de selección, localización, análisis, almacenamiento, búsqueda, recuperación, difusión y conservación de la información generada en la empresa u organización.

1.4.5. Repositorio digital

El término repositorio digital, ha sido utilizado por distintas agrupaciones destinadas a resguardar la memoria documental: archivos, museos, bibliotecas y comunidad científica. Por motivo de las necesidades específicas de cada agrupación, han habido diferentes enfoques en su definición y objetivos. Sin embargo, se mantiene la similitud teórica en la que los repositorios digitales son espacios en los que se gestionan los objetos digitales a largo plazo para beneficiar a los usuarios actuales y futuros (Marini, 2006, p.78-79).

Así como sucede con los SGDEA, el término de repositorio digital se centra principalmente en una plataforma o programa informático, como herramienta tecnológica para llevar a cabo una parte de la gestión de la información que contiene. Es decir, tanto los SGDEA como los repositorios tienen como fin facilitar la organización y uso de la información perteneciente a una entidad.

Desde esta perspectiva, a continuación, se presentan algunas de las definiciones de repositorios digitales y los conceptos más relevantes que se desprenden de cada una de ellas, y que pueden presentarse en común a la hora de definir un repositorio digital (Tabla 1):

Tabla 1. *Definiciones de Repositorio Digital.*

Autor	Definición de Repositorio Digital	Conceptos destacados
Sandí-Delgado y Cruz-Alvarado (2017)	"consiste en una plataforma web con una infraestructura sólida e interoperable con distintos sistemas mediante el protocolo OAI-PMH y de acceso abierto (en inglés, *open access* [OA]) que permite gestionar, almacenar, preservar, resguardar y difundir de forma digital sin restricciones que permita potenciar la visibilidad de la producción científica, académica, intelectual o de cualquier otro índole a nivel nacional e internacional" (p.4)	Plataforma web Interoperable Acceso abierto Preservar Difundir Sin restricciones

Bustos-González y Fernández-Porcel (2008)	"un archivo electrónico de la producción científica de una institución, almacenada en un formato digital, en el que se permite la búsqueda y la recuperación para su posterior uso nacional o internacional(…) contiene mecanismos para importar, identificar, almacenar, preservar, recuperar y exportar un conjunto de objetos digitales, normalmente desde un portal web. Esos objetos son descritos mediante etiquetas o metadatos que facilitan su recuperación." (p.7)	Archivo electrónico Producción científica Uso Formato digital Preservar Objetos digitales Metadatos
Clifford A. Lynch (2003)	"*A university-based institutional repository is a set of services that a university offers to the members of its community for the management and dissemination of digital materials created by the institution and its community members. It is most essentially an organizational commitment to the stewardship of these digital materials, including longterm preservation where appropriate, as well as organization and access or distribution (...) an effective institutional repository represents a collaboration among librarians, information technologists, archives and records managers, faculty, and university administrators and policymakers. At any given point in time, an institutional repository will be supported by a set of information technologies*" (p.2)	Servicios Manejo y difusión Materiales digitales Preservación a largo plazo Colaboración Tecnologías de la información
Universidad de la Plata (2019)	"es una estructura web que permite organizar, almacenar, preservar y difundir de manera abierta la producción intelectual resultante de la actividad académica e investigadora una institución" (párr. 1)	Estructura web Preservar Difundir de manera abierta Producción intelectual
Archivo General de la Nación de Colombia (2018)	"sistema informático donde se almacena la información de una organización con el fin de que sus miembros la puedan compartir (traducción definición TERMCAT). Un depósito de documentos digitales, cuyo objetivo es organizar, almacenar, preservar y difundir en modo de acceso abierto (Open Access). Archivo centralizado donde se almacenan y administran datos y documentos electrónicos y sus metadatos (definición según ENI) (p.15)	Sistema informático Documentos digitales Preservar Difundir Acceso abierto Documentos electrónicos Metadatos
Voutssas y Barnard-Amozorrutia (2014)	"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" (p.189)	Servicios Instalaciones Comunidad Diseminación Materiales digitales

Fuente: Elaboración propia a partir de bibliografía consultada. 2022.

Como puede observarse en la Tabla 1, las definiciones de repositorio digital tienen características o conceptos en común que resultan fundamentales para poder considerar un programa informático como un repositorio. Así, por ejemplo, todas las definiciones indican que se requiere de una plataforma tecnológica, en la que se pueda preservar información y que la misma pueda ser usada y difundida a largo plazo.

Otra información importante que nos revela la Tabla anterior es que en la mayoría de los casos los repositorios digitales pueden verse inmersos principalmente bajo el plano de los sistemas de

biblioteca, al indicar que su contenido se enfoca en la producción científica, académica o intelectual de acceso abierto, siendo así que hace falta más exploración desde el campo archivístico (Archivoz, 2020, párr.1):

> En la profesión archivística, por lo general los repositorios digitales son vistos como una herramienta propia del campo bibliotecario, desde esta perspectiva podemos considerar que los profesionales archiveros no han dimensionado los beneficios que abrigaría su implementación en los archivos.

Así también, Francesca Marini (2006, p.78), indica que el enfoque de la comunidad bibliotecaria hacia la definición de repositorio digital, ha sido quizás el más extendido, pero también se está haciendo mucho en los archivos.

Al observar detenidamente estas definiciones, no se ajustan a la realidad de las necesidades de un repositorio de preservación digital a largo plazo desde la especialidad de la archivística. Esto sucede, en gran medida, debido a que los documentos de archivo presentan algunas particularidades que no pueden ser cubiertas por dichas definiciones.

De esta forma, por ejemplo, no todos los documentos de archivo son de acceso abierto o público, cualidad que puede verificarse a través de instrumentos como las tablas de acceso documental o que viene determinado por la legislación vigente. Si bien la difusión y el acceso abierto son características comunes de las definiciones de los repositorios digitales, esto no responde por completo a las necesidades de protección de datos que algunos documentos de archivo requieren.

Castillo-Solano y Umaña-Alpízar (2018), indican que para contar con un repositorio en el cual se logre mantener disponible la información en la actualidad y en el futuro, es necesario que se apliquen políticas y estrategias de preservación, políticas de acceso, de metadatos y protocolos de transferencia.

De acuerdo con esto, se puede tomar como referencia la norma *UNE-ISO 16363:2017 Sistemas de transferencia de información y datos espaciales. Auditoría y certificación de repositorios digitales de confianza*, para que el repositorio de preservación digital que conformará el Archivo Digital, sea un repositorio de confianza, donde se consideren la monitorización constante, planificación y mantenimiento, las amenazas y riesgos en los sistemas, colaboración y proyecciones de presente y futuro; lo cual, por su parte, requiere de un compromiso institucional

que asegure los recursos económicos necesarios para mantener el funcionamiento a largo plazo (AENOR, 2017).

Al tratarse de perspectivas sobre apoyo y compromiso de la organización, son temas que deberán manejarse desde las políticas, ya sea de forma general en una política institucional de preservación digital o que se disponga de forma específica de una política de acceso al repositorio, pero debe ser un tema regulado desde los altos mandos jerárquicos para que su aplicación sea sostenida en el tiempo.

Así, para efectos de las necesidades observadas en esta investigación, respecto a la preservación de documentos electrónicos de archivo, se definen el repositorio de preservación digital como el sistema informático en el cual se transfieren, se almacenan, y se mantienen disponibles y usables los Paquetes de Información Archivística, que deben ser conservados a largo plazo por una organización en el ejercicio de sus funciones. Este sistema deberá ser el resultado de una política institucional que asegure la correcta planificación, gestión de riesgos y la mejora continua, capaces de garantizar el resguardo de la información durante el tiempo que resulte necesario.

Además, según la norma *UNE-ISO 17068:2020 Información y documentación. Repositorio de tercero de confianza para documentos electrónicos*, los repositorios de documentos electrónicos deben contar con las siguientes funciones (2020, p.30)

- captura, navegación y búsqueda de los documentos electrónicos;
- emisión de certificados y de documentos electrónicos;
- migración y recepción del documento electrónico;
- conversión del documento electrónico;
- control de la integridad del documento electrónico;
- disposición del documento electrónico.

Esto, sumado con las características de interoperabilidad con otros sistemas para recibir transferencias documentales, así como la adecuada gestión de los metadatos, completan los requerimientos, desde el punto de vista archivístico, del repositorio que forma parte de un Archivo Digital.

1.4.6. Archivo digital

El término Archivo Digital ha sido utilizado por diversas disciplinas, no obstante, se debe abordar un concepto que permita comprender su alcance desde la perspectiva archivística.

Considerando la palabra de origen anglosajona *archive*, un archivo digital es *"An agency or institution responsible for the preservation and communication of records selected for permanent preservation. [Archives]*" (InterPARES, 2018a). También, un archivo digital hace referencia a un lugar donde los documentos son preservados y resguardados (InterPARES, 2018a).

A lo anterior, se le debe sumar una entidad encargada de llevar a cabo dicha preservación; así, según el Glosario de Preservación Archivística Digital de Voutssas y Barnard-Amozorrutia, corresponde a una "Instancia responsable de la preservación y distribución de documentos de archivo seleccionados para su preservación permanente" (2014, p.112).

Por lo tanto, para esta investigación se define al Archivo Digital como una entidad compuesta por el conjunto de personas, políticas y plataformas o aplicaciones informáticas necesarias para llevar a cabo la preservación de los objetos digitales gestionados en la Universidad de Costa Rica. De esta manera, no se limita su definición a un aspecto meramente tecnológico ni espacial, sino a un conjunto de acciones planificadas y ajustadas a la normativa, que se llevan a cabo por un equipo interdisciplinario, para asegurar la preservación a largo plazo del fondo documental institucional.

Así también, resulta indispensable analizar qué son los sistemas de producción de documentos y los Sistema de Gestión de Documentos Electrónicos de Archivo (SGDEA), para poder compararlos con la definición de Archivo Digital. A pesar de que los tres temas están relacionados, y pueden requerirse para llegar hasta la preservación digital, deben reconocerse las diferencias entre cada uno de ellos.

En el caso de los sistemas de producción de documentos, estos hacen referencia a aquellas herramientas tecnológicas, que utilizan por ejemplo procesadores de texto, programas de digitalización, gestores de correos electrónicos, entre otros; mediante los cuales se producen documentos, flujos de trabajo, normalización de plantillas, tipos documentales, consecutivos, entre otros.

Los SGDEA son entendidos como aplicaciones tecnológicas que están basadas en conocimiento archivístico para crear y gestionar documentos de archivo en soporte electrónico. Así, la definición de *records system* brindada en la UNE-ISO 15489:2016, hace referencia a elementos técnicos de *software*, junto con elementos no técnicos, como políticas, personas, procedimientos, entre otros, que tienen como prioridad capturar, gestionar y facilitar el acceso a los documentos a lo largo del tiempo (AENOR, 2016, p.9).

Sin embargo, una diferencia fundamental con respecto al Archivo Digital está determinada por la conservación misma de los documentos. Por un lado, en el caso del SGDEA, el tiempo en el que se mantienen los documentos, depende directamente de los plazos de conservación archivísticos, llegando al proceso técnico de disposición final: la información se debe conservar (transferir) o eliminar permanentemente. Por otro lado, el Archivo Digital, al contar con la figura de un repositorio digital de confianza, permite que se conserve la información de forma indefinida, al aplicar estándares y estrategias para garantizar la integridad de dicha información, mitigando la obsolescencia tecnológica (Castillo-Solano y Umaña-Alpízar 2018, p.73).

Cabe recalcar que para poner en funcionamiento el Archivo Digital, es necesario aplicar un conjunto de aspectos estratégicos y técnicos, que permitan conservar adecuadamente cualquier información que se genere o reciba en la institución, como resultado de sus funciones. Es decir, su ámbito de aplicación debe ser lo suficientemente amplio para abordar documentos de archivo, datos u otras evidencias de información.

Las información recibida en el Archivo Digital, debe transferirse por medio de paquetes de información, definidos dentro de un entorno de archivo OAIS (en el que se profundizará más adelante) como paquetes conceptuales que incluyen tanto el Contenido de Información, es decir, el objeto a conservar, y la Información de Descripción de la Conservación, la cual permite identificar la procedencia, el contexto, los derechos de acceso, entre otras características del contenido de información, para comprender su entorno de creación y poderlo preservar a largo plazo (AENOR, 2015-b, p.31-32).

1.4.7. Preservación digital

Según el Decreto N° 40554 -C Reglamento a la Ley del Sistema Nacional de Archivos, la *preservación* junto con la restauración, componen la conservación documental, es decir, las

acciones que tienen como objetivo evitar, detener o reparar el deterioro y los daños sufridos por los documentos, de manera que puedan perdurar en el tiempo (Poder Ejecutivo, 2017). Esta conceptualización puede ser aplicada tanto para documentos en soportes analógicos como electrónicos.

No obstante, para poder abordar específicamente los documentos que se crean y conservan mediante plataformas tecnológicas, se debe definir el término de *preservación digital*. Así, InterPARES indica que la preservación digital es el proceso de mantener funcionales los objetos digitales durante el tiempo, a través de las diferentes generaciones de tecnología (InterPARES, 2018b).

Según el Archivo General de la Nación de Colombia (2018, p.11), la preservación digital se define como "el conjunto de principios, políticas, estrategias y acciones específicas que tienen como fin asegurar la estabilidad física y tecnológica de los datos, la permanencia y el acceso de la información de los documentos digitales y, proteger el contenido intelectual de los mismos por el tiempo que se considere necesario".

Cabe destacar que la preservación debe permitir la recuperación y el uso de la información de archivo a través del tiempo. Para ello, es importante que desde la ciencia archivística se logre establecer un conjunto de planteamientos teóricos, normativos y conocimientos técnicos aplicados, que aseguren la integridad de los documentos.

Al respecto, Leija-Román (2017, p.32), postula que:

> El concepto de preservación digital se compone tanto de actividades técnicas como de elementos económicos, legales y de organización que definen un amplio rango de actividades para el mantenimiento de recursos. Todos ellos actúan en un entorno de organización con la influencia de factores externos e internos cambiantes como la obsolescencia tecnológica, los sistemas financieros o marcos legales de operación.

Además, es posible diferenciar un proceso completo de preservación digital, del simple hecho de almacenar, respaldar o migrar la información, ya que según la UNESCO (s.f.):

> No puede decirse que se han conservado los objetos digitales si, al haber dejado de existir los medios de acceso a ellos, resulta imposible utilizarlos. El objetivo de la preservación de los

> objetos digitales es mantener su accesibilidad, es decir, la capacidad de tener acceso a su mensaje o propósito esencial y auténtico.

Para poder cumplir con este propósito es necesario que se desarrolle una estrategia a largo plazo que permita mantener la información electrónica de forma exacta, fiable y veraz, es decir, que pueda ser leída e interpretada correctamente por una aplicación informática; que pueda ser representada en un formato comprensible para las personas y mantener dentro de su estructura lógica y física, el contenido y el contexto que fueron evidentes al crearse o recibirse dicha información (AENOR, 2008, p.11).

De esta manera, la preservación digital sistémica de documentos de archivo puede verse como esa estrategia a largo plazo, pues es la que se lleva a cabo cuando el documento archivístico digital es mantenido auténtico desde su creación, transmisión, preservación y custodia o eliminación. Además, al aplicar la preservación sistémica, la producción del documento es confiable, es decir, bajo requisitos archivísticos que garanticen la información que contiene. Para ello, debe ser posible comprobar que los documentos siempre se mantuvieron en entornos digitales con requisitos de archivo comprobados. (Daniel Flores, 2020-b, 20m08s).

Este tipo de preservación sistémica, debe mantenerse siempre bajo una cadena de custodia, la cual garantice que los documentos no han sido alterados en ningún momento, desde su creación (sistemas de gestión, por ejemplo SGDEA) hasta su almacenamiento permanente (Archivo Digital), manteniendo una conexión entre los productores y los preservadores.

Es fundamental que, para mantener la preservación sistémica, no se debe romper la cadena de preservación, esta última definida por InterPARES (2012, p.7) como la "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". Esto se logra mediante una custodia ininterrumpida, lo que significa mantener el contexto de los documentos de archivo desde su producción hasta su preservación, como medio para asegurar su autenticidad (InterPARES, 2012, p.12).

Por consiguiente, en esta investigación se define la preservación digital como el conjunto de políticas y acciones que permiten conservar a lo largo del tiempo la información digital, creada o recibida, dentro de un ambiente tecnológico controlado con métodos archivísticos, mediante una

planificación sistemática que asegure sus características de autenticidad, fiabilidad, integridad y usabilidad, de forma ininterrumpida desde su creación hasta su disposición final, es decir, su conservación permanente o eliminación.

Es importante destacar que los rápidos cambios que se dan a nivel tecnológico, generan un inevitable estado de obsolescencia sobre los objetos digitales, aspecto que debe ser considerado a fondo para la preservación digital. La norma UNE-ISO/TR 18492:2008, define obsolescencia tecnológica como el desplazamiento de una solución técnica, como resultado de mejoras y desarrollos tecnológicos. Estos cambios (ya sean a nivel de *software* o *hardware*), pueden provocar que la información creada o almacenada dentro de sistemas informáticos sea irrecuperable (AENOR, 2008, p.7).

La obsolescencia tecnológica ha sido tratada por medio de distintas estrategias que permitan la preservación, recuperación y uso de la información (AENOR, 2008, p.8-9), para que dicha información sea:

- Legible: que la cadena de bits que comprende la información pueda ser accesible por un sistema o dispositivo tecnológico (ya sea, el que lo creó, el que lo almacena, el que lo accede o el que lo utilizará para almacenar en el futuro).
- Inteligible: es la capacidad de un programa informático para interpretar lo que la cadena de un objeto digital representa, de manera que se pueda visualizar la información.
- Identificable: facilita la búsqueda y recuperación de la información, al brindar atributos únicos para los objetos digitales, como nombres o números de identificación, es decir, identificadores únicos.
- Recuperable: permite la ubicación física donde la información se encuentra ubicada, en el dispositivo de almacenamiento. Este aspecto es fundamental porque los desarrollos de *software* pueden causar que solo los sistemas solo soporten algunos formatos de documentos, mientras que otros soportan varios formatos.

Así, para llevar a cabo una preservación digital eficiente y eficaz, dentro de la planificación estratégica y políticas de preservación, se deben considerar el rápido cambio tecnológico y la fragilidad de los soportes digitales, que implica dificultades como la obsolescencia. En este sentido, el Archivo Digital debe realizarse mediante las características descritas para OAIS, en la

UNE-ISO 14721, de manera que se promueva una mayor normalización en la gestión de documentos y la correcta preservación a largo plazo de la información.

Además de esto, se deben tomar en consideración otras cualidades como lo son las Propiedades Significativas de los objetos digitales. Estas propiedades se definen como "las características de un objeto que deben mantenerse a través de las acciones de preservación" (Caplan, 2009, p.7).

Por su parte, dentro del proyecto InSPECT (por sus siglas en inglés *Investigating the Significant Properties of Electronic Content over Time*), define las propiedades significativas como "*The characteristics of digital objects that must be preserved over time in order to ensure the continued accessibility, usability, and meaning of the objects, and their capacity to be accepted as evidence of what they purport to record*" (Grace, 2009, p.3).

El autor Arribas-del Pozo (2019), señala que dentro del proyecto InSPECT, las propiedades significativas son clasificadas en cinco categorías (pp.69-70):

- **Contenido**: expresión de la información, no necesariamente de forma legible (texto, imágenes, entre otros). Otros ejemplos pueden ser la duración, el número de caracteres, entre otros.
- **Contexto**: la información que permite la comprensión del entorno tecnológico y administrativo con el que el objeto se relaciona, así como su procedencia (autor, fecha, entre otros).
- **Apariencia**: la forma en que el contenido se visualiza ante el usuario (fuentes, colores, entre otros).
- **Estructura**: la organización de las partes que componen el objeto y la forma en la que se relacionan una con otras (cabeceras, paginación, entre otros).
- **Comportamiento**: las funciones propias del objeto, como los enlaces hipertextuales, las fechas actualizables (entre otros).

De esta forma, cuando existen riesgos de obsolescencia tecnológica, y se toman acciones para contrarrestar sus efectos (como lo son por ejemplo los procesos de migración), se debe realizar un análisis previo de las propiedades significativas de los objetos digitales, con el fin de mantenerlas a lo largo del tiempo, ya que "si un documento no conserva intactas sus propiedades

significativas, se pueden ver afectadas condiciones como la calidad, disponibilidad y su representación visual" (Castillo-Solano y Umaña-Alpízar 2018, p.81).

1.4.8. Preservación Digital Sistémica y la Cadena de Custodia Digital Archivística

El objetivo de la preservación digital es asegurar que la información se mantenga íntegra, fiable, disponible y auténtica, durante todo el tiempo que sea requerida, según su plazo de conservación. Para cumplir con este propósito, es necesario que se realice la Preservación Digital Sistémica (PDS), es decir, preservación basada en métodos ordenados y estructurados a partir de lo definido en una Política de Preservación Digital.

La información se debe transferir y procesar con base en normas y modelos aceptados y utilizados ampliamente a nivel mundial, permitiendo el intercambio de conocimiento y la normalización de los procesos, al tiempo que se asegura el éxito en su utilización.

Por esta razón, la información debe ser gestionada por medio de paquetes archivísticos OAIS (SIP, AIP, DIP), por medio del procesamiento automatizado utilizando sistemas basados en requisitos de archivo (Flores, 2020-a, párr.10).

La aplicación de la PDS asegura que se cumpla con la Cadena de Custodia Digital Archivística (CCDA), lo que implica que haya un monitoreo ininterrumpido en la gestión de la información desde su creación hasta su eliminación o conservación permanente. Esto significa que existe una custodia de los objetos digitales en entornos tecnológicos seguros que cumplan con requisitos archivísticos aprobados, desde su producción (en sistemas transaccionales y en SGDEA), almacenamiento, acceso y hasta su disposición final.

Por lo tanto, asegurar la CCDA permite a los encargados del Archivo Digital demostrar la trazabilidad de la información, según la sucesión de las personas jurídicas que han tenido bajo su responsabilidad la custodia de dicha información, garantizando la "Autenticidad, Fiabilidad, Integridad y Fijabilidad con el tiempo, en un enfoque de Preservación Digital Sistémica" (Flores, 2020-a, párr.8).

Resulta importante destacar que existe una ruptura de la Cadena de Custodia cuando los objetos digitales son extraídos de los ambientes controlados en los que se produjeron, sin que se haya realizado de forma segura y directa a un repositorio digital como lo es el Archivo Digital. De esta

forma, según Daniel Flores (2020-a, párr. 4), por ejemplo, al descargar los documentos a un disco duro externo, se rompe la garantía de autenticidad y confiabilidad de los documentos, abriéndose la posibilidad de que se presenten adulteraciones digitales.

Otro término importante es el de *Preservación Digital Pasiva No Sistémica* la cual hace referencia a "todas aquellas colecciones y transferencias de documentos analógicos que ya hemos producido o acumulado, de representantes digitales, resultado de digitalizaciones y nacidos digitales que aún no han implementado una Preservación Digital Activa o Sistémica" (Flores, 2020-a, párr. 9).

Así, por ejemplo, se da el caso de los documentos que nacen en soporte físico y que son digitalizados, pero que aún no han sido ingresados a un sistema informático ni a un Archivo Digital, por lo cual no se pueden probar con certeza los cambios o propietarios que han tenido los objetos digitalizados.

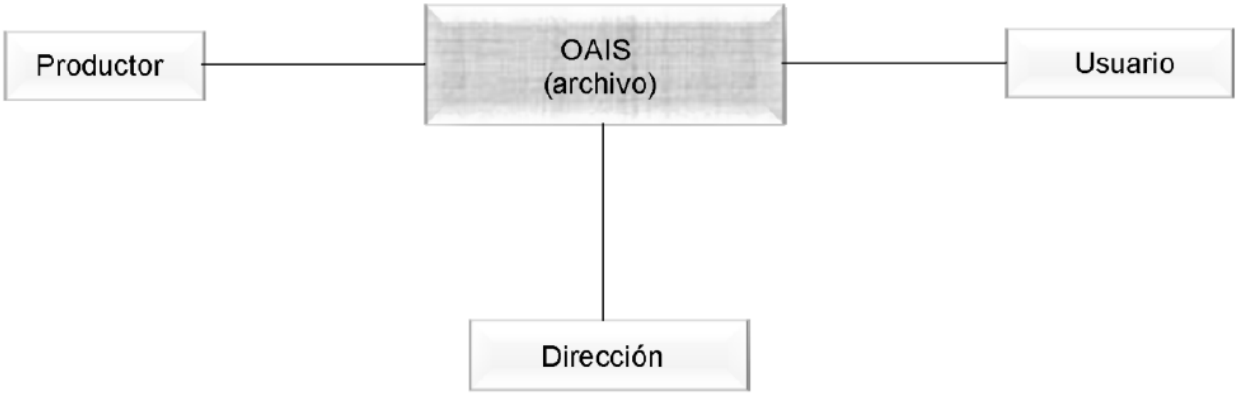
1.4.9. OAIS

El Sistema Abierto de Información de Archivo (OAIS, por sus siglas en inglés), presenta un modelo aplicable para la conservación a largo plazo de información en soporte electrónico. Cuando se hace referencia al término *largo plazo*, se entenderá como un periodo de tiempo "lo suficientemente amplio para estar afectado por los impactos de los cambios tecnológicos, que incluyen la adaptación a nuevos soportes y formatos de datos, o a los cambios en una comunidad de usuarios. A Largo Plazo se puede extender indefinidamente" (AENOR, 2015-b, p.14).

El modelo OAIS está dirigido principalmente a organizaciones que tienen la responsabilidad de resguardar información a largo plazo. No obstante, también puede ser aplicado por organizaciones que generan dicha información o que requieran acceder a esta. (AENOR, 2015, p.15).

Cabe resaltar que el OAIS es quién lleva a cabo las funciones de Archivo (en general el ingreso, administración y facilitación de la información conservada), y el funcionamiento diario del sistema, por medio de entidades funcionales. No obstante, existen tres actores fuera del OAIS que resultan de suma importancia, como se muestra a continuación:

Figura 2. *Entorno de un Archivo OAIS.*

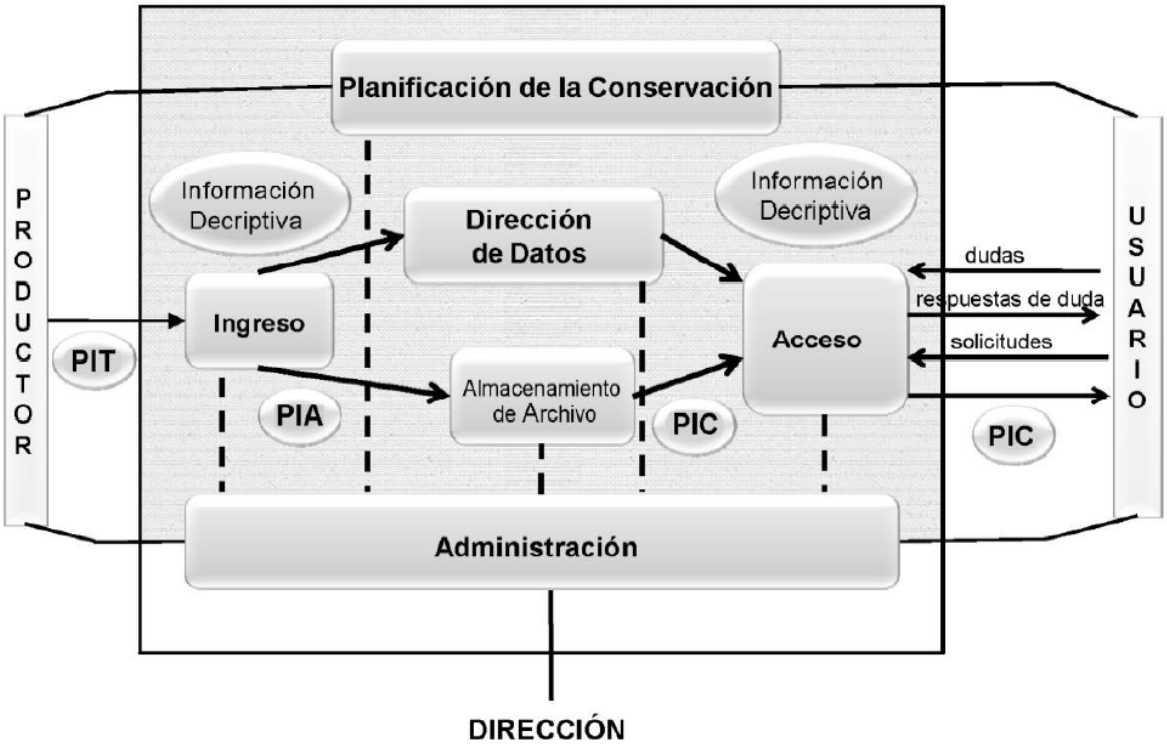


Fuente: AENOR, 2015-b, p.29.

A partir de la figura anterior, el Productor representa a las personas o clientes que brindan información que debe ser conservada. La Dirección, es el papel que se desempeña para establecer la política general de OAIS. Esta instancia no es quién se encarga de ejercer las operaciones de Archivo, día a día, en el sistema; más bien, se encarga de la financiación del OAIS, la revisión y evaluación del progreso del proyecto, resolución de conflictos entre productores, usuarios y administradores del OAIS, entre otras. Y el Usuario son las personas que interactúan con el OAIS para acceder a la información conservada (AENOR, 2015, p.34).

El modelo funcional de OAIS (figura 3) presenta el desglose de las 6 Entidades Funcionales que administran el sistema, además de mostrar los paquetes de información por medio de los cuales se recibe, se administra y se facilita la información conservada:

Figura 3. *Modelo Funcional de OAIS.*



Fuente: AENOR, 2015-b, p.41.

Dentro del modelo OAIS, la información se transmite mediante tres tipos de paquetes de información:

a. SIP (Paquete de Información de Transferencia - PIT): mediante este paquete, el productor envía la información al OAIS. El formato y contenido detallado deben definirse entre el productor y el OAIS.
b. AIP (Paquete de Información de Archivo - PIA): los SIP que ingresan al OAIS son transformados en AIP, de manera que puedan ser administrados dentro del sistema.
c. DIP (Paquete de Información de Consulta - PIC): cuando el usuario solicita información conservada en el OAIS, se le brinda a través del DIP, los cuales deben lograr ser interpretables por el usuario.

La transferencia de los paquetes archivísticos SIP desde los sistemas donde se originan los documentos, es decir, desde los sistemas transaccionales o desde los SGDEA, hacia el Archivo Digital para su preservación, se puede realizar por medio de los métodos *pull* o *push.*

Por un lado, el método de transferencia *pull*, está basado en el paradigma de la solicitud-respuesta (*data polling*), en el cual el Archivo Digital envía una solicitud al sistema productor y este último responde enviando la información de forma sincrónica o asincrónica. En otras palabras, el Archivo Digital "recoge" (*pull*) la información desde el sistema productor (Martin-Flatin, 1998, p.5).

Según Serra-Serra (2013c, p.6), este tipo de transferencia conecta al sistema de información transferente con el Archivo Digital. El sistema transferente genera automáticamente el SIP y el Archivo Digital también lo recibe de forma automática.

Por otro lado, el método de transferencia *push*, se basa en el paradigma de publicar-suscribir-distribuir, por medio del cual el sistema productor genera los paquetes de información y "empuja" (*push*), es decir, los transfiere al Archivo Digital (Martin-Flatin, 1998, p.5).

En este caso, la transferencia tiene intermediación humana y está enfocada principalmente a documentos y datos que se crean mediante herramientas de oficina o que se almacenan en red local o sistemas de ficheros. Para ello, el Archivo Digital debe proveer una aplicación para que el usuario transferente genere los SIP y los envíe al Archivo Digital (Serra-Serra, 2013c, p.6).

Como se ha notado, debe existir una relación estrecha entre el OAIS y los 3 agentes externos que participan del proceso de conservación de la información (figura 2). Cada parte del proceso debe planificarse desde el punto de vista archivístico y tecnológico, de manera que se puedan conservar tanto los objetos digitales como los metadatos que los describen, logrando asegurar el contenido, contexto y la estructura de los documentos.

1.4.10. Metadatos

La gestión de documentos está ligada intrínsecamente a la gestión de metadatos, los cuales permiten crear, registrar, clasificar, acceder, conservar y disponer de los documentos de archivo a lo largo del tiempo.

InterPARES (2013, p.11) define los metadatos como cualquier información que caracteriza a otro recurso de información, para documentar, describir, preservar o administrar ese recurso, describiendo la estructura, el contexto y los sistemas en los que existen.

Los metadatos tienen impacto desde la perspectiva archivística y tecnológica. En el primer caso, facilitan la correcta gestión de los documentos, con lo cual se puede asegurar que la información sea auténtica, fiable, disponible e íntegra (AENOR, 2018, p.6). Además, permiten que se mejore la recuperación y acceso de la información, al tiempo que se garantiza el valor probatorio de los documentos. En el segundo caso, permiten la identificación de los entornos tecnológicos en los que se crean y mantienen los documentos. También hacen posible los procesos como la migración exitosa y eficiente de los documentos electrónicos y la implementación de procesos de preservación digital, fundamental para llevar a cabo un Archivo Digital (AENOR, 2018, pp.6-7).

Por ello, los metadatos se convierten en elementos indispensables a la hora de gestionar documentos electrónicos de archivo, a través de la implementación de Archivos Digitales, ya que permiten "a los organismos e instituciones de las administraciones públicas identificar autenticar, describir, localizar y gestionar sus documentos electrónicos de manera sistemática y consistente para cumplir sus fines, permitir la rendición de cuentas, y conservar sus archivos" (García-Morales, 2013, p.62).

Así, los metadatos permiten caracterizar otras fuentes de información para documentar, describir, preservar y gestionar dichas fuentes (InterPARES, 2018b, p.33), permitiendo que exista un mejor control sobre los documentos de archivo.

La UNE-ISO 15489:2016 (AENOR, 2016, p.12), indica que los metadatos deberían representar el contexto de la organización; las dependencias y relaciones entre los documentos y las aplicaciones de gestión documental; las relaciones con el contexto legal y social; y las relaciones con los agentes que crean, gestionan y usan los documentos.

También, los metadatos se convierten en los elementos para probar la existencia y los cambios realizados a los documentos de la organización. Es a través de estos que se puede realizar la trazabilidad de la información y los agentes que participan en la gestión de documentos. Por lo tanto, debe existir un estricto control en el uso de los metadatos, de manera que se protejan contra la pérdida o eliminación no autorizada. Además, se deben establecer reglas de accesos

autorizados para controlar quiénes pueden ver, modificar o eliminar metadatos específicos (AENOR, 2016, p.12).

Los metadatos tienen un papel indispensable en los procesos de preservación digital, al punto que en el Diccionario de Datos PREMIS, se determina que existen metadatos fundamentales que constituyen 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" (Biblioteca Nacional de España, s.f., p.10).

Además, los metadatos, se pueden clasificar según su uso (CEPAL, 2020b), en:

a. Metadatos descriptivos: que sirven para encontrar, recuperar o entender un recurso de información.
b. Metadatos administrativos: son metadatos técnicos, de preservación y de derechos, los cuales se utilizan para decodificar y renderizar archivos, para la gestión de archivos a largo plazo y para hacer efectivos derechos de propiedad intelectual adjuntos al contenido
c. Metadatos estructurales: describe relaciones entre las partes de un conjunto de datos.

Para que los metadatos puedan ser utilizados de forma efectiva, deben ser agrupados mediante estructuras lógicas, es decir, esquemas de metadatos, los cuales posibilitan que existan sintaxis formales y definiciones estandarizadas (InterPARES, 2018b, p.33).

Según Woodley (2005), los esquemas de metadatos son especificaciones procesables que definen la estructura y la sintaxis de elementos digitales por medio de un lenguaje formal, es decir, por medio de un esquema de codificación, basado en reglas que normalizan los términos para una comunidad de usuarios.

Los esquemas de metadatos deben ser adaptados a las necesidades de información de cada entidad, ya que a través de estos se determina "qué metadatos se usan para identificar, describir y gestionar procesos de gestión de documentos" (AENOR, 2016, p.12).

Es fundamental resaltar que los esquemas de metadatos que se utilicen, deben estar dirigidos y planificados para facilitar la interoperabilidad entre aplicaciones informáticas existentes. Este aspecto cobra gran importancia en el caso de los esquemas utilizados en un Archivo Digital, ya

que se necesita estandarizar la información que será transferida al Archivo, para que pueda ser recibida, procesada y facilitada a los usuarios, cuando así lo requieran: "Los esquemas de metadatos para la gestión de documentos se deberían expresar en formatos que permitan la interoperabilidad entre aplicaciones, compartir información, y los procesos de migración y transferencia." (AENOR, 2016, p.22).

Así, existen esquemas de metadatos internacionalmente conocidos y utilizados, que ayudan a la interoperabilidad y el intercambio de la información. Cada uno de estos esquemas tienen una estructura lógica y una sintaxis específica para poder describir los distintos elementos que conforman un objeto digital.

Cabe destacar que algunos de estos esquemas de metadatos se han desarrollado con base en normas archivísticas internacionales, lo que permite su aplicación de forma normalizada en procesos de preservación digital.

Entre estos se tiene el DACS (Describing Archives): es la adaptación para Estados Unidos de América de los estándares de descripción archivística ISAD-G e ISAAR (CPF). Permite la descripción multinivel de los objetos digitales y es aplicable a todos los formatos (InterPARES, 2013).

También se cuenta con otro grupo de esquemas de metadatos que han sido adaptados a partir de normas internacionales de descripción archivística, que posibilitan el intercambio y procesamiento de información a través de ficheros XML.

La primera es la EAD (*Encoded Archival Description*): se usa específicamente para descripciones archivísticas pues se encuentra basada en la norma ISAD (G) y permite realizar la descripción multinivel de los objetos digitales, es decir, fondos, subfondos, series, subseries, etc., mediante la descomposición de grupos y subgrupos (Ministerio de Cultura y Deporte - Gobierno de España, s.f.).

La segunda es la EAC (*Encoded Archival Context*): es una adaptación de la norma ISAAR (CPF) y es utilizada para reflejar los registros de autoridad (Ministerio de Cultura y Deporte - Gobierno de España, s.f.).

En tercer lugar, se encuentra la EAG (*Encoded Archival Guide*): su función es llevar a cabo el intercambio de información general de los centros de custodia de documentación, al derivar de la norma ISDIAH (Ministerio de Cultura y Deporte - Gobierno de España, s.f.). .

Y en cuarto lugar, se encuentra el esquema llamado MIX (NISO Metadata for Images in XML - NISO MIX): este estándar es dirigido a establecer metadatos para procesar imágenes ráster o mapas de bits, en otras palabras, va dirigido a imágenes fijas como las captadas por cámaras de fotografía o escáneres, por lo cual no se incluyen imágenes vectoriales, ráster animadas o videos (National Information Standards Organization [NISO], 2017, p.1).

1.4.11. METS

Metadata Encoding and Transmission Standard (METS), es un estándar de estructura informática para codificar metadatos descriptivos, administrativos y estructurales, mediante el lenguaje XML. El objetivo de METS es facilitar la transferencia de objetos digitales entre distintos depósitos.

La estructura de un documento METS está compuesta por 7 secciones (Library of Congress, 2016):

1. Cabecera METS (METS Header): su etiqueta tiene la siguiente estructura <metsHdr>. Los datos que contiene describen al mismo documento METS, indicando la fecha en que se creó, la última fecha en que se modificó y su estado. Además, se puede registrar el nombre de alguno de uno o más agentes que participó en la creación del documento METS.
2. Metadatos descriptivos: su etiqueta es <dmdSec>. Tiene un elemento de identificación ID que resulta ser un identificador único para cada elemento en el documento METS.

   Estos metadatos pueden ser externos o internos al documento METS. Y describen los objetos digitales que se quieren procesar o preservar, por ejemplo, título, creador, fecha, tipo documental, etc.

3. Metadatos Administrativos: su etiqueta se define <amdSec>. También pueden ser internos o externos al documento METS. Brindan información sobre cómo se crearon y almacenaron los archivos que conforman el objeto digital, derechos de propiedad

intelectual, metadatos del documento original a partir del cual se obtuvo la representación del objeto digital y su procedencia (copias maestras, derivaciones, migraciones o transformaciones).

4. Sección Archivo: su etiqueta es <fileSec>, compuesto por uno <fileGrp>, por cada versión del objeto digital, por ejemplo, para copias maestras, para la versión PDF, etc.
5. Mapa Estructural: se define con <structMap>, el cual permite que el usuario pueda navegar a través del objeto digital y resulta fundamental cuando se trata de objetos digitales extensos como una revista. Define una estructura jerárquica del objeto y cada una de sus secciones.
6. Enlaces Estructurales: se etiqueta como <smLink>. Es la estructura más sencilla del documento METS y sirve para registrar hiperenlaces entre las distintas partes del mapa estructural.
7. Comportamientos: Asocia comportamientos ejecutables al contenido de un documento METS. Se define con la etiqueta <METS:behavior>.

METS resulta muy importante para la preservación digital porque permite llevar a cabo la gestión de los objetos digitales y facilitar el intercambio de estos entre repositorios y entre repositorios y usuarios. Además, un documento METS tiene la posibilidad de utilizarse como los paquetes de información archivística planteados por el modelo OAIS, es decir, paquetes SIP, DIP y AIP.

1.4.12. PREMIS

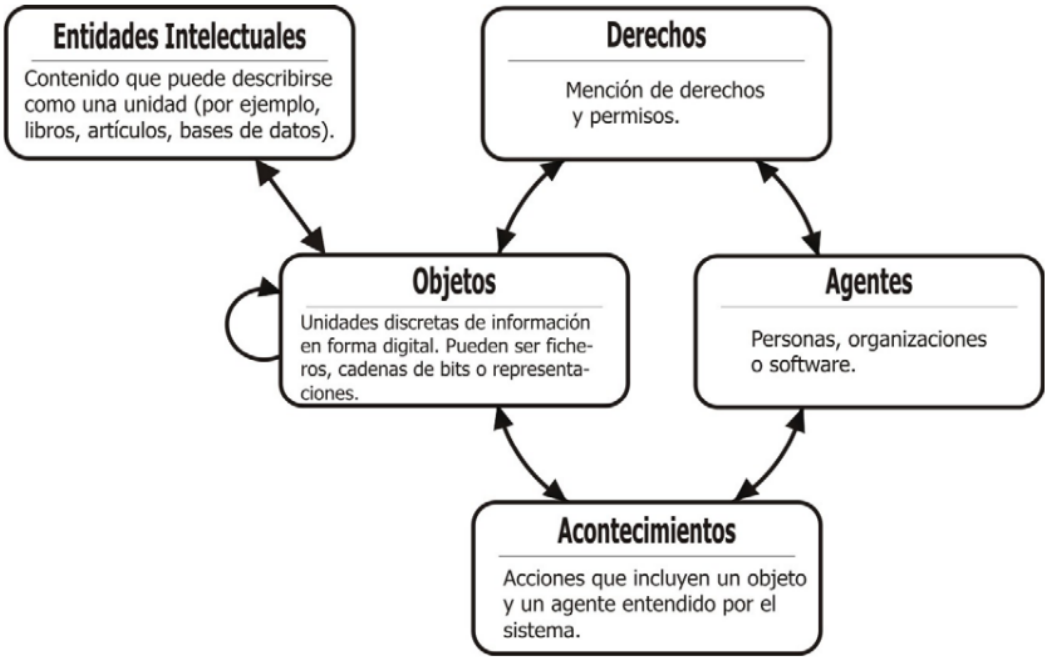
El diccionario de datos PREMIS para metadatos de preservación, se plantea como un recurso práctico para la implementación de metadatos de preservación en sistemas de Archivo Digital. El objetivo de utilizar este diccionario es incluir (Caplan, 2009, p.4-5):

> acciones que garanticen que los objetos digitales permanezcan viables (es decir, que los soportes se puedan leer) y recuperables (es decir, que puedan visualizarse, ejecutarse o representarse de alguna manera por una aplicación de software) y que aseguren que los objetos digitales del repositorio no se han alterado inadvertidamente y que se han documentado los cambios legítimos de los objetos.

Está constituido como un modelo compuesto por cinco entidades: entidades intelectuales, objetos, eventos o acontecimientos, agente y derechos. (PREMIS Editorial Committee, 2015, p.11).

A continuación (figura 4), se presenta la estructura básica que representa las entidades que conforman el modelo PREMIS:

Figura 4. *Representación de las Entidades del Diccionario de Datos PREMIS.*



Fuente: Caplan, 2009, p.10.

Cada una de estas entidades tiene propiedades conocidas como unidades semánticas, las cuales pueden 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»." (PREMIS Editorial Committee, 2015, p.12).

Regularmente, cada entidad tiene sus propias unidades semánticas, sin embargo, en algunos casos estas unidades pueden pertenecer a más de una entidad. De ahí que en la figura 4, las flechas designan las distintas relaciones que pueden darse entre cada entidad (PREMIS Editorial Committee, 2015, p.12).

Otra característica importante es que, en algunos casos, las unidades semánticas pueden utilizarse como *contenedor*, agrupando varias unidades semánticas. Estas subunidades agrupadas son conocidas como componentes semánticos del contenedor (PREMIS Editorial Committee, 2015, p.13).

1.5. Objetivos

1.5.1. Objetivo General

Proponer un modelo de preservación digital sistémica para el desarrollo de un Archivo Digital que permita la conservación a mediano y largo plazo de la información producida y recibida por la Universidad de Costa Rica.

1.5.1.1. Objetivos Específicos

- Evaluar el estado actual de la preservación digital de la información generada y recibida por la Universidad de Costa Rica, mediante la aplicación de un diagnóstico, que permita determinar su situación archivística, normativa y tecnológica.
- Definir las estrategias de preservación digital y los requisitos del modelo funcional y modelo tecnológico para el desarrollo de un Archivo Digital en la Universidad de Costa Rica.

1.6. Metodología

1.6.1. Tipo de investigación

Se determina que parte de esta investigación será de tipo descriptiva, ya que se pretende detallar la situación actual en cuanto a la preservación digital de los documentos producidos en la Universidad de Costa Rica. Al respecto, Hernández-Sampieri (2014, p.92), indica que este tipo de investigación consiste en describir fenómenos y contextos, para detallar cómo son y cómo se manifiestan. La preservación digital implica interdisciplinariedad, por lo tanto, la investigación descriptiva permitirá abordar los distintos aspectos desde el punto de vista archivístico, legal y tecnológico.

Sumado a ello, se trata de una investigación aplicada, porque busca resolver un problema, a través de la aplicación de los conocimientos obtenidos (Arango-Quintero, 2012, como se citó en

Chávez-Abad, 2015) porque se propondrá un modelo de preservación digital, como respuesta a la necesidad de la Universidad de Costa Rica de mantener las características de autenticidad, integridad, fiabilidad y disponibilidad de la información a largo plazo.

1.6.2. Enfoque de la investigación

Se aplicará un enfoque cualitativo de investigación, ya que éste "utiliza la recolección y análisis de los datos para afinar las preguntas de investigación o revelar nuevas interrogantes en el proceso de interpretación" (Hernández-Sampieri, 2014, p.7).

Al utilizar el enfoque cualitativo de investigación (Bernal-Torres, 2010), lo que se pretende es entender una situación como un todo, en este caso sobre la preservación digital a mediano y largo plazo, tomando en cuenta sus propiedades y su dinámica, basándose en la información obtenida de la población puntual que se estudia.

Siguiendo este enfoque, una vez se recolectan los datos, se requiere de un análisis a profundidad de las condiciones de preservación digital de los documentos electrónicos producidos por la UCR, con una perspectiva cualitativa, es decir, que permita la descripción de actividades y medios, que no necesariamente se pueden medir de manera numérica.

Según Hernández-Sampieri, en este tipo de enfoque se pueden desarrollar la hipótesis y las preguntas "antes, durante o después de la recolección y el análisis de los datos" (2014, p.7). Además, el mismo autor señala que "las investigaciones cualitativas se basan más en una lógica y proceso inductivo (explorar y describir, y luego generar perspectivas teóricas). Van de lo particular a lo general" (2014, p.8).

A partir del método cualitativo, se espera analizar cómo se llevan a cabo los procesos de gestión documental de las series documentales que se generan en las distintas unidades de la UCR, para luego determinar los requerimientos funcionales y tecnológicos con los cuales se debe contar para lograr una verdadera preservación digital sistémica en la institución.

Aunado a esto, la selección de la muestra en un proceso de investigación utilizando el enfoque cualitativo, "depende de que comprendamos el fenómeno bajo estudio (casos suficientes)" y "se determina de acuerdo con el contexto y necesidades" (Hernández-Sampieri, 2014, p.15). De esta

forma, utilizando este enfoque de investigación, la muestra a utilizar se determinará basado en las necesidades de la UCR en cuanto al tema de preservación digital sistémica.

1.6.3. Modalidad del Trabajo Final de Graduación

Para la elaboración del presente Trabajo Final de Graduación, se propone la modalidad de Proyecto de Graduación; el cual, según el artículo 7, del Reglamento General de los Trabajos Finales de Graduación en grado para la Universidad de Costa Rica (Consejo Universitario, 2020, p.2): "Es una actividad científica y profesional de carácter teórico-práctico, dirigida al diagnóstico de un problema que se presente en el entorno de la realidad nacional, su análisis, la determinación de los medios apropiados para atenderlo y su eventual solución."

De esta forma, se pretende realizar un diagnóstico inicial de la situación en cuanto a la preservación digital de la información que se genera y utiliza a raíz de las funciones que desarrolla la Universidad de Costa Rica, dando paso a la generación de un modelo de preservación digital sistémica que permita la implementación de un Archivo Digital para esta institución de educación superior.

1.6.4. Población

La población está constituida por todos los sistemas informáticos que producen y/o gestionan datos y documentos electrónicos en la Universidad de Costa Rica, puesto que dicha información debe ser preservada a largo plazo, asegurando su integridad, autenticidad, fiabilidad y disponibilidad.

1.6.4.1. Muestra

Se utilizará una muestra no probabilística, delimitada a un sistema informático y una serie documental que se encuentra fuera de un sistema, con el fin de aplicar los métodos *pull* y *push* para la transferencia de paquetes de información SIP hacia el Archivo Digital, planteados en el modelo OAIS, así como las clases documentales textual e imagen fija:

- Sistema de Gestión de Documentos Institucional (SiGeDI): método *pull*, aplicado a la clase documental textual.

- Colección fotográfica de la Unidad de Programas Deportivos, Recreativos y Artísticos (UPDRA): método *push*, aplicado a clase documental de imágenes fijas.

1.6.5. Técnicas de recolección de datos

Con el fin de resolver el problema de investigación, se requiere del uso de técnicas e instrumentos de recolección de datos para recabar información oportuna y pertinente, que permita realizar un diagnóstico verídico, por medio del cual se logre la construcción de herramientas valiosas para contribuir a mejorar la situación problemática presentada.

Cabe destacar que los instrumentos que se desarrollen para llevar a cabo la recolección de datos, deberán realizarse específicamente para los distintos colaboradores con la investigación, de acuerdo con sus funciones, puesto, nivel académico, entre otros aspectos que resulten relevantes.

A continuación, se propone la utilización de dos principales técnicas de recolección de datos:

a) Análisis documental y bibliográfico

Se realizará el análisis de fuentes documentales que incluye la revisión de fuentes bibliográficas, de forma que se pueda abordar la temática en estudio, esto principalmente consultando libros, artículos de revistas científicas, literatura gris, entre otros. Al tratarse de un tema de reciente tratamiento en Costa Rica, la revisión de la bibliografía internacional también resulta de gran importancia.

A esto se le suma el análisis de normativa vinculante atinente a la Universidad de Costa Rica. Además, se podrán consultar documentos de archivo que puedan aportar información importante sobre las decisiones y acciones que se han tomado en la UCR para tratar el tema de la preservación digital a mediano y largo plazo.

b) Encuesta

De esta forma, se pretende implementar cuestionarios para obtener información sobre la situación de la información electrónica generada por las unidades académicas, administrativas y de investigación de la UCR, así como las medidas de preservación digital de los sistemas en los que se genera dicha información.

c) Entrevista

Se aplicarán para profundizar en el tema de la preservación digital con base en la opinión de expertos en materia archivística y tecnológica a través del desarrollo de instrumentos estructurados.

1.6.6. Fuentes de información

Según la procedencia y el origen de la información, se plantea la utilización de fuentes documentales y bibliográficas:

- Fuentes documentales: dentro de estas, destacan los documentos producidos y custodiados a través de los archivos que conforman el Sistema de Archivos Universitarios.
- Fuentes bibliográficas: artículos de revistas, libros, literatura gris, manuales, entre otras.

Además, se propone la utilización de las fuentes, según el grado de información, primarias y secundarias:

- Fuentes primarias: se utilizarán libros, manuales, monografías, literatura gris, publicaciones periódicas, compilaciones y legislación, que se relacionen con la gestión documental y, específicamente, con la preservación documental y archivos digitales.
- Fuentes secundarias: En este caso se utilizarán catálogos en línea (por ejemplo, el OPAC de la UCR), bases de datos de texto completo como el Sistema Nacional de Legislación Vigente (SINALEVI) y las del Sistema de Bibliotecas, Documentación e Información (SIBDI).

Finalmente, para lograr tener acceso a algunas las fuentes de información se utilizarán los siguientes servicios:

- Biblioteca Carlos Monge Alfaro, Universidad de Costa Rica.
- Biblioteca Luis Demetrio Tinoco, Universidad de Costa Rica.
- Recursos electrónicos disponibles.

2. Estado actual de la preservación digital de la información generada por la Universidad de Costa Rica

La gestión de la información organizacional, es un pilar fundamental en el cumplimiento del derecho humano de acceso a la información. Sin embargo, no basta con un simple "almacenamiento", sino que se trata de garantizar a los ciudadanos que requieren que los datos, documentos de archivo y otra evidencias de información, que los mismos se van a mantener disponibles, usables, íntegros y auténticos a lo largo de todo el tiempo sean requeridos.

La Universidad de Costa Rica, como la principal institución de educación superior costarricense, posee una amplitud organizacional y una diversidad de funciones desarrolladas, que representan un verdadero reto para lograr cumplir con esa gestión y, por lo tanto, con la preservación a largo plazo de información.

De esta manera, a continuación se realiza el diagnóstico del estado de la preservación digital de la UCR, enfocado en tres escenarios principales: organizativo, archivístico y tecnológico, como un recorrido por las responsabilidades y los principales actores que deben verse involucrados en un proceso para mantener la información institucional preservada a lo largo del tiempo.

Conocer el contexto actual de la preservación digital en la Universidad, permite identificar las necesidades archivísticas y tecnológicas existentes, con el fin de tomar acciones acertadas para asegurar la preservación y uso de la información institucional. Por lo tanto, se lleva a cabo una evaluación de riesgos para la preservación digital de la información.

Además de esto, se presenta un análisis de herramientas tecnológicas que ofrece el mercado, como parte de un acercamiento inicial a las posibles soluciones que puede tomar la UCR para responder a sus necesidades de preservación digital de la información.

2.1. Análisis del escenario organizativo

2.1.1. Organización administrativa

La Universidad de Costa Rica es una institución docente y de cultura superior, creada en 1940 mediante la *Ley N° 362 Ley Orgánica de la Universidad de Costa Rica*, la cual en su artículo 1 indica que su misión será la de "cultivar las ciencias, las letras y las bellas artes, difundir su

conocimiento y preparar para el ejercicio de las Profesiones liberales" (Asamblea Legislativa, 1940, p.1).

En el Estatuto Orgánico, la UCR se define como "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" (Consejo Universitario, 1974, p.1)

Para cumplir con su misión, la UCR cuenta con 12 sedes y recintos universitarios. Como institución docente, en los niveles de pregrado y grado ofrece 12 diplomados, 195 bachilleratos y 176 licenciaturas, mientras que a nivel de posgrado cuenta con 76 especialidades, 91 maestrías profesionales, 81 maestrías académicas y 12 doctorados, esto a través de 13 facultades conformadas por 46 escuelas. En el campo de la investigación, cuenta con 34 centros, 13 institutos y un programa, así como 2 estaciones experimentales, 18 fincas, reservas y jardines, 6 museos, 4 unidades especiales y 1 planetario (Universidad de Costa Rica, 2020).

Respecto a la estructura interna de la UCR, en el artículo 7 del Estatuto Orgánico (Consejo Universitario, 1974), se indica que se encuentra regida por los siguientes órganos y representantes: la Asamblea Universitaria, el Consejo Universitario, el Rector y los Vicerrectores. Esta organización, se representa en el Organigrama Institucional de la siguiente manera (Universidad de Costa Rica, 2016):

1. **Asamblea Universitaria**: es el organismo de más alta jerarquía de la Universidad, en el cual reside la máxima autoridad de la Institución. Se divide en Asamblea Plebiscitaria y Asamblea Representativa, cada una de ellas con su propia organización y con funciones separadas (Consejo Universitario, 1974).
    1.1. Tribunal Electoral Universitario
2. **Consejo Universitario**: es el organismo inmediato en jerarquía a la Asamblea Universitaria.
    2.1. Contraloría Universitaria
3. **Rectoría**: encabezada por el Rector, quien es el funcionario académico de más alta jerarquía ejecutiva, a quien, entre otras funciones, le corresponde ejercer la

representación judicial y extrajudicial de la UCR (Consejo Universitario, 1974). Bajo la responsabilidad de la Rectoría, se encuentran las siguientes unidades:

3.1. Archivo Universitario (AUROL)
3.2. Oficina de Asuntos Internacionales
3.3. Oficina Jurídica
3.4. Oficina de Planificación
3.5. Oficina Ejecutora del Programa de Inversiones
3.6. Centro de Informática
3.7. Vicerrectoría de Administración
    3.7.1. Recursos Humanos
    3.7.2. Servicios Generales
    3.7.3. Oficina de Suministros
    3.7.4. Administración Financiera
3.8. Vicerrectoría de Investigación
    3.8.1. Sistema de Bibliotecas
    3.8.2. Sistema de Estudios de Posgrado
    3.8.3. Centros de Investigación
    3.8.4. Dirección Editorial
    3.8.5. Programa de Innovación
    3.8.6. Estaciones experimentales
3.9. Vicerrectoría de Acción Social
    3.9.1. Trabajo Comunal Universitario
    3.9.2. Extensión Cultural
    3.9.3. Medios de Comunicación
    3.9.4. Extensión Docente
    3.9.5. Centros Infantiles
    3.9.6. Oficina de Comunicación Institucional
3.10. Vicerrectoría de Vida Estudiantil
    3.10.1. Oficina de Registro
    3.10.2. Oficina de Bienestar y Salud
    3.10.3. Oficina de Orientación

3.10.4. Oficina de Becas

3.11. Vicerrectoría de Docencia

3.11.1. Centro de Evaluación Académica

3.11.2. Área de Ciencias Agroalimentarias

3.11.3. Área de Artes y Letras

3.11.4. Área de Salud

3.11.5. Área de Ciencias Sociales

3.11.6. Área de Ingeniería

3.11.7. Área de Ciencias Básicas

3.11.8. Sedes Regionales

3.11.9. Posgrados

Todas estas instancias universitarias, producen y reciben documentos en el ejercicio de sus funciones, siendo así que con el auge de las TIC, la mayoría de esta información se encuentra en soporte electrónico, y como tal, requiere de características especiales para su gestión y preservación a largo plazo.

La UCR como institución pública de educación superior, para hacer frente a todas las necesidades organizacionales, cuenta con una de las características más importantes en cuanto a su propia administración: independencia para el cumplimiento de sus funciones, conocida como *autonomía universitaria*, la cual se asegura en el artículo 4 de su ley orgánica (Asamblea Legislativa, 1940):

> ARTÍCULO 4º-La Universidad será autónoma y gozará de capacidad jurídica plena para adquirir derechos y contraer obligaciones. Será de su incumbencia exclusiva, por consiguiente, adoptar programas y planes de estudio, nombrar personal docente y administrativo, otorgar grados académicos y títulos profesionales, disponer de su patrimonio y dictar los reglamentos necesarios para el gobierno de sus escuelas y servicios, todo de acuerdo con las leyes que la rijan.

Así como en el artículo 84 de la Constitución Política de Costa Rica (Asamblea Nacional Constituyente, 1949):

> ARTÍCULO 84.- La Universidad de Costa Rica es una institución de cultura superior que goza de independencia para el desempeño de sus funciones y de plena capacidad jurídica para adquirir derechos y contraer obligaciones, así como para darse su organización y gobierno propios. Las demás instituciones de educación superior universitaria del Estado tendrán la misma independencia funcional e igual capacidad jurídica que la Universidad de Costa Rica. El Estado las dotará de patrimonio propio y colaborará en su financiación.

Y, finalmente en su Estatuto Orgánico (Consejo Universitario, 1974), en el artículo 2:

> ARTÍCULO 2.- La Universidad de Costa Rica goza de independencia para el desempeño de sus funciones y de plena capacidad jurídica para adquirir derechos y contraer obligaciones, así como para darse su organización y gobierno propios. Su régimen decisorio es democrático y por consiguiente en ella las decisiones personales y colectivas se realizan con absoluta libertad.

La autonomía universitaria de la UCR, le permite tomar sus propias decisiones administrativas, entre ellas aquellas relacionadas con la gestión de los documentos de archivo, y en este caso particular, con respecto a la necesidad de su preservación a largo plazo.

De esta forma, la UCR cuenta con las siguientes instancias encargadas de la creación, implementación y mantenimiento del Archivo Digital y la Política de Preservación Digital: la Rectoría, como ente superior administrativo; el Archivo Universitario Rafael Obregón Loría (AUROL), como autoridad técnica sobre los archivos de la Universidad y encargado de desarrollar métodos y prácticas archivísticas que faciliten la administración documental universitaria (Consejo Universitario, 2008); la Comisión Institucional de Archivo Digital (CIADi), como órgano asesor sobre la estrategia y planificación del Archivo Digital de la UCR (Serra-Serra, 2013d); y el Centro de Informática, como instancia encargada de asegurar que las TIC contribuyan al cumplimiento de los objetivos institucionales de la UCR (Rectoría, 2018).

2.1.2. Análisis de normativa

La Universidad de Costa Rica es una institución de educación superior, con autonomía y capacidad jurídica plena. Forma parte del sector público costarricense y como tal, está sujeto a la

aplicación de la legislación nacional vigente. Además, cuenta con un amplio marco normativo interno, que dirige el accionar de la institución y las funciones que desarrolla dentro de los tres ejes de docencia, investigación y acción social que componen su marco estratégico.

Conocer la normativa que afecta a la UCR, es de relevancia ya que "facilita que el diseño de la propuesta del modelo de preservación de documentos digitales contemple las necesidades o requerimientos de la Universidad con respecto a legislación nacional y normativa institucional vigente" (Castillo-Solano & Umaña-Alpízar, 2019, p.109), es decir, reconoce el origen de los documentos de archivo y evidencias de información, ya que se liga con las funciones que se desarrollan por medio del estatuto legal de la institución.

De esta forma, a continuación se adjunta un índice de normativa (Tabla 2) con los principales preceptos de aplicación para la UCR:

Tabla 2. *Índice de normativa de la Universidad de Costa Rica.*

Tipo de norma	Fecha de publicación	Número de Normativa	Título de la Normativa	Temática
Constitución Política	1949-11-08	-	Constitución Política de la República de Costa Rica	Título VII. De la Educación y la cultura.
Convenio	1982-04-20	-	Convenio de coordinación de la educación superior universitaria estatal	Capítulo I Los Organismos de Coordinación de la Educación Superior Universitaria Estatal
Convenio	1992-02-11	-	Convenio marco entre la Organización de Naciones Unidas para la educación, la ciencia y la cultura (UNESCO) y las instituciones de la educación superior estatal de Costa Rica	Facilitar las relaciones entre las Instituciones de Educación Superior Estatales de Costa Rica y la UNESCO en los campos de la educación, la ciencia, la cultura, las ciencias sociales y la comunicación
Convenio	1993-03-01	-	Convenio para la creación del Sistema Nacional de Acreditación de la Educación Superior	Creación del Sistema Nacional de Acreditación de la Educación Superior (SINAES)
Convenio	1997-09-22	-	Convenio de articulación y cooperación de la educación superior estatal de Costa Rica y sus adhesiones	Se establece el Consejo de Articulación de la Educación Superior Estatal de Costa Rica
Convenio	1998-09-01	-	Convenio marco para el desarrollo de sedes regionales interuniversitarias en la educación superior universitaria estatal de Costa Rica	Autorizar el funcionamiento de Sedes Regionales Interuniversitarias
Ley	1940-08-06	362	Ley Orgánica de la Universidad de Costa Rica	Creación de la Universidad de Costa Rica
Ley	1976-06-10	5909	Ley de Reforma Tributaria de 1976	Establece el Fondo Especial para el Financiamiento de la Educación Superior
Ley	1978-05-02	6227	Ley General de la Administración Pública	Administración Pública de Costa Rica
Ley	1980-07-15	6450	Ley de Reforma al Código Fiscal y de la Ley de impuesto sobre la renta	Asignación de recursos para la Universidades Públicas
Ley	1981-05-18	6580	Ley de Reforma Constitucional	Reforma al artículo 85 de la Constitución Política
Ley	1994-04-05	7386	Reforma la Ley Nº 6450 "Reforma Código Fiscal, ley de impuesto sobre la Renta, Ley de Creación del Ministerio de Obras Públicas y Transportes"	Modifica los montos asignados a las universidades estatales y dispone su actualización anual.

Tipo de norma	Fecha de publicación	Número de Normativa	Título de la Normativa	Temática
Ley	1996-05-01	7494	Ley de Contratación Administrativa	Proceso de contratación administrativa en Costa Rica
Ley	2002-03-04	8220	Ley de protección al ciudadano del exceso de requisitos y trámites	Protección al ciudadano del exceso de requisitos y trámites
Ley	2002-05-17	8256	Ley del Sistema Nacional de Acreditación de la Educación Superior	Ley que reconoce al Sistema Nacional de Acreditación de la Educación Superior (SINAES)
Ley	2002-07-31	8292	Ley General de Control Interno	Control Interno
Ley	2004-10-06	8422	Ley contra la Corrupción y el Enriquecimiento Ilícito en la Función Pública	Lucha contra la Corrupción y el Enriquecimiento Ilícito en la Función Pública
Ley	2005-08-30	8454	Ley de Certificados, firmas digitales y documentos electrónicos	Certificados, firmas digitales y documentos electrónicos
Ley	2010-04-16	8798	Ley de fortalecimiento del Sistema Nacional de Acreditación de la Educación Superior (SINAES)	Fortalecimiento del SINAES
Ley	2011-09-05	8968	Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales	Protección de la Persona Frente al Tratamiento de sus Datos Personales
Ley	2013-04-22	9126	Reforma Integral ley N° 1362 "Creación del Consejo Superior de Educación Pública"	Creación del Consejo Superior de Educación Pública
Ley	2018-03-12	9635	Fortalecimiento de las finanzas públicas	Fortalecimiento de las finanzas públicas
Reglamento	2005-04-28	Decreto Nº 32565-MEIC	Reglamento a la Ley de protección al ciudadano del exceso de requisitos y trámites administrativos	Protección al ciudadano del exceso de requisitos y trámites administrativos
Reglamento	2006-03-20	Decreto N.° 33018	Reglamento a la Ley de Certificados, Firmas Digitales y Documentos Electrónicos	Certificados, Firmas Digitales y Documentos Electrónicos
Norma	2009-02-06	La Gaceta N.° 26	Normas de Control Interno en el Sector Público, de la Contraloría General de República	Control Interno
Estatuto Orgánico	1974-03-15	-	Estatuto Orgánico de la Universidad de Costa Rica	Normativa interna UCR

Tipo de norma	Fecha de publicación	Número de Normativa	Título de la Normativa	Temática
Reglamento	2005-09-29	-	Reglamento sobre el Acceso a la Biodiversidad en actividades de Docencia, Acción Social y de Investigación de la Universidad de Costa Rica,	Normativa interna UCR
Reglamento	1983-04-19	-	Reglamento de los Actos de graduación	Normativa interna UCR
Reglamento	2000-07-10	-	Reglamento para la Administración y asignación del programa de Becas Clyde J. Surgi,	Normativa interna UCR
Reglamento	2011-06-09	-	Reglamento para la Administración y Control de los Bienes Institucionales de la Universidad de Costa Rica,	Normativa interna UCR
Reglamento	2003-03-07	-	Reglamento del proceso de Admisión mediante prueba de aptitud académica	Normativa interna UCR
Reglamento	2006-09-29	-	Reglamento Específico para el Apoyo financiero complementario a estudiantes y grupos estudiantiles de la Universidad de Costa Rica,	Normativa interna UCR
Reglamento	1979-08-20	-	Reglamento del Área de acción social de la Facultad de Derecho	Normativa interna UCR
Reglamento	1987-07-10	-	Reglamento del Artículo 30 del convenio de coordinación de la educación superior universitaria estatal	Normativa interna UCR
Reglamento	1987-08-21	-	Reglamento del Artículo 41 del convenio de coordinación de la educación superior universitaria estatal en Costa Rica,	Normativa interna UCR
Reglamento	1986-08-20	-	Reglamento de la Asamblea Colegiada Representativa	Normativa interna UCR
Reglamento	2018-12-07	-	Reglamento para la Asignación de recursos financieros a los funcionarios que participen en eventos académicos internacionales	Normativa interna UCR
Reglamento	2004-06-30	-	Reglamento para el uso de Auditorios de la Universidad de Costa Rica	Normativa interna UCR

Tipo de norma	Fecha de publicación	Número de Normativa	Título de la Normativa	Temática
Reglamento	1975-02-03	-	Reglamento de Ausencias a asamblea	Normativa interna UCR
Reglamento	2013-10-23	-	Reglamento de adjudicación de Becas a la población estudiantil	Normativa interna UCR
Reglamento	2004-09-09	-	Reglamento del Beneficio de residencias para la población estudiantil de la Universidad de Costa Rica	Normativa interna UCR
Reglamento	2011-04-06	-	Reglamento del régimen de Beneficios para el mejoramiento académico en el exterior para el personal docente y administrativo en servicio	Normativa interna UCR
Reglamento	1983-05-13	-	Reglamento para facilitar la Capacitación de los profesores no incorporados en régimen académico	Normativa interna UCR
Reglamento	1978-03-06	-	Reglamento de Carreras interdisciplinarias	Normativa interna UCR
Reglamento	2011-03-18	-	Reglamento de las Casas Infantiles Universitarias	Normativa interna UCR
Reglamento	2022-06-09	-	Reglamento del Centro Centroamericano de Población (CCP)	Normativa interna UCR
Reglamento	2009-10-09	-	Reglamento del Centro de Electroquímica y Energía Química (CELEQ)	Normativa interna UCR
Reglamento	2021-01-18	-	Reglamento del Centro de Evaluación Académica (CEA)	Normativa interna UCR
Reglamento	2018-06-01	-	Reglamento del Centro de Informática	Normativa interna UCR
Reglamento	2011-09-13	-	Reglamento del Centro de Investigación en Biología Celular y Molecular (CIBCM)	Normativa interna UCR
Reglamento	2007-02-19	-	Reglamento del Centro de Investigación en Ciencia e Ingeniería de Materiales (CICIMA)	Normativa interna UCR
Reglamento	2020-11-06	-	Reglamento del Centro de Investigación en Ciencias del mar y Limnología (CIMAR)	Normativa interna UCR
Reglamento	2021-09-16	-	Reglamento del Centro de Investigación en Ciencias del Movimiento Humano (CIMOHU)	Normativa interna UCR

Tipo de norma	Fecha de publicación	Número de Normativa	Título de la Normativa	Temática
Reglamento	2022-02-17	-	Reglamento del Centro de Investigación en Comunicación (CICOM)	Normativa interna UCR
Reglamento	2005-02-17	-	Reglamento del Centro de Investigación en Contaminación Ambiental (CICA)	Normativa interna UCR
Reglamento	2021-02-25	-	Reglamento del Centro de Investigación en Cuidado en Enfermería y Salud	Normativa interna UCR
Reglamento	2005-02-18	-	Reglamento del Centro de Investigación en Desarrollo Sostenible (CIEDES)	Normativa interna UCR
Reglamento	2005-02-23	-	Reglamento del Centro de Investigación en Enfermedades Tropicales (CIET)	Normativa interna UCR
Reglamento	2010-05-28	-	Reglamento del Centro de Investigación en Estructuras Microscópicas (CIEMIC)	Normativa interna UCR
Reglamento	2006-02-10	-	Reglamento del Centro de Investigación en Estudios de la Mujer (CIEM)	Normativa interna UCR
Reglamento	2009-08-28	-	Reglamento del Centro de Investigación en Hematología y Trastornos Afines (CIHATA)	Normativa interna UCR
Reglamento	2014-06-20	-	Reglamento del Centro de Investigación en Identidad y cultura Latinoamericanas (CIICLA)	Normativa interna UCR
Reglamento	2020-07-30	-	Reglamento del Centro de Investigación en Matemática Pura y Aplicada (CIMPA)	Normativa interna UCR
Reglamento	2022-03-04	-	Reglamento del Centro de Investigación en Protección de Cultivos (CIPROC)	Normativa interna UCR
Reglamento	2019-11-04	-	Reglamento del Centro de Investigación y Capacitación en Administración Pública (CICAP)	Normativa interna UCR
Reglamento	2022-03-03	-	Reglamento del Centro de Investigaciones Agronómicas (CIA)	Normativa interna UCR

Tipo de norma	Fecha de publicación	Número de Normativa	Título de la Normativa	Temática
Reglamento	2009-05-19	-	Reglamento del Centro de Investigaciones en Ciencias Atómicas, Nucleares y Moleculares (CICANUM)	Normativa interna UCR
Reglamento	2009-07-14	-	Reglamento del Centro de Investigaciones en Ciencias Geológicas (CICG)	Normativa interna UCR
Reglamento	1987-01-14	-	Reglamento para el Centro de Investigaciones en granos y semillas (CIGRAS)	Normativa interna UCR
Reglamento	2021-09-22	-	Reglamento del Centro de Investigaciones en Neurociencias (CIN)	Normativa interna UCR
Reglamento	1978-12-19	-	Reglamento del Centro de Investigaciones en productos naturales (CIPRONA)	Normativa interna UCR
Reglamento	2019-10-25	-	Reglamento del Centro de Investigaciones en Tecnologías de la Información y Comunicación (CITIC)	Normativa interna UCR
Reglamento	2021-06-30	-	Reglamento del Centro de Investigaciones Espaciales (CINESPA)	Normativa interna UCR
Reglamento	2019-12-10	-	Reglamento del Centro de Investigaciones Históricas de América Central (CIHAC)	Normativa interna UCR
Reglamento	2020-07-30	-	Reglamento del Centro de Investigaciones Matemáticas y Meta-Matemáticas (CIMM)	Normativa interna UCR
Reglamento	2013-11-19	-	Reglamento del Centro de Investigaciones sobre Diversidad Cultural y Estudios Regionales (CIDICER)	Normativa interna UCR
Reglamento	2010-11-24	-	Reglamento del Centro de Investigaciones y Estudios Políticos (CIEP)	Normativa interna UCR
Reglamento	2012-04-27	-	Reglamento de Ciclos de estudio de la Universidad de Costa Rica	Normativa interna UCR
Reglamento	1997-10-24	-	Reglamento de Circulación y estacionamiento de vehículos en la Universidad de Costa Rica	Normativa interna UCR

Tipo de norma	Fecha de publicación	Número de Normativa	Título de la Normativa	Temática
Reglamento	2017-10-25	-	Reglamento de Cobro Administrativo y Judicial de la Universidad de Costa Rica	Normativa interna UCR
Reglamento	2014-03-18	-	Reglamento del Comité Gerencial de Informática de la Universidad de Costa Rica	Normativa interna UCR
Normas	1999-04-12	-	Normas para la asignación de Complementos salariales a funcionarios universitarios con fondos extrauniversitarios	Normativa interna UCR
Reglamento	1990-03-14	-	Reglamento que regule la Concesión a terceros de la autorización para realizar obras en inmuebles de la Universidad	Normativa interna UCR
Reglamento	2017-06-28	-	Reglamento del Consejo Universitario	Normativa interna UCR
Convención	2018-06-06	-	Convención Colectiva de Trabajo	Normativa interna UCR
Reglamento	2006-05-16	-	Reglamento para el Cuido y Uso de Animales de Laboratorio en la Universidad de Costa Rica	Normativa interna UCR
Convención	1976-07-19	-	Convenio para unificar la Definición de crédito en la Educación Superior de Costa Rica	Normativa interna UCR
Reglamento	1985-10-23	-	Reglamento sobre Departamentos, secciones y cursos	Normativa interna UCR
Reglamento	1988-03-16	-	Reglamento de la Dirección Editorial y de Difusión Científica de la Investigación de la Universidad de Costa Rica (DIEDIN)	Normativa interna UCR
Reglamento	2020-04-20	-	Reglamento de la Universidad de Costa Rica en contra de la Discriminación	Normativa interna UCR
Reglamento	2022-04-05	-	Reglamento interno del Doctorado en Estudios de la Sociedad y la Cultura	Normativa interna UCR
Reglamento	2010-04-13	-	Reglamento Específico para la Aceptación de Donaciones a la Universidad de Costa Rica	Normativa interna UCR
Reglamento	2010-04-13	-	Reglamento General para la aceptación de Donaciones en la Universidad de Costa Rica	Normativa interna UCR

Tipo de norma	Fecha de publicación	Número de Normativa	Título de la Normativa	Temática
Reglamento	1976-08-31	-	Reglamento para la Edición de revistas	Normativa interna UCR
Reglamento	1995-07-12	-	Reglamento de Elecciones universitarias	Normativa interna UCR
Lineamientos	2004-10-27	-	Lineamientos para la Emisión de la Normativa Institucional	Normativa interna UCR
Reglamento	2012-10-20	-	Reglamento de la Universidad de Costa Rica En contra del hostigamiento en el trabajo o acoso laboral	Normativa interna UCR
Reglamento	2011-11-07	-	Reglamento de la Escuela de Estadística	Normativa interna UCR
Reglamento	1980-05-05	-	Reglamento de la Escuela de Estudios Generales	Normativa interna UCR
Reglamento	2008-10-24	-	Reglamento de la Escuela de Medicina	Normativa interna UCR
Reglamento	1996-10-04	-	Reglamento de la Escuela de Salud Pública	Normativa interna UCR
Reglamento	2022-01-05	-	Reglamento de Estudio independiente	Normativa interna UCR
Reglamento	2000-06-22	-	Reglamento Ético científico de la Universidad de Costa Rica para las investigaciones en las que participan seres humanos	Normativa interna UCR
Reglamento	1977-12-05	-	Reglamento de la Facultad de Ingeniería	Normativa interna UCR
Reglamento	1976-12-15	-	Reglamento de la Facultad de Microbiología	Normativa interna UCR
Reglamento	1989-06-21	-	Reglamento de la Facultad de Odontología	Normativa interna UCR
Reglamento	2001-06-06	-	Reglamento de la Finca Experimental de Santa Cruz (FESC)	Normativa interna UCR
Reglamento	2015-02-10	-	Reglamento de la Finca Experimental Interdisciplinaria de Modelos Agroecológicos (FEIMA)	Normativa interna UCR
Reglamento	2002-06-26	-	Reglamento para la administración del Fondo de Desarrollo Institucional	Normativa interna UCR
Lineamientos	2003-04-30	-	Lineamientos para la gestión de los programas de posgrado con financiamiento complementario,	Normativa interna UCR

Tipo de norma	Fecha de publicación	Número de Normativa	Título de la Normativa	Temática
			Normativa de procedimientos y criterios para el manejo del Fondo especial de becas	
Normativa	2003-04-30	-	Normativa de procedimientos y criterios para el manejo del Fondo Restringido 170	Normativa interna UCR
Reglamento	2008-11-17	-	Reglamento general del Fondo solidario estudiantil para el apoyo a estudiantes con situaciones calificadas de salud	Normativa interna UCR
Reglamento	2009-02-26	-	Reglamento general para la administración y fiscalización de Fondos de Trabajo	Normativa interna UCR
Normas	2009-02-12	-	Normas generales y específicas para la Formulación, ejecución y evaluación del presupuesto de la Universidad de Costa Rica	Normativa interna UCR
Reglamento	2001-07-10	-	Reglamento de Gastos de viaje y de transporte para funcionarios públicos	Normativa interna UCR
Lineamientos	2004-10-27	-	Lineamientos para la implementación de un modelo de Gestión de la calidad en la Universidad de Costa Rica	Normativa interna UCR
Normas	1989-08-25	-	Normas sobre Graduación de honor para estudiantes del Sistema de Estudios de Posgrado	Normativa interna UCR
Reglamento	1989-11-01	-	Reglamento para conferir Honores y distinciones por parte de la Universidad de Costa Rica	Normativa interna UCR
Reglamento	2015-09-23	-	Reglamento de Horas estudiante, horas asistente y horas asistente de posgrado	Normativa interna UCR
Reglamento	2020-08-31	-	Reglamento de la Universidad de Costa Rica en contra del Hostigamiento Sexual	Normativa interna UCR
Reglamento	2015-01-13	-	Reglamento del Instituto Clodomiro Picado (ICP)	Normativa interna UCR
Reglamento	1989-09-22	-	Reglamento del Instituto de Investigaciones Agrícolas (IIA)	Normativa interna UCR

Tipo de norma	Fecha de publicación	Número de Normativa	Título de la Normativa	Temática
Reglamento	2021-03-11	-	Reglamento del Instituto de Investigaciones en Arte	Normativa interna UCR
Reglamento	2007-05-23	-	Reglamento del Instituto de Investigaciones en Ciencias Económicas (IICE)	Normativa interna UCR
Reglamento	2021-12-17	-	Reglamento del Instituto de Investigaciones en Educación (INIE)	Normativa interna UCR
Reglamento	2021-10-08	-	Reglamento del Instituto de Investigaciones en Ingeniería (INII)	Normativa interna UCR
Reglamento	2021-02-10	-	Reglamento del Instituto de Investigaciones en Salud (INISA)	Normativa interna UCR
Reglamento	2021-11-26	-	Reglamento del Instituto de Investigaciones Farmacéuticas (INIFAR)	Normativa interna UCR
Reglamento	2004-06-04	-	Reglamento del Instituto de Investigaciones Filosóficas (INIF)	Normativa interna UCR
Reglamento	2005-10-03	-	Reglamento del Instituto de Investigaciones Jurídicas (IIJ)	Normativa interna UCR
Reglamento	2019-10-08	-	Reglamento General del Instituto de Investigaciones Lingüísticas (INIL)	Normativa interna UCR
Reglamento	2021-04-22	-	Reglamento del Instituto de Investigaciones Psicológicas (IIP)	Normativa interna UCR
Reglamento	2021-06-02	-	Reglamento del Instituto de Investigaciones Sociales (IIS)	Normativa interna UCR
Reglamento	1969-10-16	-	Reglamento Interno de trabajo	Normativa interna UCR
Reglamento	2001-11-14	-	Reglamento sobre Inversiones en Títulos Valores de la Universidad de Costa Rica	Normativa interna UCR
Reglamento	2016-04-05	-	Reglamento de la Investigación en la Universidad de Costa Rica	Normativa interna UCR
Reglamento	2004-07-08	-	Reglamento del Jardín Botánico Lankester	Normativa interna UCR

Tipo de norma	Fecha de publicación	Número de Normativa	Título de la Normativa	Temática
Reglamento	2020-06-30	-	Reglamento de la Junta administradora del fondo de ahorro y préstamo de la Universidad de Costa Rica	Normativa interna UCR
Reglamento	2016-09-08	-	Reglamento para la creación y funcionamiento del Laboratorio Didáctico de Interactividad y Comunicación Audiovisual y Multimedial de la Escuela de Ciencias de la Comunicación Colectiva	Normativa interna UCR
Reglamento	2012-04-13	-	Reglamento específico del Laboratorio Nacional de Materiales y Modelos Estructurales (LANAMME)	Normativa interna UCR
Reglamento	1977-11-04	-	Reglamento de Licencia sabática para los profesores de la Universidad de Costa Rica	Normativa interna UCR
Lineamientos	2022-04-01	-	Lineamientos en favor del derecho de Petición	Normativa interna UCR
Lineamientos	1983-08-29	-	Lineamientos generales del Centro Infantil Laboratorio	Normativa interna UCR
Lineamientos	2022-03-14	-	Lineamientos para galardonar con la Medalla Conmemorativa Institucional del 75.º Aniversario	Normativa interna UCR
Reglamento	1978-04-14	-	Reglamento de Matrícula del Sistema de Estudios de Posgrado	Normativa interna UCR
Reglamento	2011-03-24	-	Reglamento para el reconocimiento de losde los Mejores promedios de la Universidad de Costa Rica	Normativa interna UCR
Convenio	2004-04-02	-	Convenio sobre la Nomenclatura de Grados y Títulos de la Educación Superior Universitaria Estatal	Normativa interna UCR
Reglamento	1996-03-15	-	Reglamento de Obligaciones financieras estudiantiles	Normativa interna UCR
Reglamento	2004-02-27	-	Reglamento del Observatorio de Desarrollo	Normativa interna UCR
Reglamento	1988-11-16	-	Reglamento de la Oficina de Administración Financiera	Normativa interna UCR
Reglamento	2011-02-23	-	Reglamento de la Oficina de Asuntos Internacionales y Cooperación Externa (OAICE)	Normativa interna UCR
Reglamento	2012-09-12	-	Reglamento de la Oficina de Bienestar y Salud	Normativa interna UCR

Tipo de norma	Fecha de publicación	Número de Normativa	Título de la Normativa	Temática
Reglamento	2018-12-21	-	Reglamento organizativo de la Oficina de Contraloría Universitaria	Normativa interna UCR
Reglamento	2017-03-08	-	Reglamento de la Oficina de Planificación Universitaria	Normativa interna UCR
Reglamento	1987-02-19	-	Reglamento de la Oficina de Registro	Normativa interna UCR
Reglamento	1989-03-07	-	Reglamento de la Oficina Ejecutora del programa de inversiones (OEPI)	Normativa interna UCR
Reglamento	1985-08-23	-	Reglamento de la Oficina Jurídica	Normativa interna UCR
Reglamento	2004-02-06	-	Reglamento general de las Oficinas Administrativas	Normativa interna UCR
Reglamento	1996-09-18	-	Reglamento de Orden y disciplina de los estudiantes de la Universidad de Costa Rica	Normativa interna UCR
Reglamento	2016-07-21	-	Reglamento para la Organización y funcionamiento de la gestión ambiental en la Universidad de Costa Rica	Normativa interna UCR
Reglamento	2019-09-02	-	Reglamento Organización y Funcionamiento de la Gestión del Riesgo de Desastres y Atención de Emergencias en la Universidad de Costa Rica	Normativa interna UCR
Reglamento	1988-11-28	-	Reglamento de Permisos para cursar estudios con goce de salario	Normativa interna UCR
Reglamento	1980-07-28	-	Reglamento para el uso y administración de las Piscinas de la Universidad de Costa Rica	Normativa interna UCR
Reglamento	2012-09-14	-	Reglamento del Premio al Investigador o Investigadora de la Universidad de Costa Rica	Normativa interna UCR
Reglamento	2018-02-12	-	Reglamento del Premio María Eugenia Dengo a la labor destacada en la Acción Social del personal docente de la Universidad de Costa Rica	Normativa interna UCR
Reglamento	2012-03-22	-	Reglamento del Premio Rodrigo Facio Brenes	Normativa interna UCR

Tipo de norma	Fecha de publicación	Número de Normativa	Título de la Normativa	Temática
Reglamento	2020-11-24	-	Reglamento que regula Prestación del servicio de personas funcionarias de la Administración Superior de la Universidad de Costa Rica	Normativa interna UCR
Convenio	1984-09-10	-	Convenio de Préstamo interbibliotecario de las instituciones de educación superior universitaria estatal	Normativa interna UCR
Procedimiento	2021-08-11	-	Procedimiento para la gestión de solicitudes de declaratoria de interés institucional	Normativa interna UCR
Reglamento	2022-02-25	-	Reglamento del Programa de Doctorado en Ciencias	Normativa interna UCR
Reglamento	2002-09-27	-	Reglamento General del Programa de Doctorado en Gobierno y Políticas Públicas	Normativa interna UCR
Reglamento	2019-05-08	-	Reglamento del Programa de Doctorado en Ingeniería	Normativa interna UCR
Reglamento	2008-04-18	-	Reglamento del Programa de estudios de posgrado en Ciencias Agrícolas y Recursos Naturales (PPCARN)	Normativa interna UCR
Reglamento	2007-09-19	-	Reglamento del Programa de Estudios de Posgrado en Matemática	Normativa interna UCR
Reglamento	2010-09-24	-	Reglamento del Programa de Maestría Profesional en Gestión Hotelera	Normativa interna UCR
Reglamento	2004-03-08	-	Reglamento del Programa de Posgrado en Administracion y Direccion de Empresas	Normativa interna UCR
Reglamento	2016-06-22	-	Reglamento del Programa de Posgrado en Bibliotecología y Estudios de la información	Normativa interna UCR
Reglamento	2014-08-10	-	Reglamento del Programa de Posgrado en Biología	Normativa interna UCR
Reglamento	2021-10-26	-	Reglamento del Programa de Posgrado en Ciencias Biomédicas	Normativa interna UCR
Reglamento	2015-07-27	-	Reglamento del Programa de Posgrado en Ciencias de la Enfermería	Normativa interna UCR

Tipo de norma	Fecha de publicación	Número de Normativa	Título de la Normativa	Temática
Reglamento	2022-02-24	-	Reglamento del Programa de Posgrado en Enseñanza del Castellano y la Literatura	Normativa interna UCR
Reglamento	2022-06-06	-	Reglamento interno del Programa de Posgrado en Español como Segunda Lengua	Normativa interna UCR
Reglamento	2021-12-08	-	Reglamento del Programa de Posgrado en Especialidades en Microbiología	Normativa interna UCR
Reglamento	2011-07-15	-	Reglamento del Programa de Posgrado en especialidades médicas	Normativa interna UCR
Reglamento	2015-01-14	-	Reglamento de Programa de Posgrado en Estadística	Normativa interna UCR
Reglamento	2006-03-30	-	Reglamento del Programa de Posgrado en Filosofía	Normativa interna UCR
Reglamento	2011-11-08	-	Reglamento del Programa de Posgrado en Geología	Normativa interna UCR
Reglamento	2021-09-01	-	Reglamento del Programa de Posgrado en Gerencia Agroempresarial	Normativa interna UCR
Reglamento	2022-01-19	-	Reglamento del Programa de Posgrado en Gerontología	Normativa interna UCR
Reglamento	2003-05-13	-	Reglamento Interno del Programa de Posgrado en Gestión Integrada de Áreas Costeras Tropicales	Normativa interna UCR
Reglamento	2021-12-16	-	Reglamento del Programa de Posgrado en Ingeniería Civil	Normativa interna UCR
Reglamento	2014-02-10	-	Reglamento del Programa de Posgrado en Lingüística	Normativa interna UCR
Reglamento	2012-03-28	-	Reglamento del Programa de Posgrado en Literatura	Normativa interna UCR
Reglamento	2021-10-27	-	Reglamento del Programa de Posgrado en Microbiología, Parasitología, Química Clínica e Inmunología	Normativa interna UCR
Reglamento	2010-09-24	-	Reglamento del Programa de Posgrado para Magíster Scientiae en Antropología	Normativa interna UCR

Tipo de norma	Fecha de publicación	Número de Normativa	Título de la Normativa	Temática
Reglamento	2014-08-29	-	Reglamento Específico del Programa de Voluntariado Estudiantil de la Universidad de Costa Rica	Normativa interna UCR
Reglamento	2010-10-26	-	Reglamento del Programa UCR-CNA	Normativa interna UCR
Lineamientos	2004-11-19	-	Lineamientos para la gestión de los Programas de posgrado con financiamiento complementario	Normativa interna UCR
Reglamento	1979-10-22	-	Reglamento sobre el uso de Propaganda, divulgación y otras actividades estudiantiles	Normativa interna UCR
Reglamento	2009-07-10	-	Reglamento del Recinto de Golfito	Normativa interna UCR
Reglamento	2007-05-29	-	Reglamento para el Reconocimiento y equiparación de estudios realizados en otras instituciones de educación superior	Normativa interna UCR
Reglamento	2012-12-10	-	Reglamento para la Recontratación de personal académico jubilado para los diferentes regímenes de pensiones y jubilaciones de la República	Normativa interna UCR
Reglamento	2019-11-14	-	Reglamento de la Red de Áreas Protegidas de la Universidad de Costa Rica (RAP)	Normativa interna UCR
Reglamento	2001-05-25	-	Reglamento de Régimen académico estudiantil	Normativa interna UCR
Reglamento	2008-11-24	-	Reglamento de Régimen académico y servicio docente	Normativa interna UCR
Normas	2002-04-04	-	Normas que regulan el Régimen de dedicación exclusiva en la Universidad de Costa Rica	Normativa interna UCR
Reglamento	2020-05-12	-	Reglamento del Régimen Disciplinario de las Autoridades Universitarias Superiores	Normativa interna UCR
Reglamento	2009-07-03	-	Reglamento de Régimen disciplinario del personal académico	Normativa interna UCR
Regulaciones	1991-08-19	-	Regulaciones del Régimen salarial académico de la Universidad de Costa Rica	Normativa interna UCR

Tipo de norma	Fecha de publicación	Número de Normativa	Título de la Normativa	Temática
Reglamento	2007-10-26	-	Reglamento del Registro de Proveedores de la Universidad de Costa Rica	Normativa interna UCR
Reglamento	2021-09-28	-	Reglamento del Centro de Investigaciones Antropológicas (CIAN)	Normativa interna UCR
Reglamento	2009-06-16	-	Reglamento del Programa de Posgrado en Computación e Informática	Normativa interna UCR
Reglamento	2022-06-17	-	Reglamento General de Centros Infantiles de la Universidad de Costa Rica	Normativa interna UCR
Reglamento	2018-11-28	-	Reglamento para la gestión y firma de convenios con otras instituciones y organizaciones	Normativa interna UCR
Reglamento	2017-06-01	-	Reglamento que regula el nombramiento adicional al tiempo completo del personal universitario	Normativa interna UCR
Reglamento	2002-02-22	-	Reglamento de la Reserva Biológica Alberto Ml. Brenes	Normativa interna UCR
Reglamento	1983-06-10	-	Reglamento del sistema de administración de Salarios de la Universidad de Costa Rica	Normativa interna UCR
Reglamento	1998-09-24	-	Reglamento de la Sede Regional de Guanacaste	Normativa interna UCR
Reglamento	1976-12-15	-	Reglamento de la Sede Regional de Occidente	Normativa interna UCR
Reglamento	2016-10-18	-	Reglamento de la Sede Regional del Pacífico Arnoldo Ferreto Segura	Normativa interna UCR
Reglamento	2018-12-06	-	Reglamento general de la Semana Universitaria	Normativa interna UCR
Reglamento	1981-02-09	-	Reglamento para el Servicio de fotocopiado en la Universidad de Costa Rica	Normativa interna UCR
Reglamento	2021-12-15	-	Reglamento del Servicio de transportes	Normativa interna UCR
Normas	1987-02-27	-	Normas generales para regular el manejo de Servicios alimenticios bajo responsabilidad de las asociaciones estudiantiles	Normativa interna UCR

Tipo de norma	Fecha de publicación	Número de Normativa	Título de la Normativa	Temática
Reglamento	1980-11-03	-	Reglamento para la concesión de Servicios universitarios a estudiantes extranjeros amparados por convenios de reciprocidad	Normativa interna UCR
Reglamento	2020-10-05	-	Reglamento para la realización de Sesiones virtuales y sesiones híbridas en órganos colegiados de la Universidad de Costa Rica	Normativa interna UCR
Reglamento	2008-10-03	-	Reglamento del Sistema de Archivos de la Universidad de Costa Rica	Normativa interna UCR
Reglamento	2021-01-06	-	Reglamento del Sistema de Bibliotecas, Documentación e Información	Normativa interna UCR
Reglamento	2018-01-17	-	Reglamento general del Sistema de Estudios de Posgrado	Normativa interna UCR
Reglamento	2013-09-30	-	Reglamento general del Sistema de Medios de Comunicación Social de la Universidad de Costa Rica	Normativa interna UCR
Lineamientos	1994-09-09	-	Lineamientos para el Sistema de Premiación Anual para Funcionarios del Sector Administrativo	Normativa interna UCR
Reglamento	2020-10-27	-	Reglamento del Sistema de seguridad institucional	Normativa interna UCR
Reglamento	2007-10-26	-	Reglamento del Sistema de Suministros de la Universidad de Costa Rica	Normativa interna UCR
Reglamento	2007-12-12	-	Reglamento del Sistema Especial de Contratación Administrativa para la adquisición de bienes y servicios con cargo a recursos administrados mediante la modalidad de fondos restringidos y empresas auxiliares	Normativa interna UCR
Reglamento	1978-05-12	-	Reglamento de Tesis del Sistema de Estudios de Posgrado	Normativa interna UCR
Reglamento	2018-08-30	-	Reglamento del Trabajo Comunal Universitario	Normativa interna UCR

Tipo de norma	Fecha de publicación	Número de Normativa	Título de la Normativa	Temática
Reglamento	2020-03-12	-	Reglamento general de los Trabajos finales de graduación en grado para la Universidad de Costa Rica	Normativa interna UCR
Reglamento	2016-10-27	-	Reglamento de Unidad de Regencia Química de la Universidad de Costa Rica	Normativa interna UCR
Reglamento	2000-02-14	-	Reglamento de la Unidad de Servicio de Apoyo Académico de la Facultad de Educación	Normativa interna UCR
Reglamento	2016-10-21	-	Reglamento de Uso de símbolos universitarios y línea gráfica institucional	Normativa interna UCR
Reglamento	1992-09-01	-	Reglamento de Vacaciones	Normativa interna UCR
Reglamento	1980-11-17	-	Reglamento de la Vicerrectoría de Acción Social	Normativa interna UCR
Reglamento	1977-08-26	-	Reglamento de la Vicerrectoría de Administración	Normativa interna UCR
Reglamento	2001-06-18	-	Reglamento general de la Vicerrectoría de Vida Estudiantil	Normativa interna UCR
Reglamento	2013-09-24	-	Reglamento del VII Congreso Universitario de la Universidad de Costa Rica	Normativa interna UCR
Reglamento	2017-12-14	-	Reglamento de la Universidad de Costa Rica para la Vinculación remunerada con el Sector Externo	Normativa interna UCR
Reglamento	2015-01-26	-	Reglamento General de Zonaje y Bonificación en la Universidad de Costa Rica	Normativa interna UCR

Fuente: elaboración propia a partir de CONARE (2012) y Consejo Universitario (s.f.).

2.1.3. Emisión de normativa institucional en la Universidad de Costa Rica

La complejidad organizacional de una institución de la magnitud de la Universidad de Costa Rica, representa un reto importante para poder controlar y ejecutar con calidad las funciones que desempeña.

Como se observó en el apartado anterior, existe una gran gama de normativa que tiene la finalidad de regular las acciones desarrolladas por las distintas unidades administrativas, académicas y de investigación que componen la Universidad.

Esto resulta relevante, ya que la implementación de un Archivo Digital requiere de la creación de normativa vinculante, entre ellas una política institucional, mediante la cual se asegure el apoyo y los recursos necesarios para mantener su funcionamiento a lo largo del tiempo.

En el caso específico de la creación de normativa interna, la UCR cuenta con los *Lineamientos para la emisión de la normativa institucional*, instrumento mediante el cual se establecen los "elementos básicos por considerar en la emisión de la normativa universitaria, con el fin de que el ordenamiento jurídico interno sea coherente con lo dispuesto en el Estatuto Orgánico, las competencias asignadas a los distintos órganos y los principios y disposiciones que rigen esta materia" (Consejo Universitario de la UCR, 2004, p.1).

Sin embargo, estos lineamientos no incluyen las políticas institucionales, las cuáles por su parte son creadas por el Consejo Universitario "órgano responsable de definir las políticas generales de la Universidad de Costa Rica, las cuales se expresan mediante acciones concretas que procuran fortalecer y mejorar el quehacer de la institución" (Consejo Universitario de la UCR, s.f.-2, p.1)

Las Políticas Institucionales que rigen la UCR, tienen la particularidad de ser enunciados generales, los cuáles (Consejo Universitario de la UCR, 2008, p.1)

> orientan y rigen todas las actividades sustantivas de la Institución, y se expresan mediante acciones concretas que fortalecen y mejoran el quehacer de la Universidad de Costa Rica, para contribuir con la transformación de la sociedad y el logro del bien común. Las políticas son un medio de relación entre la Universidad y la sociedad, de manera que constituyen también el referente que tiene la sociedad para pedirle a esta Institución el cumplimiento de sus fines y propósitos. La comunidad universitaria debe conocer las políticas, para afirmar su

identidad institucional y, a la vez, sustentar su quehacer académico, estudiantil o de gestión administrativa.

De esta manera, la construcción de las Políticas Institucionales, no lleva más especificaciones que un enunciado general, así como unos objetivos que permitan el cumplimiento de dichas políticas. Las acciones específicas para el desarrollo de estas políticas, implican a distintos actores y planes u otros instrumentos normativos, por lo que no se desarrollan en el marco del documento general llamado "Políticas Institucionales".

Esto puede observarse en las políticas vigentes de la UCR, llamadas "Políticas Institucionales 2021-2025", aprobadas en la Sesión N.º 6357, artículo 6, del 05/03/2020, publicada en el Alcance La Gaceta Universitaria 13-2020, del 17/03/2020 (Consejo Universitario de la UCR, 2020, p.1), donde se utiliza la siguiente estructura:

- Ejes (11): Ejes generales sobre los que la UCR trabaja.
    - Políticas (46): enunciados generales, rigen las actividades sustantivas de la UCR.
        - Objetivos (175): objetivos para el cumplimiento de las políticas propuestas.

Es así como, las Políticas de la Universidad, están divididas entre los principales ejes que se trabajan desde la institución y los objetivos (aunque también se pueden ver como enunciados generales), especifican la manera de cumplir con dichas Políticas.

Si bien en el *Eje VII. Gestión universitaria*, toca el tema de la preservación de documentos en la Política 7.4 al mencionar la creación de mecanismos de integración de la información de manera segura e interoperable, y al especificar en el objetivo 7.4.5 la necesidad de "Fomentar las buenas prácticas para la conservación y preservación del patrimonio documental y el acervo bibliográfico institucional, en formato impreso y digital" (Consejo Universitario de la UCR, 2020, p.14), este instrumento normativo no resulta lo suficientemente específico para llevar a cabo la preservación digital sistémica de las evidencias de información que se generan en la Universidad.

2.2. Análisis del escenario archivístico

Para comprender el contexto archivístico que se desarrolla en la UCR, a continuación se presentan los principales órganos encargados del desarrollo técnico de los procesos archivísticos institucionales.

2.2.1. Sistema de Archivos de la Universidad de Costa Rica

El Sistema de Archivos de la Universidad De Costa Rica (SAU), es la figura responsable de "regular la articulación y la coordinación de los diferentes archivos de la Universidad de Costa Rica, con el propósito de asegurar la buena gestión documental, así como la conservación, la difusión y el acceso a los documentos universitarios" (Consejo Universitario, 2008, p.1).

El SAU se define como "el conjunto de archivos universitarios (gestión, centrales, especializados e históricos), integrados a partir de un marco normativo, regulador y coordinador del funcionamiento del Sistema, así como de una estructura operativa que involucra el quehacer cotidiano de esos archivos" (Consejo Universitario, 2008, p.2).

Su creación se da por medio del Reglamento del Sistema de Archivos de la Universidad de Costa Rica, aprobado en sesión 5282-05, 02/09/2008 del Consejo Universitario y publicado en La Gaceta Universitaria 32-2008 del 03/10/2008 (Consejo Universitario, 2008, p.1).

Según el artículo 3 de dicho reglamento (2008), el SAU está conformado por:

- El Archivo Universitario Rafael Obregón Loría (AUROL): es el ente coordinador de SAU.
- Los archivos centrales, los archivos históricos, los archivos de gestión, los archivos especializados de todas las dependencias universitarias.
- La Comisión Universitaria de Selección y Eliminación de Documentos (CUSED).

Dentro de los propósitos del SAU mencionados en el artículo 2 de su reglamento, destacan: la adecuada gestión del fondo documental institucional; la protección, integridad y seguridad de la información; el libre acceso a la información; así como integrar la gestión documental, la gestión de la información y la gestión del conocimiento.

2.2.2. Archivo Universitario Rafael Obregón Loría (AUROL)

El AUROL es una unidad administrativa, que depende de manera directa de la Rectoría y ejerce la autoridad técnica sobre los archivos de la Universidad (Consejo Universitario, 2008, p.2). Se trata de un archivo histórico, "cuyo contenido documental es de conservación permanente, tras la valoración hecha en este archivo o en los archivos de gestión, centrales o especializados" (Consejo Universitario, 2008, p.1).

A pesar de que la Universidad de Costa Rica nace desde el año 1940, es hasta el año 2003 que el AUROL entra en funcionamiento, lo que significa un rezago de más de 60 años en cuanto a gestión documental. Aunado a ésto, es para el año 2008 que propiamente se elabora el Reglamento del SAU.

Sin embargo, desde su creación, el AUROL ha trabajado arduamente en la recuperación del patrimonio documental de la UCR. A raíz de la instalación del SAU, con el AUROL como ente coordinador, y la integración de la Comisión Universitaria de Selección y Eliminación de Documentos (CUSED), se trabaja en la elaboración de normativa y de instrumentos pertinentes para hacer frente a la gestión de los documentos institucionales, así como en la difusión de la información que conforma el fondo documental de la Universidad de Costa Rica.

Según el reglamento del SAU, al AUROL le corresponde emitir las directrices generales y los procedimientos en materia de archivística, por medio del Comité Técnico, que no tengan que ver con el proceso de evaluación documental; debe coordinar, asesorar y capacitar técnicamente a los encargados de archivos de la Universidad; además de rescatar, custodiar y difundir el patrimonio documental universitario; garantizar el acceso a la información archivística universitaria; diseñar, desarrollar y mantener un sistema de información archivística institucional, acorde con los avances tecnológicos; y apoyar las acciones académicas de la Institución en materia archivística, entre otras (Consejo Universitario, 2008, p.2).

Para comprender mejor la historia de la creación del AUROL, se pueden definir 5 etapas iniciales (AUROL, 2009):

I Etapa: 1978-1990: presentación de la propuesta para crear un archivo central en la Universidad. Aprobado por el Consejo Universitario en la sesión No. 3157, artículo 8, del 13 de febrero de 1985.

II Etapa 1990-1999: creación del Sistema Nacional de Archivos en 1990, mediante la aprobación de la Ley No. 7202. En acatamiento de la Ley, la Universidad integra por primera vez un Comité Institucional de Selección y Eliminación de Documentos.

III Etapa 1999-2002: El Rector asigna al Archivo Universitario un terreno para construir el depósito. El Consejo Universitario acuerda aplicar en la Universidad el Reglamento de la Ley 7202 hasta contar con un reglamento propio.

IV Etapa (2002-2004): Una Comisión Institucional nombrada por el rector Dr. Gabriel Macaya, propone organizar el Sistema de Archivos Universitarios (SAU). En 2003 se finaliza la construcción del edificio del Archivo Universitario y en 2004 el Consejo Universitario aprueba los Lineamientos para la gestión documental en la UCR.

V Etapa (2005-2008): En 2005 se inician los estudios para dotar a la Universidad de un software especializado en gestión de documentos, así como la elaboración de la tabla general de plazos de conservación de documentos para las unidades académicas. En el 2006 se aprueba la construcción de un segundo depósito, con el cual se amplía la capacidad de custodia del Archivo, y para 2008 se aprueba el Reglamento del Sistema de Archivos Universitarios.

Además, de manera más reciente se pueden mencionar las siguientes dos etapas:

VI Etapa (2009-2015): con la aprobación del Reglamento del Sistema de Archivos de la UCR, se derogan los Lineamientos para la Gestión Documental de la Universidad de Costa Rica, aprobados en 2004; y en 2009 se crea la plaza de la Dirección del Archivo Universitario. En 2012, inicia la construcción de un segundo depósito, así como una sala de sesiones; además en ese año, el AUROL comienza por primera vez la creación e implementación de un sistema de gestión de documentos llamado SISDOC. Desde el año 2013, el AUROL ha sido uno de los entes precursores y con mayor involucramiento en cuanto a la necesidad de la UCR de desarrollar acciones que permitan la preservación de información digital a largo plazo, ha trabajado en proyectos y propuestas tanto para la creación de una Comisión Institucional de Archivo Digital, como para la Política de preservación digital. A partir de 2013, se trabaja de manera interdisciplinaria con otras unidades un proyecto para la implementación de un Archivo

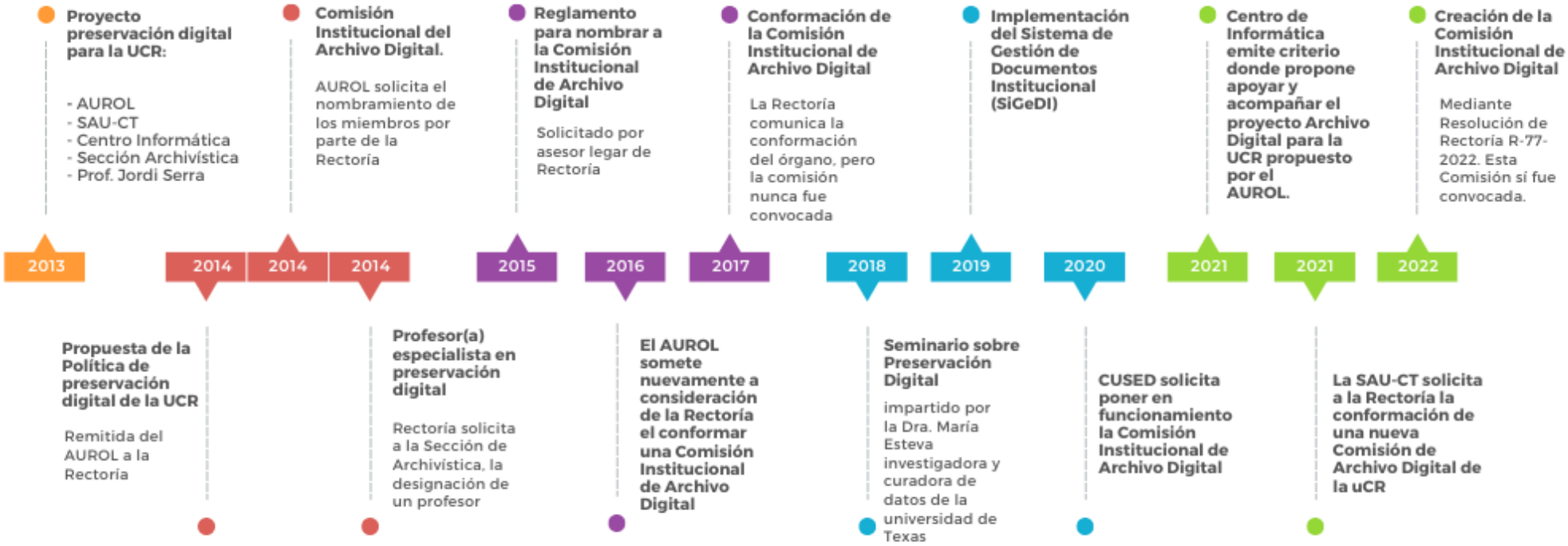
Digital. En 2014 se presenta ante la Rectoría la primera propuesta para una Política de Preservación Digital. Sin embargo, ambas iniciativas no recibieron el apoyo esperado por parte de las altas jerarquías. En el año 2015, se elabora y remite para su revisión y aprobación, una propuesta para el Reglamento de la Comisión Institucional de Archivo Digital.

VII Etapa (2016-actualmente): debido a que los esfuerzos anteriores no recibieron el apoyo esperado, en 2016 se vuelve a someter a consideración de la Rectoría, la conformación de una Comisión Institucional de Archivo Digital. Para 2017, la Rectoría conforma dicha Comisión, pero la misma nunca fue convocada a sesionar, por lo que no fue formalmente constituída. Además, en 2018, por medio de un plan piloto, se comienza la implementación de un nuevo sistema de gestión de documentos, que viene a reemplazar al SISDOC, llamado SiGeDI. Finalmente, en 2021 la Comisión Universitaria de Selección y Eliminación de Documentos, retoma esfuerzos para gestionar el tema de la Preservación Digital en la UCR, los cuales se ven respaldados por el Centro de Informática y el Comité Técnico del SAU. De esta forma, en el año 2022, se crea e inicia labores la Comisión Institucional de Archivo Digital.

Como se observa, el trabajo del AUROL ha tenido una evolución paulatina (figura 5) enfocada hacia el tratamiento de la información en soporte electrónico, al tiempo que sigue trabajando y resguardando el patrimonio documental universitario en soporte físico.

A continuación, se representa mediante una línea de tiempo (figura 5), las acciones más importantes que ha desarrollado el AUROL para enfrentarse al reto que supone para la Universidad de Costa Rica la preservación digital:

Figura 5. *Línea de tiempo de acciones tomadas por el AUROL para la preservación digital de información.*



Fuente*:* elaboración propia, 2023.

2.2.3. Comité Técnico (SAU-CT)

El Comité Tecnico es un órgano asesor del AUROL, de carácter permanente, el cual es nombrado por la Rectoría y está encargado de emitir políticas y directrices específicas en cuanto a la materia archivística de la UCR (Consejo Universitario, 2008, p.2).

El Reglamento del SAU (Consejo Universitario, 2008, p.3), señala en el artículo 10 que:

> Se establece un Comité Técnico que tiene como función la emisión y revisión de las directrices generales en materia de archivística, excepto las relacionadas con la valoración, selección y eliminación de documentos, correspondientes a la CUSED. El Comité se reunirá al menos dos veces al año en forma ordinaria y podrá realizar sesiones extraordinarias cuando se requiera. La convocatoria a las reuniones estará a cargo de la dirección del AUROL.
>
> El Comité Técnico estará conformado de la siguiente manera:
>
> a) La persona que ocupa la dirección del AUROL, quien coordina.
> b) La persona que ocupa la coordinación de la carrera de Archivística.
> c) Dos representantes de cada uno de los siguientes tipos de archivos: Archivos de Gestión, Archivos Centrales, Archivos Especializados.
>
> Estos representantes serán nombrados por la Rectoría por un período de cuatro años renovables.

Las directrices y procedimientos que emita el Comité en ejercicio de sus funciones, deben ser aprobados por la Rectoría y publicados en la Gaceta Universitaria; además, el Comité deberá elaborar un informe anual en el que se comunique su labor a la comunidad universitaria (SAU-CT, 2016).

La participación del Comité Técnico en cuanto a la preservación digital institucional, se reactiva a partir de la emisión del oficio CI-480-2021 del Centro de Informática de la UCR, donde se retoma la importancia del tema la correcta gestión de documentos producidos en la modalidad virtual en la institución.

En respuesta a la preocupación externada en este oficio, el Comité dictamina la necesidad urgente de conformar un equipo de trabajo que retomara el proyecto que se inició desde 2013, en

conjunto con el AUROL, el Centro de Informática y la Sección de Archivística, con la asesoría del profesor Jordi Serra Serra, de la Facultad de Biblioteconomía y Documentación de la Universidad de Barcelona. (SAU-CT, 2021)

El Comité Técnico, mediante el oficio SAU-CT-23-2021, comunica a la Rectoría de la Universidad los antecedentes del proyecto y solicita la conformación de una nueva Comisión de Archivo Digital de la Universidad de Costa Rica, integrada por: el Rector(a) o a quien se delegue, el director (a) del Centro de Informática o a quien se delegue, el director(a) del AUROL o a quien se delegue, un(a) profesor(a) de la Sección de Archivística con conocimientos en preservación digital, el representante de la Oficina Jurídica en la CUSED y un(a) representante de los medios de comunicación con conocimiento en la gestión de documentos audiovisuales (SAU-CT, 2021).

Ante esta solicitud, junto con los criterios emitidos por otros órganos, la Rectoría de la UCR toma la decisión de crear la Comisión Institucional de Archivo Digital, mediante la Resolución de Rectoría R-77-2022.

2.2.4. Comisión Universitaria de Selección y Eliminación de Documentos (CUSED)

La UCR cuenta con un órgano encargado de la evaluación documental institucional (como proceso técnico archivístico) desde el año 1993, cuando la Rectoría mediante la resolución R-2736-93, crea el Comité Institucional de Selección y Eliminación de Documentos (CISED), para cumplir con lo estipulado en la Ley 7202 Ley del Sistema Nacional de Archivos; este Comité comienza la presentación de tablas de plazos de conservación y valoraciones parciales ante la Comisión Nacional de Selección y Eliminación de Documentos (CUSED, 2015, p.1).

Sin embargo, a raíz de la creación del AUROL en el año 2003, así como de cuestionamientos sobre la aplicación de la Ley 7202 en la UCR, durante 2005, se realizan consultas a la Procuraduría General de la República, la cual mediante los dictámenes C-230-2006 del 5 de junio de 2006 y C-420-2006 del 20 de octubre de 2006, señala que la UCR posee autonomía universitaria para elaborar sus tablas de plazos de conservación de documentos (CUSED, 2015, p.1).

De esta forma, y a partir de la creación del Reglamento del Sistema de Archivos de la Universidad de Costa Rica en el año 2008, nace la Comisión Universitaria de Selección y Eliminación de Documentos (CUSED) como órgano técnico del Sistema, con la capacidad de aprobar las tablas de plazos de conservación institucionales, así como también las valoraciones parciales y cuyas directrices deben ser acatadas por las distintas instancias universitarias (CUSED, 2015, p.1).

La CUSED se define, en el artículo 11 del Reglamento del SAU, como "un órgano técnico del Sistema nombrado por la Rectoría. Esta Comisión establece las directrices en materia de valoración, selección, y eliminación de documentos de las dependencias universitarias, con el propósito de salvaguardar el patrimonio documental universitario" (Consejo Universitario, 2008, p.1).

Como se observa en la definición anterior, que la CUSED tiene la responsabilidad de emitir las directrices que requiera la UCR en materia de evaluación documental, de forma que los documentos que produce y recibe la Universidad, se mantengan disponibles durante el plazo que sean requeridos.

La CUSED, también ha tomado un importante papel en cuanto a la preservación digital de la información a largo plazo en la Universidad, siendo que en marzo de 2021 tiene la iniciativa de informar a la Rectoría la preocupación en cuanto a la preservación de documentos gestionados de manera digital, situación que se ha venido externando desde años anteriores, indicando mediante el oficio CUSED-13-2021 (p.1) que:

> (...) se ha detectado que los sistemas automatizados de la Universidad no garantizan la recuperación de la información a largo plazo y que aún no se ha implementado un proyecto de Archivo Digital que permita garantizar la conservación y acceso de los documentos universitarios durante el tiempo que sean requeridos en el ámbito administrativo y legal; así como la conservación de los documentos que han sido declarados de conservación permanente y con valor científico-cultural.

La preocupación que expresa la CUSED sobre la preservación digital, se ve acentuada por los cambios que ha representado para la comunidad universitaria la llegada de la pandemia por COVID-19, en el año 2020, principalmente en la dinámica laboral, donde el trabajo remoto de

los funcionarios “intensificó la producción de documentos electrónicos con firma digital certificada o firma digitalizada, documentos que en algunos casos se desconoce su ubicación porque no se ha podido capacitar a todo el personal sobre las mejores prácticas para archivar esos documentos” (CUSED, 2021, p.3).

2.2.5. Comisión Institucional de Archivo Digital (CIADi)

A raíz de las necesidades identificadas en la UCR con respecto a la preservación de información digital a largo plazo, en el año 2013, el AUROL, el Comité Técnico del SAU, el Centro de Informática y la Sección de Archivística de la Escuela de Historia trabajaron en un proyecto para darle respuesta a la situación (Rectoría, 2022).

El desarrollo de este proyecto, desencadenó una serie de acciones, dirigidas inicialmente desde el AUROL, con el objetivo de enfrentar el tema de preservación digital de la UCR de una manera formal y con apoyo de las altas jerarquías.

De esta forma, se llevan a cabo los siguientes eventos (Rectoría, 2022):

- 2014: El Archivo Universitario remite a la Rectoría la primera propuesta de la “Política de preservación digital de la Universidad de Costa Rica” con el oficio AUROL-183-2014.
- 2015: se remite una propuesta del Reglamento de la Comisión Institucional de Archivo Digital de la Universidad de Costa Rica para revisión y aprobación.
- 2016: el AUROL, mediante oficio AUROL-207-2016, somete a consideración de la Rectoría el conformar una Comisión Institucional de Archivo Digital en la Universidad de Costa Rica.
- 2017: la Rectoría conforma una Comisión Institucional de Archivo Digital, sin embargo, esta nunca fue convocada.
- 2021: La Rectoría recibió los oficios CUSED-13-2021 y CUSED-48-2021 de la CUSED y el oficio CI-480-2021 del Centro de Informática (CI), sobre las acciones que deben considerarse para el desarrollo de la segunda fase del Sistema de Gestión de Documentos Institucional (SiGeDI) y del proyecto de Preservación Digital de la Universidad de Costa Rica.

- 2021: el Comité Técnico del SAU, en el oficio SAU-CT-23- 2021, solicita nuevamente a la Rectoría conformar una comisión de Archivo Digital.

Ante esta serie de acciones, la Rectoría mediante la Resolución de Rectoría R-77-2022, resuelve crear la Comisión Institucional de Archivo Digital, integrada por funcionarios de las siguientes unidades (Rectoría, 2022):

- Rectoría
- Vicerrectoría de Acción Social
- Oficina Jurídica
- Centro de Informática
- Archivo Universitario Rafael Obregón Loría (AUROL)
- Escuela de Historia

De esta forma, la CIADi ha desarrollado sesiones desde marzo de 2022 para retomar el trabajo realizado en el año 2013. A través de estas reuniones se ha determinado la importancia de la creación del Archivo Digital de la Universidad de Costa Rica, con base en un marco normativo aprobado por la Rectoría y el Consejo Universitario, que permita definir las instancias universitarias que tendrán a cargo el desarrollo, implementación y mantenimiento del proyecto, al tiempo que se designan los roles y responsabilidades.

De esta forma, se han tomado como insumo los documentos desarrollados por el Máster Jordi Serra Serra, entre los que se encuentran la propuesta de política de preservación digital, el informe de evaluación de riesgos, el protocolo de ingreso y custodia, entre otros. A través de estas referencias se busca crear la estructura política, funcional y técnica necesaria para que se ponga en marcha el Archivo Digital.

La CIADi también ha tomado como insumo para su trabajo, los aspectos desarrollados en esta investigación, de manera que los resultados obtenidos aquí, puedan cubrir parte importante del trabajo teórico, contextual y técnico, necesario para adaptar un proyecto de Archivo Digital en la Universidad.

De esta forma, por ejemplo, en la Sección 2.4, se presenta el resultado de la actualización de la evaluación de los riesgos para continuidad digital, de forma que se cuente con un contexto

actual, que le ha contribuido a la CIADi en la toma de decisiones. También, en la Sección 2.5, se realiza el análisis de varias herramientas informáticas ofrecidas en el mercado como soluciones para la preservación digital, de forma que se puedan comparar sus principales características, para determinar si cumplen con los requisitos mínimos que requiere un Archivo Digital seguro.

Se plantea que el enfoque de la CIADi sea de carácter estratégico, como órgano asesor sobre la estrategia y la planificación del ADiUCR y fungiendo como encargado de solicitar al AUROL los recursos y medios necesarios para el funcionamiento de este (Serra-Serra, 2013d, p.8).

2.2.6. Disposiciones institucionales sobre procesos técnicos archivísticos

Los procesos técnicos archivísticos de la UCR, se pueden observar en dos grandes grupos: aquellos que están relacionados con la evaluación de documentos (valoración, selección y disposición final), y las directrices generales en materia de archivística.

En primera instancia, los procesos técnicos relacionados con la evaluación de documentos, son emitidos por un órgano técnico especializado, la CUSED. Esta Comisión, como se vio anteriormente, es la encargada de establecer las directrices en materia de evaluación documental: valoración, selección, y disposición final de documentos.

Dentro del ejercicio de sus funciones, la CUSED ha emitido informes de valoración (valoraciones parciales) y tablas de plazos de conservación para la institución; de las cuáles, las siguientes se encuentran vigentes (AUROL, 2017-b):

- Informe de valoración 15-2015: Archivo Universitario Rafael Obregón Loría
- Informe de valoración 16-2015: Comisión Universitaria de Selección y Eliminación de Documentos
- Informe de valoración 17-2015: Comité Técnico del SAU
- Informe de valoración 18-2018: Oficina de Divulgación e Información
- Tabla de Plazos de Conservación y Eliminación de Documentos (2018): Programas De Posgrado (Parcial) - *Actualizada 2019*
- Informe de Valoración 19-2019: Oficina Jurídica
- Informe de Valoración 20-2021: Centro De Evaluación Académica

- Tabla de Plazos de Conservación y Eliminación de Documentos (2018): Series Comunes en la Universidad de Costa Rica (Parcial) - *Actualizada 2021*
- Tabla de Plazos de Conservación y Eliminación de Documentos (2018): Unidades Académicas y Unidades Académicas De Investigación (Parcial) - *Actualizada 2021*

A través de estos informes de valoración y tablas de plazos de conservación, se han determinado las siguientes series documentales de conservación permanente:

- Archivo Universitario Rafael Obregón Loría
    - Expedientes de transferencia de documentos.
    - Expediente de donación de documentos.
    - Registro de consultas.
    - Expediente de capacitaciones en gestión de documentos y archivos.
    - Expediente de actividades de difusión.
    - Expediente de proyectos archivísticos.
    - Expediente de asesoría archivística.
    - Expediente de apoyo a la academia.

- Comisión Universitaria de Selección y Eliminación de Documentos
    - Expediente de valoración de documentos.
    - Informes de valoración (Tablas de plazos aprobadas por la CUSED).
    - Informes de valoración parcial.
    - Expediente de eliminación de documentos.
    - Actas de eliminación.
    - Expediente de directrices y procedimientos en materia de valoración, selección y eliminación de documentos.
    - Directrices y procedimientos en materia de valoración, selección y eliminación de documentos.
- Comité Técnico del SAU
    - Expediente de directrices y procedimientos en materia archivística.
    - Directrices y procedimientos en materia archivística.
- Oficina de Divulgación e Información
    - Expediente de manuales y guías de identidad institucional.

- Expedientes de diseño gráfico (publicaciones gráficas-material de diseño gráfico).
- Programas y guiones de radio y televisión de carácter informativo del quehacer universitario.
- Boletines de prensa.
- Monitoreo de noticias (parcial). (*Valor científico-cultural*).
- Expediente de evaluación de las comunicaciones y de la identidad institucional (parcial).

- Oficina Jurídica
  - Expediente de dictámenes. (*Valor científico-cultural*).
  - Expediente de procesos administrativos (no judiciales ante instancias externas). (*Valor científico-cultural*).
  - Expedientes judiciales. (*Valor científico-cultural*).
- Centro De Evaluación Académica
  - Expediente de gestión curricular. (*Valor científico-cultural*).
  - Expediente de procesos de autoevaluación y gestión de la calidad y excelencia académica de carreras de grado. (*Valor científico-cultural*).
  - Expediente de cargas académicas. (*Valor científico-cultural*).
  - Expediente académico docente. (*Valor científico-cultural*).
- Series Comunes en la Universidad de Costa Rica (Parcial)
  - Actas de eliminación de documentos.
  - Actas de órganos colegiados. (*Valor científico-cultural*).
  - Boletines técnicos.
  - Circulares enviadas de carácter procedimental.
  - Discursos. (*Valor científico-cultural*).
  - Expediente de actos oficiales universitarios. (*Valor científico-cultural*).
  - Expedientes de contratación administrativa (fracción).
  - Expedientes de reuniones.
  - Expedientes de sesiones de órganos colegiados.
  - Fotografías. (*Valor científico-cultural*).
  - Invitaciones enviadas.
  - Minutas.

- Unidades Académicas y Unidades Académicas De Investigación (Parcial)
    - Actas de notas finales de los cursos del Proyecto MATEM. (*Valor científico-cultural*).
    - Expediente clínico odontológico de sedes y recintos universitarios. (*Valor científico-cultural*).
    - Expediente de gestión curricular. (*Valor científico-cultural*).
    - Expediente de procesos de autoevaluación y gestión de la calidad y excelencia académica de carreras de grado. (*Valor científico-cultural*).
    - Expedientes de coordinación de los cursos del Proyecto MATEM.
    - Informe final de labores de los docentes del Programa de Educación Abierta. (*Valor científico-cultural*).
    - Trabajos finales de graduación/Anteproyectos (que se encuentran en la Biblioteca Luis Demetrio Tinoco). (*Valor científico-cultural*).

Además de estos informes de valoración y tablas de plazos de conservación, la UCR cuenta con diferentes comunicados para las instancias universitarias, los cuáles son remitidos a través de circulares, que permiten mejorar los procesos relacionados con la evaluación documental.

También, ofrece a la comunidad universitaria, los siguientes procesos, junto con sus respectivos anexos descargables (AUROL, 2017-a):

- *Identificación Archivística para la Universidad de Costa Rica*: este proceso se lleva a cabo a través de tres fases que posibilita "determinar el contexto de la unidad, así como las series documentales producto de sus procesos sustantivos: Identificación de la unidad productora, análisis de procesos e identificación de las series documentales. Para llevarla a cabo es necesario que las unidades soliciten la asesoría correspondiente al personal del Archivo Universitario" (CUSED, 2018-a, p.7).
- *Valoración de documentos en la Universidad de Costa Rica*: para llevar a cabo la valoración documental, primero el AUROL brinda asesoría a las unidades que lo soliciten, para realizar el proceso de identificación (según el procedimiento anterior); luego la unidad remite a la CUSED la tabla de plazos de conservación. La CUSED, por su parte, valora las series documentales y establece las vigencias de conservación correspondientes, ya sea para conservación, transferencia o eliminación de los

documentos. Finalmente, el AUROL elabora el informe de valoración para que sea aprobado por la CUSED, quien lo comunica a la Unidad solicitante. En el caso de tablas de plazos generales, son elaborados también por el AUROL con el apoyo de la CUSED y los profesionales de distintas unidades productoras (CUSED, 2018-b)

- *Eliminación de documentos de la Universidad de Costa Rica*: para llevar a cabo la eliminación de documentos, en primer lugar la unidad lleva a cabo la selección de los documentos, agrupándolos documentos según las vigencias señaladas en el Informe de valoración y luego elabora el acta de eliminación de documentos, la cual remite a la CUSED. Para concluir, la unidad lleva a cabo la eliminación transformando los documentos en material no legible y por último, lo recicla (CUSED, 2018-c).

En segunda instancia, las directrices generales en materia archivística, excepto las relacionadas con la evaluación de documentos, son emitidas gracias al trabajo del Comité Técnico del SAU. Dentro de estas disposiciones se encuentran disponibles para consulta, las siguientes:

- Directrices
    - Lineamientos generales que regulan la firma autógrafa y la firma digital en los documentos que se producen o reciben en la Universidad de Costa Rica (2020).
    - Directriz para la elaboración de cartas, circulares y memorandos oficiales (2014).
    - Resolución de Rectoría R-188-2021: Resolución de Rectoría R-188-2021 Se comunica el Procedimiento para la gestión de las actas y expedientes de sesiones de los órganos colegiados de la Universidad de Costa Rica (2021).
    - Procedimiento para la gestión de las Actas y Expedientes de Sesiones de los Órganos Colegiados de la Universidad de Costa Rica (2021).
- Circulares
    - Circular SAU-CT-1-2020 Se comunica el deber de imprimir, firmar y sellar las actas de sesiones de los órganos colegiados universitarios, aunque las sesiones se realicen de manera virtual.
    - Circular SAU-CT-2-2020 Aclaración y adición a la Circular SAU-CT-1-2020 con la que se comunica el deber de imprimir, firmar y sellar las actas de sesiones de los órganos colegiados universitarios, aunque las sesiones se realicen de manera virtual.

- Circular SAU-CT-4-2020 Responsabilidad de las autoridades y demás funcionarios sobre el uso y conservación de los documentos dentro y fuera de las instalaciones universitarias
- Circular SAU-CT-5-2020 Solicitud de comunicar al Comité Técnico previamente la emisión de cualquier lineamiento o directriz que afecte directa o indirectamente la gestión de documentos en formato físico o electrónico.
- Circular SAU-CT-6-2020 Enlaces para consultar las guías oficiales elaboradas por el Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT), el video tutorial para firmar documentos digitalmente desde el Sistema de Gestión de Documentos Institucional (SiGeDI) y el enlace para la validación de documentos firmados digitalmente.
- Circular SAU-CT-1-2021 Instructivo para la configuración del programa Adobe Acrobat Reader DC y para la validación de la firma digital mediante la plataforma de Central Directo del Banco Central de Costa Rica.

Las directrices emitidas por el Comité Tecnico, deben ser acatadas y aplicadas por las distintas instancias universitarias. Otros procesos técnicos archivísticos, necesarios para mejorar la gestión de documentos de archivos de la Universidad, y sus respectivos instrumentos (ejemplo, clasificación documental), se encuentran en proceso de construcción y aprobación, por las instancias correspondientes.

2.2.7. Recurso humano

La UCR cuenta con recurso humano dedicado a la administración de los distintos archivos que forman parte del SAU. Las personas designadas como encargadas de los archivos, son en su gran mayoría archivistas, aunque se pueden encontrar algunos profesionales con formación en otras ciencias, como la administración.

De esta forma, actualmente la Universidad tiene el siguiente personal (Tabla 3):

Tabla 3. *Cantidad de personal asignado a los Archivos de la Administración.*

Unidad	Personas asignadas	Unidad	Personas asignadas
AUROL	8	Oficina de Recursos Humanos	3
Centro de Evaluación Académica	1	Oficina de Registro e Información	2
Centro de Informática	1	Oficina de Servicios Generales	1
CELEQ	1	Oficina de Suministros	1
Consejo Universitario	3	Rectoría	4
Escuela de Artes Musicales	1	Sede del Atlántico	1
Escuela de Ingeniería Civil	1	Sede de Guanacaste	1
Facultad de Ciencias Sociales	1	Sede de Occidente	1
Facultad de Derecho	1	Sede del Pacífico	1
Instituto de Investigaciones Psicológicas	1	Sede del Sur	1
LANAMME	1	Sede Interuniversitaria de Alajuela	1
Oficina de Administración Financiera	2	Sistema de Estudios de Posgrado	2
Oficina de Asuntos Internacionales y Cooperación Externa	1	Sistema Editorial de Difusión de la Investigación de la UCR	1
Oficina de Becas y Atención Socioeconómica	1	Vicerrectoría de Acción Social	2
Oficina de Bienestar y Salud	1	Vicerrectoría de Administración	1
Oficina de Contraloría Universitaria	1	Vicerrectoría de Docencia	2
Oficina de Comunicación Institucional	1	Vicerrectoría de Investigación	2
Oficina de Planificación	1	Vicerrectoría de Vida Estudiantil	1
		Total	**56**

Fuente: Elaboración propia a partir de AUROL, 2017-c.

2.2.8. Servicios archivísticos en la Universidad de Costa Rica

Los servicios archivísticos especializados que se ofrecen en la UCR, son brindados por el AUROL (AUROL, 2009) y se presentan a continuación:

- Acceso a su sitio web: http://www.archivo.ucr.ac.cr
- Base de datos fotográfica.
- Bibliografía especializada sobre la historia de la Universidad de Costa Rica.
- Consulta en sala.
- Copias digitales de sus fotografías.
- Exposiciones temporales.
- Facilidades para la realización de prácticas de los estudiantes de Archivística y carreras afines.
- Lista de las transferencias recibidas y acceso a los inventarios.
- Información sobre el Archivo Universitario Rafael Obregón Loría.
- Orientación y referencia, localización y préstamo de documentos y fotografías.
- Transferencia de datos vía electrónica.
- Visitas guiadas.

Así también, desde el AUROL se ofrece el servicio de asesoría archivística para las distintas unidades académicas, administrativas y de investigación de la UCR, que lo soliciten. Además, se brinda acceso a la fonoteca universitaria y a la colección digitalizada del Semanario Universidad.

Por su parte, los distintos archivos del SAU, ofrecen servicios básicos generales como atención de consultas y préstamo de documentos.

2.3. Análisis del escenario tecnológico

Para diseñar y poner en funcionamiento un Archivo Digital institucional, resulta esencial conocer el escenario tecnológico: cómo se organiza la institución en esta materia, cuál es la normativa vigente y cuáles son las funciones de las instancias involucradas.

De esta manera, se presentan aspectos e instancias relacionadas con el ámbito tecnológico, que le permiten a la Universidad de Costa Rica el desarrollo óptimo de sus funciones.

2.3.1. Centro de Informática

Según la Resolución R-96-2018, el Centro de Informática (CI) es la oficina administrativa coadyuvante de la Rectoría que funciona como instancia estratégica, asesora, técnica y de servicio, para asegurar que las TIC estén acordes con los objetivos institucionales (Rectoría, 2018, p.3).

Dentro de las principales funciones asignadas al Centro de Informática, se encuentran (Rectoría, 2018, p.3-4):

1. Participar con la Administración Superior en la elaboración de planes y políticas institucionales relacionadas con el desarrollo y aplicación de las TIC.
2. Emitir lineamientos, directrices, estándares y normas en materia de TIC.
3. Brindar asesoría técnica a la comunidad universitaria, incluyendo al Consejo Universitario, Rectoría, Vicerrectorías, Comité Gerencial de Informática, sedes y recintos, facultades y escuelas y otras entidades institucionales, que lo requieran.
4. Proporcionar los servicios de TIC a la comunidad universitaria.
5. Promover y desarrollar investigación sobre TIC para innovar en este campo.
6. Mantener la operación continua y eficiente en los productos y servicios de TIC ofrecidos a la comunidad universitaria.
7. Participar activamente en las comisiones, comités o programas y proyectos institucionales en los que se involucre por designación, iniciativa o interés.

El CI está conformado de la siguiente manera (Rectoría, 2018, p.4-15):

1. Jefatura: conformada por el Jefe y subjefe, quiénes son nombrados y removidos por la persona que ocupa la Rectoría. El jefe tiene como responsabilidades la toma de decisiones al mayor nivel del centro, la delegación de tareas y la gestión de todos los procesos administrativos, de soporte y sustantivos.
2. Bloque Administrativo: encargado de las actividades financieras, de recursos humanos, transportes, mensajería, calidad, entre otras, las cuales son importantes para la administración del CI.
3. Bloque de Desarrollo: dedicado a la investigación y el desarrollo de los proyectos de innovación y mejora de la infraestructura de las TIC en la institución, así como el desarrollo de sistemas de información y aplicaciones.
4. Bloque de Gestión: sus funciones incluyen la relación hacia los usuarios de los servicios de TIC, la administración de estos servicios, su manejo diario y su mejora. También incluye el soporte de los aspectos relacionados con las comunicaciones e infraestructura tecnológica de la UCR.
5. Consejo Técnico Asesor: es el órgano interno del CI que asesora a la jefatura. Se encarga de gestionar las actividades y proyectos de investigación o acción social que se desarrollen. Entre sus funciones están apoyar en la elaboración del Plan Estratégico y colaborar en la elaboración y ejecución del plan de trabajo del CI.

A raíz de lo expuesto anteriormente, es importante rescatar que el proyecto para desarrollar un Archivo Digital, está relacionado directamente con las funciones que debe desempeñar el Centro de Informática, ya que dicho proyecto tiene un amplio componente archivístico y tecnológico.

El Archivo Digital tendrá un alcance institucional y se desprende del planteamiento estratégico desarrollado por la CIADi, comisión en la cuál participa directamente el CI, al haber sido designado por la Rectoría.

2.3.2. Comité Gerencial de Informática

El Comité Gerencial de Informática (CGI) es la instancia institucional, con dependencia directa de la Rectoría, que tiene por objetivo asesorar en asuntos estratégicos relativos a las TIC, priorizando el Portafolio de Proyectos de TIC, para impulsar el equilibrio entre la asignación de

recursos y la atención de necesidades universitarias (Rectoría, 2013, p.2). Este órgano colegiado se encuentra en funcionamiento desde el año 2013.

De esta forma, el CGI está integrado por el Rector, quien preside; los vicerrectores; el director del CI; el director de la Oficina de Planificación Universitaria (OPLAU) y un representante de las Sedes Regionales (Rectoría, 2013, p.2).

Asimismo, el CGI cuenta con el apoyo de un consejo técnico asesor, conformado por el director del CI, el directo de la Escuela de Ciencias de la Computación e Informática, un representante de la Vicerrectoría que corresponda según el tema a tratar y dos expertos técnicos con experiencia en el tema a desarrollar (Rectoría, 2013, p.2-3).

Entre las funciones que debe desarrollar el CGI se encuentran (Rectoría, 2013, p.3-4):

1. Impulsar el desarrollo del plan institucional de las TIC.
2. Proponer políticas institucionales en cuanto a las TIC.
3. Analizar y emitir criterio sobre asuntos técnicos en TIC, como la adquisición e implementación de soluciones tecnológicas, contratación externa y *outsourcing*, desarrollo de sistemas de información, administración de sistemas de información y sistemas informáticos, entre otros.
4. Recomendar prioridades institucionales relacionadas con el Portafolio de Proyectos de TIC.

Según lo explicado anteriormente, el Comité Técnico Gerencial tendrá un alto grado de decisión en el desarrollo, puesta en marcha y mantenimiento a largo plazo del Archivo Digital, puesto que será el órgano que deberá definir la prioridad que tendrá este proyecto para la institución. Al respecto, la MAP. Laura Castro Jiménez, coordinadora del Área de Desarrollo de Sistemas del CI, señala que el Centro de Informática presenta proyectos al CGI para que, este órgano defina las prioridades institucionales, pero que una vez que CGI prioriza un proyecto, el CI debe atenderlo (CIADi, 2022, p.7).

2.3.3. Infraestructura y plataforma tecnológica institucional

Para hacer posible el cumplimiento de sus objetivos institucionales, la Universidad de Costa Rica ha tenido que abordar de forma integral los cambios y retos que se presentan de forma intrínseca por el rápido avance de la tecnología.

Es por esto, que ha sido necesario desarrollar distintos marcos normativos que permitan definir de forma clara, las medidas que se deben tomar con el fin de satisfacer las necesidades de la población universitaria en materia de TIC.

Con estas acciones, la institución busca facilitar la ejecución de sus funciones en un ambiente tecnológico seguro, que permitan dar continuidad a los servicios, al tiempo que se pueda asegurar la transparencia y la rendición de cuentas. De esta manera, a continuación se presenta el contexto de la UCR en cuanto a su infraestructura y plataforma tecnológica.

- **Políticas institucionales sobre tecnologías**

A nivel general, la UCR cuenta con las Políticas Institucionales 2021-2025 y el Plan Estratégico Institucional 2021-2025.

Las Políticas Institucionales 2021-2025 están estructuradas en 11 Ejes:

- Eje I. Universidad y sociedad
- Eje II. Excelencia académica
- Eje III. Cobertura y equidad
- Eje IV. Regionalización
- Eje V. Posgrado
- Eje VI. Talento humano
- Eje VII. Gestión universitaria
- Eje VIII. Igualdad e inclusividad
- Eje IX. Bienestar y vida universitaria
- Eje X. Compromiso ambiental
- Eje XI. Independencia de gobierno, organización y finanzas

Cada uno de estos ejes enmarca políticas específicas y sus respectivos objetivos para lograr solventar las principales problemáticas institucionales que enfrenta la UCR.

Dentro de las políticas específicas relacionadas con el tema de las TIC, se pueden resaltar las siguientes (Tabla 4):

Tabla 4. *Políticas Institucionales 2021-2025 relacionadas con TIC en la UCR.*

Eje	Políticas	Objetivos
Eje I. Universidad y sociedad	1.4 Propiciará la transferencia del conocimiento generado en las actividades de docencia, investigación y acción social, de manera que contribuya con el desarrollo científico, tecnológico, cultural, social y ambiental del país.	1.4.1 Propiciar el acceso abierto a los datos y a la información institucional, mediante los mecanismos de comunicación oficial, con el propósito de poner a disposición de la comunidad nacional e internacional la producción académica y la gestión universitaria.
		1.4.2 Proteger el conocimiento generado en las actividades de docencia, investigación y acción social cuando sea susceptible a la aplicación de las leyes nacionales e internacionales de propiedad intelectual u otro tipo de instrumentos válidos legalmente.
Eje II. Excelencia académica	2.6 Aumentará la integración tecnológica en todos sus ámbitos, al igual que la actualización constante, para su aplicabilidad en las actividades sustantivas.	2.6.1 Optimizar el uso de las herramientas tecnológicas de información y comunicación (TIC), como instrumentos facilitadores de la docencia, investigación, acción social y la toma de decisiones.
		2.6.2 Fomentar el aprendizaje mediado por las tecnologías de información y comunicación (TIC), de manera que favorezca el éxito académico.
Eje VII. Gestión universitaria	7.3 Reforzará una cultura de transparencia, rendición de cuentas y participación de la comunidad universitaria, mediante mecanismos de control y evaluación para un uso racional de los recursos.	7.3.1 Crear y fortalecer los sistemas automatizados, que promuevan una cultura de transparencia y rendición de cuentas.
		7.3.2 Revisar y mejorar los mecanismos de evaluación y control, orientados a la rendición pública de cuentas de las autoridades universitarias en los ámbitos interno y externo.
		7.3.3 Velar porque la gestión universitaria responda a los objetivos propuestos y de acuerdo con los recursos asignados.
		7.3.4 Fortalecer los mecanismos de acceso al marco normativo y a la información de la gestión universitaria.
	7.4 Diseñará y desarrollará los mecanismos de integración de la información universitaria, de	7.4.1 Analizar y automatizar los procesos estratégicos institucionales que aún se administren de forma manual o semiautomática, para lograr mayor eficacia y eficiencia.

	forma estandarizada, segura e interoperable, que apoyen la toma de decisiones estratégicas institucionales.	7.4.2 Propiciar la mejora, investigación, seguridad y automatización de los procesos universitarios, que permitan la implementación de herramientas tecnológicas de información y comunicación (TIC) que impacten en el quehacer institucional.
		7.4.3 Promover la alfabetización informacional, con una perspectiva crítica, en la comunidad universitaria.
		7.4.4 Impulsar procesos de integración de los sistemas informáticos institucionales y mejorar su capacidad para compartir datos que permitan generar información para la toma de decisiones.
		7.4.5 Fomentar las buenas prácticas para la conservación y preservación del patrimonio documental y el acervo bibliográfico institucional, en formato impreso y digital.

Fuente: Elaboración propia a partir de Consejo Universitario, 2020.

Por su parte, el Plan Estratégico Institucional (PEI) 2021-2025, se estructura en 6 ejes:

- Eje 1: Excelencia académica
- Eje 2: Desarrollo territorial y sedes
- Eje 3: Inclusión social y equidad
- Eje 4: Internacionalización
- Eje 5: Excelencia en la gestión
- Eje 6: Vida universitaria

Los objetivos estratégicos relacionados con las TIC en el PEI son (Tabla 5):

Tabla 5. *Objetivos Estratégicos del PEI 2021-2025 relacionados con TIC en la UCR.*

Eje	Objetivo Estratégico	Estrategia	Meta
Eje 5: Excelencia en la gestión	5.1 Fortalecer acciones de planificación institucional que contribuyan a la sostenibilidad, la transparencia y el equilibrio económico.	5.1.3 Fortalecer, integrar y facilitar el acceso externo a la información institucional.	5.1.3.1 Poner a disposición de la sociedad los resultados producto del quehacer académico y la información general de la Universidad.
	5.2 Implementar mecanismos y acciones para simplificar, flexibilizar, descentralizar	5.2.1 Mejorar la gestión académica y administrativa	5.2.1.1 Agilizar y simplificar diferentes procesos y trámites relacionados con las áreas sustantivas y de apoyo.

	y automatizar los procesos institucionales, con el fin de agilizar la gestión académica y la rendición de cuentas.	5.2.2 Fortalecer, integrar y facilitar el acceso a los sistemas de información institucional de uso interno	5.2.2.1 Diseñar sistemas unificados de información accesibles para la comunidad universitaria, orientados a la transparencia y la rendición de cuentas.

Fuente: Elaboración propia a partir de Universidad de Costa Rica, 2021.

Resulta importante destacar estas políticas y estrategias institucionales generales, ya que es a partir de ellas que se dirigen las líneas de actuación, que permiten asignar recursos y redirigir esfuerzos para mejorar la infraestructura y la plataforma tecnológica institucional que requiere la Universidad.

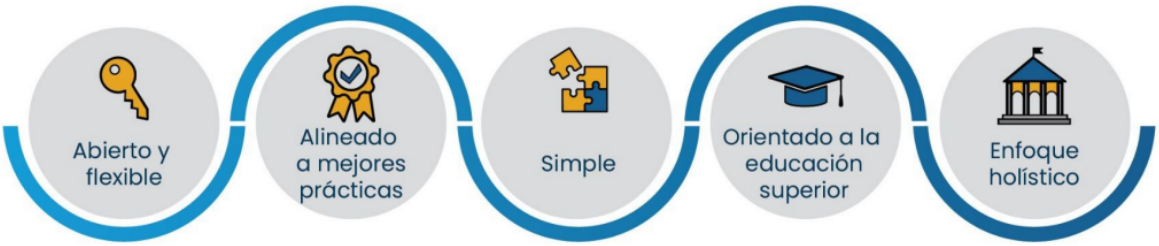
De manera específica, la institución cuenta con el Marco de Gobierno y Gestión de TI de la Universidad de Costa Rica, el cual (Centro de Informática de la UCR, 2021-a, p.1):

> Es un marco orientador del gobierno y gestión de la tecnología de información en la Institución, alineado a la estrategia institucional, que garantiza un balance adecuado de las inversiones, la organización de recursos y actividades sustantivas, respetando la normativa institucional y nacional, basado en las buenas prácticas y ajustado al contexto, tamaño, naturaleza, restricciones y estrategia institucional. Su principal objetivo es crear valor a la Institución, a través de la obtención de beneficios con las TI, a un costo favorable, mientras se optimiza el riesgo, soportados por un conjunto de elementos como estructuras, procesos y mecanismos relacionados entre sí.

Este documento, propone una estructuración basada en cinco principios rectores y seis objetivos de gobierno, cada uno de los cuáles se subdividen en objetivos de gestión, y estos a su vez en actividades, las cuales permitirán cumplir con los objetivos propuestos (Centro de Informática de la UCR, 2021-a).

Los cinco principios en los que se basa el Marco, y que dirigen las propuestas son los siguientes (figura 6):

Figura 6. *Principios del Marco de Gobierno y Gestión de TI de la UCR.*



Fuente: Centro de Informática UCR, 2021-a, p.13.

Por su parte, los objetivos de gobierno y gestión de TI, "son las metas o fines hacia los cuales se dirigen las acciones que buscan alcanzar los objetivos estratégicos de la institución" (Centro de Informática de la UCR, 2021-a, p.15) y se presentan en la figura 7:

Figura 7. *Objetivos de gobierno y gestión de TI del Marco de Gobierno y Gestión de TI de la UCR.*

Fuente: Centro de Informática UCR, 2021-a, p.15.

De esta forma, a continuación se presenta un cuadro resumen en el que se describen brevemente los objetivos de gobierno y gestión de TI presentes en el Marco de Gobierno y Gestión de TI de la Universidad de Costa Rica (Tabla 6).

Tabla 6. *Resumen de objetivos de gobierno y gestión de TI en el Marco de Gobierno y Gestión de TI de la UCR.*

Objetivos de gobierno	Objetivos de gestión	Prácticas
1. Alineación Estratégica y Operativa Asegurar, de manera óptima, que lo planificado y desarrollado por TI está en conformidad o correspondencia con lo definido por la administración superior de la institución, de tal forma que se garantice que TI contribuye satisfaciendo las necesidades y expectativas institucionales.	**Marco Estratégico** Enfoque uniforme, integrado y alineado con la dirección de la institución.	Definir el ADN estratégico de TI
		Fijar los principios del marco estratégico de TI
		Alinear los ejes transversales de TI con los ejes transversales institucionales
		Determinar las directrices de TI.
		Establecer los ejes de conocimiento de TI.
	Planificación estratégica Gestionar y dirigir los recursos de TI para que permita alcanzar sus objetivos Balance óptimo entre requerimientos, capacidad financiera y las oportunidades que brindan las tecnologías existentes e innovadoras	Analizar las tendencias de la educación superior referentes al desarrollo e innovación tecnológica.
		Evaluar el entorno institucional y su situación actual con un enfoque de TI
		Establecer prioridades
		Definir las estrategias de TI
	Planificación operativa Plasmar las estrategias por seguir sobre las labores operacionales de TI. Darles seguimiento mediante un plan anual operativo, acorde con la prioridad establecida estratégicamente.	Gestionar los servicios de TI
		Gestionar la plataforma tecnológica.
		Gestionar el recurso humano de TI
		Gestionar la entrega de valor de los servicios de TI
		Gestionar el portafolios de proyectos TI
		Elaborar el plan de trabajo operativo
2. Optimización y gestión del riesgo de TI Producir información que apoye la toma de decisiones orientada a ubicar a la institución en un nivel de riesgo aceptable y así promover, de manera razonable, el logro de los objetivos institucionales.	**Continuidad de los servicios de TI** La institución debe mantener una continuidad razonable de sus procesos y su interrupción no debe afectar significativamente a los usuarios.	Planificar los requerimientos de continuidad
		Diseñar y ejecutar los mecanismos y procedimientos de continuidad de los servicios de TI adecuados y medibles
		Evaluar y realizar las mejoras para favorecer la continuidad de los servicios de TI

Objetivos de gobierno	Objetivos de gestión	Prácticas
	Gestión de riesgos Asistir a la institución para integrar la gestión del riesgo en todas sus actividades y funciones significativas. La eficacia de la gestión del riesgo dependerá de su integración en la gobernanza de la administración superior, incluyendo la toma de decisiones.	Identificar el riesgo de TI.
		Analizar el riesgo de TI
		Evaluar el riesgo de TI
		Administrar el riesgo de TI
		Monitorear y revisar
		Comunicar y socializar
3. Optimización de recursos Disponer de manera óptima de los recursos de tecnologías de información, de tal forma que se obtenga el mayor beneficio para la institución y la posibilidad de realizar cambios futuros.	**Gestión financiera** Fomentar la rendición de cuentas de costos y valor agregado a la institución de los productos y servicios de TI de forma transparente. Promover el uso eficaz y eficiente de los recursos relacionados con TI	Alinear la gestión financiera de TI institucionalmente
		Priorizar la asignación de recursos TI
		Planificar y formular el presupuesto
		Dar seguimiento al presupuesto
	Organización TI Diseñar las estructuras organizativas relacionadas con TI con responsabilidades claras y definir la composición de dichas estructuras, las competencias y habilidades requeridas para cada rol.	Definir e implementar estructuras organizativas
		Establecer roles y responsabilidades de TI
		Identificar al personal clave de TI
		Mantener actualizadas las habilidades y competencias.
		Gestionar al personal contratado
	Gestión del conocimiento Proporcionar el conocimiento e información relevante para la gestión de TI y facilitar la toma de decisiones relacionadas con el gobierno de TI.	Mejorar la calidad y el uso de la información de gestión de TI
		Crear un entorno de uso, desarrollo e intercambio de conocimiento
		Evaluar y mantener la información de gestión de TI

Objetivos de gobierno	Objetivos de gestión	Prácticas
	Gestión de proveedores y aliados Supervisar que los contratos y el desempeño de los proveedores de TI se gestionen de manera adecuada. Seleccionar los proveedores y crear relaciones estrechas y colaborativas que permitan agregar valor, reducir riesgos y consolidar aliados estratégicos.	Identificar y seleccionar proveedores de TI
		Gestionar contratos y relaciones con los proveedores y aliados
		Evaluar el desempeño de proveedores y aliados
	Gestión de la capacidad de TI Proporcionar mecanismos para respaldar la prestación de los servicios TI, basados en la administración adecuada de la capacidad de la infraestructura TI, para que sea suficiente, efectiva y correctamente dimensionada a la planificación de la demanda	Evaluar la capacidad actual
		Planificar e implementar los cambios en la capacidad
		Monitorear la capacidad de la infraestructura
	Arquitectura empresarial Establecer por medio de dominios de arquitectura, los componentes que conforman la Institución a nivel de tecnologías de información, así como sus interrelaciones, con la finalidad de: aumentar la agilidad en respuesta a la estrategia de TI institucional, mejorar la calidad de la información y optimizar recursos por medio de la reutilización de componentes.	Definir la línea base de la arquitectura
		Diseñar la base para la ejecución
		Implementar, revisar y mantener la arquitectura
4. Gestión de Servicios de TI Dirigir, evaluar y dar seguimiento a las actividades que permitan facilitar la integralidad de la cadena de valor del servicio TI en relación con las prácticas o procesos de las instituciones universitarias, de tal forma que los servicios de TI funcionen eficientemente y se alineen con los objetivos de cada institución.	**Estrategia del servicio de TI** Mecanismos para obtener, entender e interpretar correctamente la estrategia institucional con respecto al uso de las tecnologías de información. Insumo para el diseño de una combinación de servicios adecuados para soportar dicha estrategia, estableciendo la visión de arquitectura empresarial con respecto a servicios de TI.	Alinear los servicios TI con los procesos institucionales
		Gestionar los riesgos asociados a los servicios TI
		Establecer los lineamientos de arquitectura de los servicios
		Definir el portafolio de servicios TI
		Establecer el modelo de gestión

Objetivos de gobierno	Objetivos de gestión	Prácticas
	Diseño de servicios Guía u orientación para diseñar y desarrollar servicios de TI, tanto para servicios nuevos como cambios en los existentes, antes de su paso a producción; incluye cambios y mejoras necesarias para mantener o incrementar el valor para los usuarios	Diseñar servicios
		Diseñar los procesos para la gestión de los servicios
		Diseñar los habilitadores de los procesos (herramientas, roles, estructuras organizativas)
		Diseñar el ciclo de vida del servicio
	Construcción de servicios Garantizar la disponibilidad de los componentes de servicio, como hardware, software, información, personal capacitado, documentación relevante, entre otros, cuándo y dónde se necesite.	Construir servicios
		Gestionar el cambio organizacional
		Adquirir recursos o servicios externos
		Realizar validación y pruebas para asegurar la calidad de los servicios antes de ponerse en producción
		Desplegar servicios
	Entrega y operación Gestionar y garantizar que los servicios que TI brinda a la institución se entreguen y cuenten con el soporte adecuado para cumplir con las expectativas de los usuarios involucrados, establecidos en los acuerdos de niveles de servicio y criterios de calidad acordados.	Gestionar las solicitudes de servicio
		Gestionar los incidentes
		Gestionar los problemas
		Gestionar la disponibilidad, seguridad, capacidad y continuidad de servicios TI
5. Mejora continua Velar por el cumplimiento de los procesos y servicios brindados por TI, así como los componentes del gobierno de TI, en referencia a la alineación con los objetivos planteados por la institución y la gestión de TI.	**Control interno** Supervisar, evaluar y ajustar las medidas que permitan mantener un apropiado control de los procesos soportados por la gestión de TI.	Dar seguimiento a las actividades de control
		Propiciar la autoevaluación del sistema control interno
		Identificar y reportar las deficiencias de control
	Cumplimiento Identificar y velar por el cumplimiento del marco jurídico atinente a la gestión de TI Evitar posibles conflictos legales que puedan ocasionar perjuicios para la institución.	Identificar la normativa de acatamiento aplicable a TI
		Velar por el cumplimiento de los requisitos internos y externos para TI

Objetivos de gobierno	Objetivos de gestión	Prácticas
	Desempeño de TI Establecer, dar seguimiento y evaluar una cultura de mejora continua en TI. Medición en la eficiencia de los procesos y la aptitud, posibilidad y habilidad de TI para aprender y lograr un crecimiento.	Instaurar los mecanismos que apoyen la observancia del desempeño de TI
		Analizar e informar sobre el desempeño de TI
	Calidad de los servicios de TI: Asegurarse de que los servicios de TI provean valor a la institución facilitando los resultados que se espera generar. Los servicios deben ser revisados y evaluados en su desempeño y rendimiento constantemente para garantizar que siguen creando valor.	Establecer los factores críticos de éxito para los servicios
		Establecer los indicadores claves de desempeño
		Recolectar, agrupar, correlacionar los datos de la medición
		Analizar la desviación con respecto a los factores críticos de éxito (FCE)
		Implementar mejoras para corrección de las posibles desviaciones
6. Seguridad de la información Propiciar, de manera razonable, la confidencialidad, integridad, disponibilidad, autenticidad de la información, conservación, trazabilidad, acceso y servicios utilizados en medios electrónicos	**Seguridad de la información de TI** Controles para establecer que la información custodiada, almacenada, transferida, procesada e incluso eliminada cumpla los requerimientos de confidencialidad, integridad, disponibilidad y autenticidad establecida en la normativa de seguridad de la información institucional.	Implementar un marco de seguridad de la información
		Gestionar riesgos ante amenazas
		Planificar y detectar procesos de la gestión de la seguridad de TI
		Implementación de la gestión de proyectos de la seguridad de TI

Fuente: Elaboración propia a partir de: Centro de Informática de la UCR, 2021.

- **Administración de sistemas de información**

El Centro de Informática de la Universidad de Costa Rica (2016, p.3) , es el principal encargado de la administración de los sistemas de información de la institución, pues su función principal es la de:

> impulsar y potenciar que la información, la tecnología y las comunicaciones soporten los objetivos de la Institución (docencia, investigación y acción social) y el quehacer administrativo de la misma, hacia una posición de vanguardia y excelencia; mediante la planificación, desarrollo, mantenimiento, control y seguimiento de la infraestructura de TIC de la Universidad; y la definición, desarrollo, mantenimiento y actualización de los servicios de TIC que se brindan; además de la generación de directrices, normativas y lineamientos relacionados con su ámbito de acción, incluyendo adquisiciones, riesgos y seguridad (física y lógica).

Para llevar a cabo la administración de los sistemas de información, el Centro de Informática de la UCR trabaja de forma estructurada, y desde distintas líneas de acción. Algunas de la que se pueden destacar son:

i. **Seguridad de la información**

En el año 2015, mediante la Resolución R-102-2015, emitida por la Rectoría, se aprueban las "Directrices de Seguridad de la Información de la Universidad de Costa Rica", la cuáles tienen como finalidad la protección de la información que pertenece a la Universidad, así como aquella que está en su custodia (Rectoría de la Universidad de Costa Rica, 2015).

Estas Directrices, son de aplicación obligatoria para la institución y en ellas se definen objetivos básicos para la seguridad de la información, como los son, por ejemplo: guía general de conductas en materia de seguridad de la información; responsabilidad sobre protección y manejo adecuado de los recursos informáticos; riesgos de seguridad de la información y medidas para mitigarlos y/o administrarlos; toma de decisiones responsables para la protección de los sistemas y recursos de información; seguridad de la información; generar conciencia sobre la importancia de la seguridad de la información; toma de decisiones para la protección de los sistemas de información y el establecimiento de controles adecuados a las necesidades de la Universidad; cumplimiento de requisitos legales, reglamentarios y contractuales; requerimientos de

capacitación, manejar, prevenir y detectar en su debido tiempo instrucciones maliciosas, acciones para mantener la continuidad de los servicios críticos de la Universidad; tomar acciones en caso de violación a los Directrices Tecnicas de Seguridad de Información y brindar una guía básica para la ejecución de auditorías de sistemas, pruebas de intrusión y análisis y valoración de riesgos (Rectoría de la Universidad de Costa Rica, 2015).

Además de esto, las directrices ofrecen un marco de acción para garantizar la seguridad de la información que incluye la "Infraestructura Integral de Seguridad de la Información", la cual (Rectoría de la Universidad de Costa Rica, 2015, p.4-5):

> se refiere tanto a la infraestructura técnica-informática, como a la normativa aprobada y exigible en la Universidad en materia de seguridad, al proceso de valoración de riesgos, a los programas de sensibilización y capacitación, que deben ser adoptados como una práctica dentro de la cultura organizacional de la Institución, al trabajo conjunto de todos los actores dentro del proceso de Seguridad de la Información, a la verificación de cumplimiento integral y por último, a la labor continuada y sinérgica de todos estos componentes.

Para 2016, se establece el "Plan Estratégico Institucional en Tecnologías de Información 2016-2020" (PEITI), el cual "surge a partir de la solicitud del Consejo Universitario (sesión No. 5740, artículo 3, encargo 2k), con el fin de contar con lineamientos claros para determinar hacia dónde se dirigirá la Universidad durante este quinquenio, con miras a mejorar la calidad de los servicios" (Comité Gerencial de Informática, 2016, p.4).

En el PEITI, dentro del Eje 5 Gestión Institucional, en su objetivo estratégico 5.1, se propone dentro de sus estrategias "Mejorar la infraestructura, gobernabilidad, seguridad y calidad de las tecnologías de información y comunicación de la Institución" (Comité Gerencial de Informática, 2016, p.4).

En el año 2020, el Centro de Informática de UCR, emite el "Lineamiento General para la Gestión de Seguridad de la Información en los Sistema de Información", cuya obligatoriedad entró a regir en 2021, el cual incluye los siguientes lineamientos generales (Tabla 7):

Tabla 7. *Lineamientos generales para la gestión de la información en los sistemas informáticos de la UCR.*

1. Toda la información que se almacena, transita, es recopilada, distribuida, reproducida, procesada y/o creada en los sistemas de información de la UCR, será considerada, para efectos de la gestión en seguridad de la información, como propiedad de la Universidad, salvo que el ordenamiento jurídico establezca lo contrario. Por lo tanto, el personal usuario no podrá, bajo ninguna circunstancia, transmitirla de ninguna manera a terceros, modificarla ni eliminarla, sin contar con autorización expresa de la autoridad universitaria correspondiente.	**4.** Deberán seguirse estrictamente todos los procedimientos y mecanismos aprobados por los sistemas de información, tendientes a garantizar: a) El ingreso seguro y controlado de datos a los sistemas de la UCR b) La protección de los datos. c) El procesamiento correcto de los mismos d) El almacenamiento de los datos e) La validación de las salidas f) Confidencialidad, integridad y disponibilidad de la información.
2. Toda información producida, generada o creada por los funcionarios de la UCR en sus quehaceres para con ésta, es información que pertenece a la Universidad. La UCR será la propietaria de todos los derechos de disposición y patrimoniales sobre la misma y podrá utilizarla, como así lo requiera. No así los funcionarios, quienes no podrán disponer de dicha información para efectos no relacionados con sus labores, a menos que cuenten con autorización válidamente emitida y por escrito, para ello, siempre que sean usos del quehacer Universitario.	**5.** Las personas designadas para hacer uso y manipulación de la información, deberán implementar estrictamente los controles para el acceso y demás controles aplicables a las bases de datos de la UCR, formalmente aprobados por la Universidad.
3. Los responsables del uso y manipulación de la información se identifican de la siguiente manera: ● Responsable de Seguridad: con la finalidad de hacer un seguimiento y coordinar todas las iniciativas puestas en marcha por la organización en materia de Seguridad de la Información. ● Responsable de Información: especialmente cuando se trata con información específica que es gestionada a través de diferentes entornos. ● Responsable de ámbito: en el caso de que se ponga en marcha iniciativas en el ámbito lógico, físico, legal y organizativo ● Persona Usuaria: Miembro de la comunidad universitaria que tiene acceso a la información de los sistemas de la Universidad, para realizar actividades propias de sus actividades labores.	**6.** Será obligación de toda persona usuaria, reportar por los medios y canales seguros provistos por la UCR, cualquier situación que pudiese comprometer la confidencialidad e integridad (es decir, la exactitud, fidelidad y veracidad) de la información de la UCR y/o en su custodia. **7.** Cada persona usuaria tendrá la obligación inexcusable de salvaguardar y proteger los datos personales de terceros de los que tenga conocimiento en virtud de su relación con la UCR. Toda la información referente a datos personales de terceras personas, tales como el número telefónico personal, correo electrónico o la dirección física, entre otros, deberá ser tratada como información confidencial y no divulgarse a terceros.

Fuente: elaboración propia a partir de: Centro de Informática de la UCR, 2020-a, p.3-4.

También, en temas de seguridad, con la aparición de la pandemia global por COVID-19, y la necesidad de la UCR de ofrecer alternativas a sus funcionarios para continuar con el funcionamiento institucional, se implementa el "Trabajo Remoto". Como esta actividad no había sido previamente planificada ni normada, se debieron tomar acciones que permitieran mantener la seguridad de la información generada y custodiada por la Universidad.

De esta forma, algunas de las medidas de seguridad para la gestión del trabajo remoto que se tomaron, fueron por ejemplo la creación de campañas como (Castro-Mattei, 2020):

- Campaña de Seguridad COVID-19 Ciberseguro: contempla consejos sobre ciberseguridad, distribuidos a través de las redes sociales.
- Campaña Directrices Técnicas de Seguridad de Información: basada en la Resolución R-102-2015 Directrices de Seguridad de la Información de UCR.

Ambas campañas se encuentran activas en el sitio web del Centro de Informática de la UCR y ofrecen material informativo a la comunidad universitaria, para un uso seguro de la información.

Observando esfuerzos más recientes, en el año 2021, la UCR elaboró un Marco de Gobierno y Gestión de TI, donde uno de sus objetivos de gobierno es el de Seguridad de la Información. Este componente de gobierno, pretende "propiciar de manera razonable la confidencialidad, integridad, disponibilidad, autenticidad de la información, acceso, trazabilidad y servicios utilizados en medios electrónicos, por medio de la toma de decisiones basada en riesgos para asegurar el cumplimiento de la normativa interna y externa de la institución en materia de seguridad de TI" (Centro de Informática, 2021, p.6).

Este objetivo de gobierno, a su vez se subdivide en 4 prácticas por realizar (Centro de Informática, 2021):

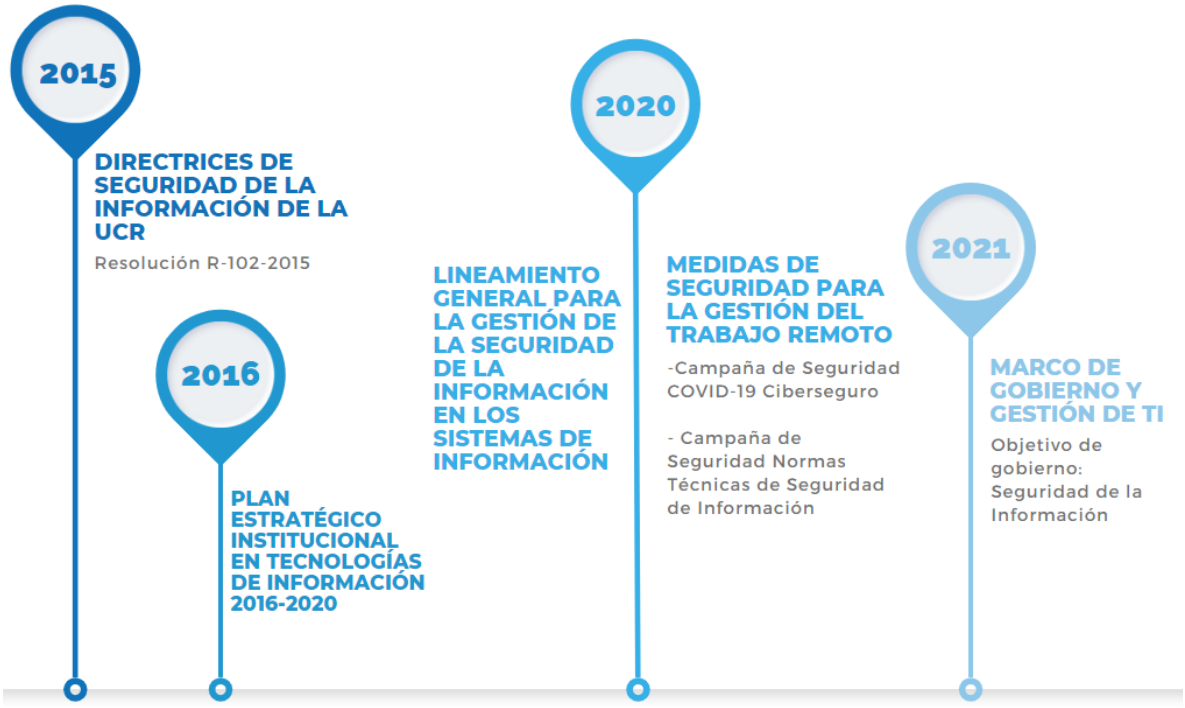
- Implementar un marco de seguridad de la información.
- Gestionar riesgos ante amenazas.
- Planificar y detectar procesos de la gestión de la seguridad de TI.
- Implementación de la gestión de proyectos de la seguridad de TI.

El propósito del objetivo sobre seguridad de la información de TI, es "cubrir los controles para establecer que la información custodiada, almacenada, transferida, procesada e incluso eliminada

cumpla los requerimientos de confidencialidad, integridad, disponibilidad y autenticidad establecida en la normativa de seguridad de la información institucional" (Centro de Informática, 2021, p.173).

Finalmente, se presenta una línea de tiempo (figura 8) que resume las acciones más recientes que ha tomado la Universidad sobre seguridad de la información:

Figura 8. *Línea de tiempo sobre acciones para la seguridad de la información en la UCR.*



Fuente: Elaboración propia. 2023.

ii. <u>Respaldos de la información</u>

Las Directrices de Seguridad de la Información de la Universidad de Costa Rica (Rectoría de la UCR, 2015), en el capítulo 8 "Resguardo y protección de la información", artículo 18, reconoce la importancia de realizar respaldos de información.

También, en el artículo 21, señala con respecto a respaldos y recuperación de la información que "la información que la Universidad de Costa Rica determine como esencial deberá ser respaldada y resguardada en instalaciones seguras y controladas, a fin de que la misma pueda recuperarse

una vez ocurrido un desastre, siniestro, emergencia o falla en/de los dispositivos y/o sistemas" (Rectoría de la UCR, 2015, p.6).

Así también, en el Marco de gobierno y gestión de TI de la UCR, se propone como actividad la administración de respaldos de información (figura 9) como parte de los mecanismos y procedimientos para la continuidad de servicios de TI, lo cual debe generar como producto un "Plan de respaldos y pruebas de recuperación de seguridad de los datos" (Centro de Informática de la UCR, 2021-a, p.52).

Figura 9. *Descripción de la Administración de Respaldos según Marco de gobierno y gestión de TI de la Universidad de Costa Rica.*

Fuente: Elaboración propia a partir de: Centro de Informática de la UCR, 2021, p.52.

Otra de las actividades propuesta en el Marco de gobierno y gestión de TI, en cuanto a la gestión de proyectos de seguridad de TI, incluye la implementación del plan de ejecución de respaldos y recuperación de información de TI, para lo cual se debe (figura 10):

Figura 10. *Descripción de la implementación del plan de ejecución de respaldos y recuperación de información de TI según Marco de gobierno y gestión de TI de la Universidad de Costa Rica.*

Fuente: Elaboración propia a partir de: Centro de Informática de la UCR, 2021-a, p.183.

Desde el Centro de Informática de la UCR, se establece según procedimientos,la frecuencia de los respaldos, dependiendo del tipo de información con la que están trabajando, donde se toman en cuenta criterios de constancia, integridad, confidencialidad y disponibilidad.

Los procedimientos actuales (a 2022) con los cuáles cuenta el CI son:

CI-AGS-P01 Procedimiento para la realización de respaldos y pruebas de recuperación de datos: establece la configuración de los respaldos, el seguimiento del resultado de los respaldos realizados, las pruebas de recuperación de datos, el registro de las pruebas de recuperación de datos, así como el seguimiento y revisión de las pruebas (Centro de Informática de la UCR, s.f.-a).

CI-AGS-P11 Procedimiento para la realización y custodia de respaldos: señala actividades como la gestión de necesidades de respaldos críticos, el diseño y configuración de respaldos, la generación y monitoreo de respaldos, la Retención y Custodia de Respaldos y las pruebas de respaldos (Centro de Informática de la UCR, 2021-b)

iii. Almacenamiento de información

El almacenamiento de información de distintas unidades administrativas, académicas y de investigación de la UCR se lleva a cabo por medio de los siguientes servicios (Centro de

Informática de la UCR, 2022-a): Servicio para base de datos; Servicios para Hospedaje Web; y Servicio Virtualizacion de Servidores

Estos servicios, constituyen lo que la Universidad conceptualiza como *resguardo de información*, el cual "está vinculado a la protección de ciertos datos que transmiten información, ya sea física o digital" (Centro de Informática de la UCR, s.f.-b, p.1).

Figura 11. *Servicios de almacenamiento ofrecidos por el Centro de Informática de la UCR.*

Fuente: Elaboración propia a partir de: Centro de Informática de la UCR, 2022-a.

En el artículo 19 de las Directrices Técnicas de Seguridad de la Información de la Universidad de Costa Rica (Rectoría de la UCR, 2015, p.5) se señala que toda la información generada en el ejercicio de sus funciones le pertenecen a la Institución:

> **ARTÍCULO 19.** Propiedad de la información: Toda la información que se almacena, transita, es recopilada, distribuida, reproducida, procesada y/o creada en los sistemas de información de la Universidad de Costa Rica, será considerada, para efectos de la gestión en seguridad de la información, como propiedad de la Universidad, salvo que el ordenamiento jurídico establezca lo contrario. Por lo tanto, no podrá bajo ninguna circunstancia, ser transmitida en manera alguna a terceros, modificada ni eliminada, sin contar con autorización formal para ello, por parte de los jerarcas y titulares subordinados responsables de la información.

Con base en el artículo anterior, se puede inferir que el almacenamiento de la información debe realizarse utilizando los recursos que ofrece la institución para tal fin. Sin embargo, en algunas unidades se utilizan equipos personales y dispositivos externos (discos duros externos, llaves mayas, discos compactos, etc.), sin ninguna seguridad comprobada, para almacenar información.

iv. Plan de continuidad de Servicios

Administrar la continuidad de las operaciones, requiere de un esquema estructurado que permite la toma de decisiones en situaciones de interrupciones imprevistas y graves de los servicios de la institución, ya sea que provengan de la infraestructura de TI o bien de desastres naturales (Centro de Informática de la UCR, 2022-b p.1).

La continuidad de los servicios se contempla como un apartado dentro de las Directrices de Seguridad de la Información de la Universidad de Costa Rica. El capítulo 18, llamado "Administración de la continuidad de las operaciones", indica la necesidad de prepararse ante posibles interrupciones de actividades, de manera que puedan protegerse los procesos críticos y cumplirse con los objetivos primordiales de la institución (Rectoría de la Universidad de Costa Rica, 2015).

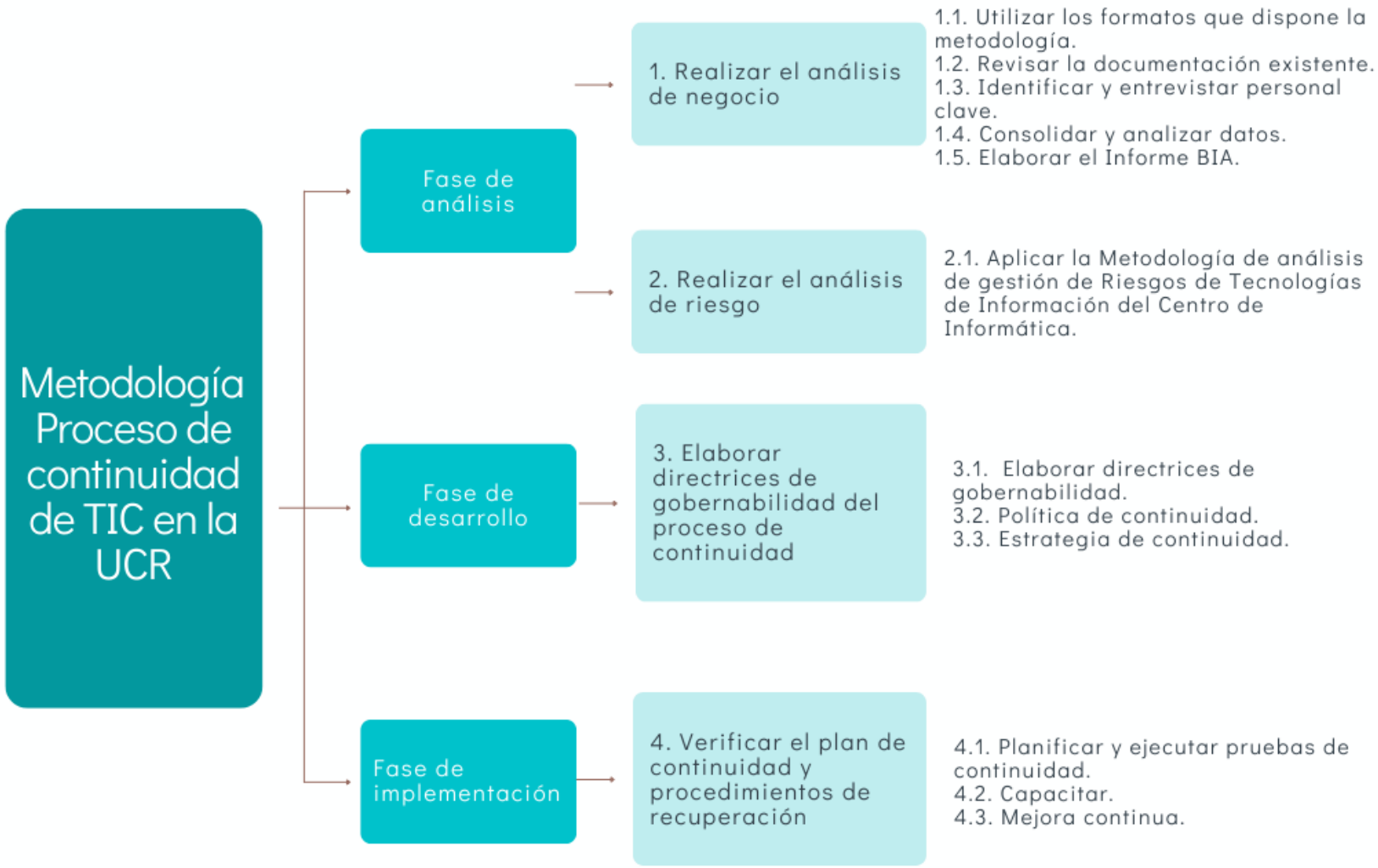
De esta forma, se impulsa el desarrollo y ejecución de planes de continuidad con el fin de "mantener o restablecer la operación de la Universidad y asegurar la disponibilidad de la información en plazos mínimos, una vez ocurrida una emergencia, evento de falla y/o interrupción de servicios, que afecte los procesos críticos" (Rectoría de la Universidad de Costa Rica, 2015, p.10).

Desde el año 2019, el Centro de Informática de la UCR emite la "Metodología del Proceso de Continuidad de Tecnologías de la Información y Comunicación", cuyo propósito es el de (p.3):

> Establecer una metodología aplicable para garantizar un adecuado nivel de seguridad, disponibilidad y confiabilidad de los procesos vitales de tecnologías de la Información y la comunicación en las operaciones del Centro de Informática o de cualquier otra unidad de la Universidad de Costa Rica,donde se desee implementar un proceso de continuidad, de manera tal que se asegure la continuidad de sus procesos.

La metodología propuesta incluye las siguientes fases (figura 12):

Figura 12. *Fases de la Metodología del Proceso de Continuidad de Tecnologías de la Información y Comunicación.*



Fuente: Elaboración propia a partir de: Centro de Informática de la UCR, 2019, p.6.

Sumado a esto, en el Marco de Gobierno y Gestión de TI de la Universidad de Costa Rica, en su objetivo de gobierno "Optimización y gestión del riesgo TI", propone como objetivo de gestión la Continuidad de los servicios TI, en el cual se indica la necesidad de aplicar las acciones propuestas en los planes de continuidad de servicios.

La Continuidad de los servicios TI, según este marco, requiere de prácticas como: planificar los requerimientos de continuidad; diseñar y ejecutar mecanismos y procedimientos adecuados y medibles; así como evaluar y realizar las mejoras para favorecer la continuidad de los servicios de TI (Centro de Informática de la UCR, 2021-a, p.47).

- **Estándares**

Los estándares que se utilizan en la UCR están regulados por el Centro de Informática. Dichos estándares están dados para poder adquirir equipos de cómputo, multimedia y redes (Centro de Informática de la UCR, 2022-c).

Dentro de los estándares de equipos, el CI establece los requisitos mínimos con los que deben cumplir los equipos que se adquieran. A continuación se presentan los principales equipos de cómputo (Tabla 8), equipo multimedial (Tabla 9) y equipos de comunicaciones (Tabla 10) para los que el CI brinda estándares:

Tabla 8. *Estándares de cómputo del Centro de Informática de la UCR.*

Computadoras portátiles	Computadoras de escritorio y de trabajo científico	Servidores de rack y de torre	Escáner	Impresoras	Equipos SAI - UPS
*Procesador *Conjunto de Chipset y Memoria *Video *Monitor *Teclado y apuntador *Almacenamiento *Puertos *Sonido *Comunicaciones *Voltaje y Batería *Peso *Seguridad *Otras características *Accesorios y equipamiento opcional	*Procesador *Conjunto de Chipset y Memoria *Video *Monitor *Teclado y apuntador *Almacenamiento *Puertos *Sonido *Comunicaciones *Voltaje y Batería *Peso *Seguridad *Chasis y cubierta *Energía *Otras características *Accesorios y equipamiento opcional	*Procesador INTEL *Conjunto de Chipset y Memoria *Tarjeta madre *Vídeo *Almacenamiento *Comunicaciones *Chasis y Cubierta *Tarjeta de red *Otras características	*Línea empresarial *Alimentador automático *Escaneo dúplex *Velocidad de escaneo *Resolución óptica *Área de escaneo *Mejoramiento de imagen escaneada *Interfase para transferencia de datos *Puerto de red Ethernet *Carga de trabajo *Fuente de alimentación *Otras características	*Tipo de impresión *Resolución óptica *Velocidad de impresión *Tamaños de papel soportados *Tipo de materiales de impresión soportados *Imprimir por ambas caras del papel *Capacidad de entrada *Capacidad de salida *Carga de trabajo *Tóner *Memoria * Conectividad *Procesador *Lenguajes *Pantalla	*Características físicas * Características técnicas mínimas de rendimiento *Administración *Otras características

Fuente: Elaboración propia a partir de: Centro de Informática de la UCR (2022-c).

Tabla 9. *Estándares de equipo multimedial del Centro de Informática de la UCR.*

Proyectores Multimedia	Cámaras Digitales	Pantallas LCD con retroalimentación LED
*Tecnología LCD o DLP *Tipo de fuente de luz *Luminosidad *Conexión a PC *Resolución nativa *Soporte de señales *Formato de salida *Compatible con sistema vídeo digital *Vida útil de la fuente de luz *Índice de contraste *Conectores HDMI * Puerto USB *Puerto RJ-45 *Entrada voltaje *Consumo de energía *Sistema de abanico silencioso *Parlante *Ajuste de enfoque y zoom manual, digital y/o motorizado *Conexión inalámbrica *Posición de proyección frontal, normal e invertida para techos *Peso máximo *Menús multi-lenguaje *Soporte de plataformas *Control remoto	*Ajuste de foco *Resolución de pantalla *Grabación en tarjeta de memoria *Montaje para lentes intercambiables *Velocidad de obturación *Grabación de vídeo *Compatibilidad de lentes de conversión *Formato de archivo *Resolución mínima *Balance de blancos *Flash integrado y montaje para flash externo *Conexión a computadora *Entrada de audio *Materiales del cuerpo *Peso *Entro otras Lente: *Montura *Peso *Apertura *Modo automático y manual *Distancia de enfoque	*Tamaño de pantalla *Tipo de pantalla *Formato de salida/aspecto *Compatible con el formato ISDB-Tb *Resolución nativa mínima *Parlantes *Conectores HDMI *Conectores compuestos y vídeo componente *Puertos USB *Puerto RJ-45 *Control remoto *Menú multi-lenguaje *Fuente de alimentación *Consumo máximo *Almacenamiento interno *Sistema operativo *Conexión inalámbrica *Entre otras

Fuente: Elaboración propia a partir de: Centro de Informática de la UCR (2022-c).

Tabla 10. *Estándares de equipos de comunicaciones del Centro de Informática de la UCR.*

Telefonía IP	Equipo activo conmutadores	Equipo inalámbrico
*Características físicas *Características de rendimiento *Administración *Protocolos soportados *Otras características	*Características físicas *Características de rendimiento *Administración *Seguridad *Protocolos soportados *Otras características	*Características básicas del equipo *Aspectos de seguridad *Normas y estándares que debe soportar *Otras características que el equipo debe incluir *Otros

Fuente: Elaboración propia a partir de: Centro de Informática de la UCR (2022-c).

- **Uso de *software* y formatos de ficheros**

La institución ha desarrollado y adquirido múltiples soluciones tecnológicas que le permiten ejecutar sus funciones sustantivas y facilitativas. Por consiguiente, actualmente existe información almacenada en sistemas informáticos licenciados o propietarios y en sistemas desarrollados con base en el *software* libre.

En el primer caso, se define como *software* licenciado a todos aquellos programas que se distribuyen bajo licencia en la cual se especifican las condiciones de uso por parte de los usuarios y que conforman los programas que son de pago (Centro de Informática de la UCR, 2020-b, p.2). Es importante destacar que generalmente los propietarios de los sistemas no brindan acceso a los códigos fuentes, ni permiten su modificación ni el compartirlo libremente.

En el segundo caso, se entiende como *software* libre a los sistemas que pueden ser usados, copiados, estudiados, mejorados y redistribuidos sin limitaciones (Centro de Informática de la UCR, 2020-b, p.2). Estos sistemas son desarrollados de forma colectiva y buscan la socialización del conocimiento.

Así, a través de la Resolución R-289-2014, se aprobaron las *Directrices para la puesta en marcha del plan de migración a software libre en la Universidad de Costa Rica*, con la que se ordena su aplicación obligatoria en todas las instancias universitarias.

Dicha Resolución presenta una serie de consideraciones que justifican la necesidad de utilizar *software libre* en la institución, entre las que destacan que (Rectoría, 2014):

- Este tipo de sistemas informáticos y formatos de fichero pueden sustituir las alternativas propietarias, sin perder productividad e incluso aumentarla.
- Su uso promueve en la educación aspectos éticos como la solidaridad, la colaboración y la legalidad, facilitando el intercambio de aplicaciones.
- Existe interés a nivel estatal de promover el uso de *software libre*, para la resolución de necesidades informáticas, en coherencia con los principios de eficiencia en el uso de recursos.
- En otras instituciones de enseñanza superior en todo el mundo, se ha demostrado que estas herramientas son funcionales, productivas y promotoras del desarrollo, la investigación, la docencia y la acción social.
- Hay una construcción colectiva del conocimiento, lo cual favorece el surgimiento de oportunidades para el desarrollo.
- Promueve la independencia tecnológica, aumentando la autonomía en la contratación de proveedores y soporte técnico, al tiempo que favorece el uso de los gastos por la adquisición de aplicaciones.

Se torna importante recalcar que actualmente existen soluciones de *software libre* para el desarrollo e implementación del ADiUCR, como se abordará más adelante en este capítulo. El uso de este tipo de aplicaciones validaría un mejor uso de los recursos públicos, ya que en varios casos son de uso gratuito y están respaldados por instituciones con amplio alcance a nivel mundial.

Sumado a ello, la implementación de estas opciones tecnológicas, permitirían que el conocimiento generado en la planificación, programación, uso y mantenimiento de las soluciones tecnológicas sea adquirido por los profesionales de la UCR, en campos del conocimiento como la Archivística y las TI.

- **Firma digital y sello electrónico**

La Universidad de Costa Rica logró identificar 4 aspectos que han impulsado la reglamentación para el uso de la firma digital a nivel institucional y así promover la agilización de los trámites y

el aseguramiento de la integridad, autenticidad y fiabilidad de los documentos (Rectoría de la Universidad de Costa Rica, 2020, p.1-2):

a. Se identificaron prácticas inadecuadas en el uso de la firma manuscrita y digital como el uso de firmas híbridas (combinación de ambos tipos de firmas en un mismo documento); documentos con firma digital con fecha posterior al día de emisión de la firma; uso de firmas digitalizadas (escaneadas o colocadas por medios digitales); posición no normalizada de las firmas en los documentos del SiGeDI, entre otras.
b. La situación de la pandemia por el COVID-19 implicó dar continuidad a los trámites administrativos y académicos, con lo cual se adoptaron prácticas como flexibilizar la cantidad de firmas de algunos documentos; recibir documentos digitalizados por correo electrónico, con el compromiso de los remitentes, de presentar los originales posteriormente; propiciar el uso de la firma digital y horarios especiales para la recepción de documentos físicos.
c. Desde el 2017, se incrementó el uso de la firma digital en algunas instancias, pero no era una práctica institucionalizada.
d. A partir del 2018, se inició la implementación del SiGeDI, el cual incorpora el uso de la firma digital, pero no todas las instancias universitarias han ingresado al uso del sistema.

Por estas razones, mediante la Resolución R-174-2020 (Rectoría de la Universidad de Costa Rica, 2020, p.6-7), se aprueban los lineamientos generales para regular la firma autógrafa y la firma digital en los documentos. Así, específicamente para firma digital, se señala la autorización del uso de la firma digital en la UCR, los deberes de configuración de los equipos, la presunción de autoría de los documentos en lo que se plasme la firma digital, asegurarse de que los documentos firmados digitalmente cumplan con la Ley 8454 de Certificados, Firmas Digitales y Documentos Electrónicos, el respaldo de los documentos firmados digitalmente, entre otros aspectos importantes.

Es importante resaltar que según la Ley 8454, Artículo 3, existe el *reconocimiento de la equivalencia funcional*, que significa que "cualquier manifestación con carácter representativo o declarativo, expresada o transmitida por un medio electrónico o informático, se tendrá por jurídicamente equivalente a los documentos que se otorguen, residan o transmitan por medios físicos" (Asamblea Legislativa, 2005). Es decir, todo documento de la Universidad de Costa Rica

que se haya sido firmado y certificado digitalmente de manera apropiada, debe ser gestionado con la misma rigurosidad que si se tratara de un documento en soporte físico, por lo cual debe ser tramitado y conservado según lo especifique la normativa correspondiente.

En cuanto al sello electrónico o firma digital institucional, en la Universidad de Costa Rica se ha conformado una comisión o grupo de trabajo multidisciplinario, con personal del Centro de Informática, el Archivo Universitario y la Oficina Jurídica, con el objetivo de analizar los aspectos tecnológicos, archivísticos y jurídicos en cuanto a la implementación de este tipo sello.

De esta manera, se han llevado a cabo reuniones con otras instituciones que tienen experiencia en el uso del sello electrónico, entre ellas el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), el Archivo Nacional y el Banco Central de Costa Rica (BCCR), este último como ente coordinador en la materia.

A raíz del trabajo desarrollado, la Universidad ha comenzado con el desarrollo tecnológico, para abordar la etapa de pruebas, para luego poner en funcionamiento el sello electrónico, posterior a la definición de las series documentales sujetas al sello y sus implicaciones jurídicas.

Para dar inicio con esta etapa de pruebas, se requirió que, el 16 de marzo de 2022, el Rector de la Universidad de Costa Rica, autorizara en el Sistema Digital del BCCR para que los funcionarios del Centro de Informática que son miembros de la comisión de sello electrónico puedan utilizar el sello electrónico en documentos de prueba (Fonseca-Chacón, 2022, p.3).

El sello electrónico será utilizado para firmar de forma automática documentos que se emiten de forma masiva y con contenido reiterativo en la institución (por ejemplo, títulos, certificaciones o documentos de alcance general interno) y que no son sujetos jurídicamente a la firma de un funcionario en particular (Fonseca-Chacón, 2022, p.2).

También se ha indicado que los riesgos asociados al uso del sello son mínimos ya que el sistema es seguro, porque el documento sellado tendrá un algoritmo de seguridad, por lo cual en el momento en el que sufra alguna modificación, perdería su validez. Además, que la utilización del sello electrónico quedará registrado en una bitácora de uso, con hora y fecha, para el rastreo de acciones e incluso la revocación de delegación, por ejemplo, en caso que el funcionario deje de trabajar para la institución (Fonseca-Chacón, 2022, p.3).

Finalmente, se han desarrollado hojas de ruta y diagramas de flujo para abordar y representar los distintos escenarios del proceso en los que se podría hacer uso del sello electrónico. Sin embargo, estos documentos también se encuentran en periodo de desarrollo.

- **Recursos y presupuesto**

En la Universidad de Costa Rica, la Oficina de Planificación Universitaria es la unidad responsable del proceso de elaboración del Plan Estratégico Institucional, así como del Plan Presupuesto, y por su parte, el Consejo Universitario es el ente encargado de conocer y aprobar el Plan Estratégico Institucional y así también el responsable de analizar y aprobar el Plan Presupuesto anual (2009, p.4-5).

Con base en el presupuesto aprobado, la Comisión Institucional de Equipamientos (CIEq), es el órgano encargado de "dotar a las unidades académicas y administrativas del equipo necesario para el cumplimiento de sus funciones" así como de dictar "las políticas para la asignación apropiada de los recursos financieros, según el presupuesto disponible y la planificación definida, mediante el análisis dentro de los criterios de razonabilidad, equidad, interés institucional y excelencia académica" (Centro de Informática de la UCR, s.f.-c, p.1-2).

Esta Comisión, está integrada por (Centro de Informática de la UCR, s.f.-c, p.3):

- Un representante de cada área académica
- Un representante de cada Vicerrectoría
- Los directores de:
    - Centro de Informática
    - Oficina de Suministros
    - Escuela de Ciencias de la Computación e Informática
    - Escuela de Ingeniería Eléctrica

En el acta CIEQ-22-2022, se expresa en el punto 3 el informe sobre "el presupuesto con que inicia este año 2022 para cubrir lo asignado a las unidades, realizar la compra de los programas de software y equipo de cómputo, dar soporte en equipo de comunicación y apoyo en repuestos y accesorios" (Comisión Institucional de Equipamiento de la UCR, p.4, 2022).

En dicha acta se describe el presupuesto asignado para los siguientes rubros:

- Repuestos y Accesorios
- Equipo de Comunicaciones
- Equipo y Mobiliario de Cómputo
- Bienes Intangibles (Programas de Cómputo)
- Equipo Sanitario, de Laboratorio e Investigación
- Equipo Educacional y Cultural

De esta manera, por medio del trabajo que realiza la CIEq, pero en conjunto con el aporte y las solicitudes de las distintas unidades académicas, administrativas y de investigación, se determina y se ejecutan los recursos necesarios para que la UCR cuente con el equipo y la infraestructura tecnológica que requiere para el cumplimiento de sus funciones.

2.4. Evaluación de riesgos para la preservación digital de la información

2.4.1. Evaluación de la Continuidad Digital y Gestión del Riesgo

Una de las aristas más importantes para entender el contexto institucional en cuanto a la preservación digital, es la evaluación de los riesgos, ya que permite determinar el nivel de seguridad con que se gestiona la información. Este análisis ayuda en la toma de decisiones para la aplicación de acciones correctivas que aseguren la preservación y el uso de la información institucional.

Con el objetivo de tener una acercamiento a la situación actual de la preservación digital en la Universidad de Costa Rica, se retomó el uso de la herramienta de autoevaluación denominada *Digital continuity self-assessment tool*, desarrollada por los Archivos Nacionales del Reino Unido. Como se explicó en el capítulo anterior, esta herramienta fue aplicada a 5 participantes en el año 2013, por lo cual fue necesario actualizar los resultados.

Por consiguiente, para esta investigación se optó por ampliar la recolección de datos a 14 instancias universitarias, las cuales fueron seleccionadas por su alcance en la toma de decisiones y en el ámbito archivístico y tecnológico. De esta forma, se consideraron al Archivo Universitario Rafael Obregón Loría y la Sección de Archivística de la Escuela de Historia porque sus funciones están relacionadas con la gestión de la información institucional y la formación de

nuevos profesionales en Archivística. Se incluyó al Centro de Informática, por su rol fundamental en el desarrollo de la infraestructura tecnológica de la institución.

También se consideraron a los medios de comunicación universitarios, es decir, a Radioemisoras UCR, Canal Quince-UCR, al Semanario Universidad y a la Oficina de Comunicación Institucional, puesto que por la naturaleza de sus funciones, producen y almacenan una amplia variedad de clases documentales, entre las que están el material audiovisual, el cual debe ser preservado.

Además, para la aplicación de la herramienta, se tomó en cuenta a la Rectoría y al Consejo Universitario ya que tienen una amplia injerencia en la toma de decisiones de la institución. Finalmente, se consideraron la Vicerrectoría de Administración, la Vicerrectoría de Acción Social, la Vicerrectoría de Vida Estudiantil, la Vicerrectoría de Investigación y la Vicerrectoría de Docencia, ya que es por medio de estas entidades que se canaliza la autoridad de la Rectoría, lo cual les brinda un amplia capacidad en la toma de decisiones (Consejo Universitario, 1974, p.10).

El cuestionario aplicado está dividido en tres secciones que permiten abordar: a) los roles y responsabilidades para la comprensión de la continuidad digital, b) los requerimientos de información y las dependencias técnicas y c) la gestión del riesgo en cuanto a la preservación digital (Anexo 1).

Cabe resaltar que la información se solicitó a las unidades administrativas por medios formales como oficios, correos electrónicos enviados a las cuentas oficiales de la Universidad y mediante llamadas telefónicas a los números de las oficinas correspondientes. No obstante, es importante recalcar que la recolección de los datos se dificultó, por la nula participación de algunas unidades. Esta situación denota el desconocimiento en cuanto a la importancia de dar prioridad a la preservación de la información digital.

A continuación, se presentan los resultados obtenidos a partir del análisis de las respuestas de 10 de las unidades con base en la perspectiva que estas tienen acerca de la preservación digital en la institución (Tablas 11, 12 y 13):

a. Roles y responsabilidades para la comprensión de la continuidad digital

Tabla 11. *Roles y responsabilidades para la comprensión de la continuidad digital en la Universidad de Costa Rica.*

Situación	Riesgo	Acciones por implementar
En los niveles superiores de la Unidades de la UCR, hay reconocimiento sobre la importancia de la preservación digital, pero no es un objetivo formal.	Medio bajo	En el año 2022, se creó la Comisión Institucional de Archivo Digital (CIADi), la cual se encuentra desarrollando la propuesta de normativa para la creación de un Archivo Digital (ADiUCR). Establecer la preservación digital como un objetivo formal, dentro de Políticas Institucionales y el Plan Estratégico Institucional, asegurará el presupuesto y el apoyo que se requiere por parte de las altas jerarquías.
En la UCR hay profesionales por debajo del nivel de Dirección en las Unidades, que son responsables de la gestión de riesgos para la preservación digital, pero no existe la figura de SIRO (*Senior Information Risk Owner* o Responsable Ejecutivo los Riesgos de la Información) como responsable de dicha gestión.	Medio alto	Se debe designar a una persona para la gestión de los riesgos para la preservación digital, mediante la figura de SIRO.
En las Unidades de la UCR, son individuos o equipos aislados los que están tomando la iniciativa en la preservación digital, quienes no siempre se encuentran a un nivel adecuado o con la autoridad suficiente para la toma de decisiones.	Medio bajo	Dentro de cada Unidad de la UCR, se debe nombrar a una persona que tenga la autoridad para ejecutar las acciones de preservación digital, en consonancia con lo determinado por el ADiUCR.
La UCR no cuenta con una estrategia para definir el alcance y el proceso de preservación digital, pero tomarán acciones para este fin.	Medio alto	El ADiUCR debe desarrollar una estrategia de preservación que incluya un Plan de Datos, de Ingreso, de Conservación, de Acceso, de Tecnología y de Continuidad, ejecutado según un calendario de obligaciones.

Situación	Riesgo	Acciones por implementar
Personas de distintas disciplinas están colaborando en una base para llevar a cabo la preservación digital.	Medio bajo	En el año 2022, se conformó la CIADi, con profesionales en Archivística, Informática y Derecho, con el fin de abordar la preservación digital desde un enfoque multidisciplinario. El ADiUCR deberá coordinar las acciones institucionales en torno a la preservación digital.
Los propietarios de los activos de información no entienden de preservación digital ni su rol para gestionarla.	Medio alto	Al crear el ADiUCR, se deben definir roles claros para cada una de las partes involucradas en la gestión de activos de información (propietario de activos de información, responsables de la gestión de riesgos, archivistas, especialistas en TI, usuarios, entre otros).

Fuente: Elaboración propia a partir de los resultados de la aplicación de la *Digital continuity self-assessment tool.* 2023.

Para llevar a cabo la preservación digital sistémica de la información institucional, es indispensable que las altas jerarquías de la Universidad, en específico la Rectoría y el Consejo Universitario, tengan clara la necesidad de que se desarrolle e implemente un Archivo Digital basado en normas archivísticas internacionales, en conjunto con el uso activo de las TIC.

La Norma UNE-ISO 14721, plantea que la Dirección es quién define el alcance del Archivo Digital y avala sus actividades. Asimismo, la Dirección es la principal fuente de financiación del Archivo Digital, al proporcionar las líneas para la utilización de los recursos como personal, equipamiento y servicios. También es la dirección quién evalúa el rendimiento y el progreso del Archivo para la consecución de los objetivos a largo plazo (AENOR, 2015-b, p.29).

De esta forma, deben existir políticas aprobadas por las altas jerarquías, que permitan colocar a la preservación digital dentro de los objetivos de alcance institucional, considerando que todas las instancias de la Universidad producen y utilizan información para el desarrollo de sus actividades y la ejecución de sus funciones.

No obstante, como se observa en la Tabla 11, actualmente existe una noción general de la importancia de la preservación digital, pero no constituye un objetivo formal. Como consecuencia, no se ha desarrollado normativa específica en este tema, ni se han destinado los recursos necesarios para el funcionamiento de un Archivo Digital.

Esta falta de un marco legal aplicable, sumado a la heterogeneidad en las actividades que se desarrollan, provocan un aislamiento en el trabajo desarrollado por las personas de distintas disciplinas relacionadas con el tema de la preservación digital, entre ellos archivistas e informáticos. También existe una segregación entre las distintas instancias universitarias en materia de preservación digital, ya que cada una ejecuta sus propias acciones, según la asignación de sus recursos y el cumplimiento de sus objetivos específicos.

Por consiguiente, aumenta el riesgo de la gestión para la continuidad digital, ya que no hay roles y responsabilidades claramente definidas. Tampoco existe claridad de quién es el propietario de la información ni de quién debería asegurarse de preservar correctamente la información, ni cómo hacerlo.

b. Requerimientos de información y dependencias técnicas

Tabla 12. *Requerimientos de información y dependencias técnicas en la Universidad de Costa Rica.*

Situación	Riesgo	Acciones por implementar
La información crítica para la UCR o datos personales es entendida y documentada, pero no incluye toda la información de valor de la organización.	Medio bajo	Se deben llevar a cabo los procesos de identificación archivística y evaluación de documentos, para conocer el valor de toda la información institucional. Estos procesos deben vincularse con los protocolos de ingreso y custodia del ADiUCR.
La UCR conoce donde se encuentra su información (sistemas, equipos, etc.), cuales son las restricciones de acceso y seguridad y si existe información con datos sensibles, pero no tiene claridad de sus características técnicas (por ejemplo, información de formatos), los plazos de retención (tablas de plazos), los requerimientos de usabilidad ni el valor que tiene la información para el negocio.	Alto	En el Protocolo de Transferencia de cada Unidad, deben incluirse los aspectos técnicos y de contexto para la transferencia de información al ADiUCR.
La UCR custodia información digital con distintos plazos de conservación (5, 10, 30 o más años) según cada serie documental, pero no se ha identificado el plazo para toda la información.	Alto	Se deben crear las tablas de plazos de conservación para la totalidad de las series documentales en la UCR, ya que el Protocolo de Transferencia requiere incluir los plazos de conservación de la información a transferir, además de los plazos de conservación de las propiedades significativas de apariencia, funcionalidades y autenticidad.
La UCR tiene información que tiene las siguientes condiciones: puede consultada de forma pública; está sujeta a la ley de protección de datos; puede contener datos sensibles o restringidos; puede servir de evidencia legal; está sujeta a actos de registros públicos; debe ser compartida con otras Unidades; debe ser publicada como información pública y apoyo a la transparencia; ayuda a los servicios del	Alto	El ADiUCR debe incluir mecanismos de control para el acceso, uso y reutilización de la información, dentro de un procedimiento de acceso. Se debe asegurar dicho acceso durante el tiempo que sea necesario, mediante un plan de conservación que mitigue la obsolescencia tecnológica y permita la migración a nuevos desarrollos tecnológicos.

Situación	Riesgo	Acciones por implementar
negocio; puede ser reutilizada, reanalizada o reasignada; puede tener una historia de cambio que se debe conservar.		
En la UCR cada Unidad tiene cierta comprensión de sus sistemas y cómo son interdependientes.	Media baja	El Centro de Informática tiene la responsabilidad de comprender toda la infraestructura tecnológica de la institución, para realizar las integraciones necesarias con el ADiUCR.
La UCR entiende las aplicaciones que utiliza, pero no los formatos específicos y versiones que posee o las aplicaciones de las cuales dependen para usarlos.	Media baja	Establecer en el protocolo de ingreso, los formatos que serán admitidos en el ADiUCR por cada Unidad. Los formatos y las versiones deberán ser verificadas de manera automática por el repositorio digital.
La UCR utiliza tecnología obsoleta para gestionar activos de información, pero tiene una estrategia para migrar a otras tecnologías, cuando sea posible.	Media baja	La CIADi y el Centro de Informática deberán identificar cuáles sistemas de la UCR se encuentran obsoletos, para recuperar la información que deba ser transferida al ADiUCR. La Política de Preservación debe incluir la revisión periódica de los sistemas para mitigar la obsolescencia. El ADiUCR debe asegurar que la información que custodia no se vuelva obsoleta y pueda ser recuperada.
La UCR utiliza tecnología hecha a la medida para gestionar activos de información, pero esta tecnología cuenta con soporte durante toda la vida útil de la información que depende de esta tecnología.	Media baja	Según sus políticas de migración al uso de *software* libre (Resolución R-254-2014: *"Directrices para la puesta en marcha del plan de migración a Software Libre en la Universidad de Costa Rica")*, la UCR debe analizar opciones tecnológicas abiertas para el desarrollo del ADiUCR, para dar a la universidad autonomía en el tema de soporte.
En la UCR se mantiene información almacenada en medios externos o extraíbles (dispositivos USB, discos duros externos, CD´s, etc.), en discos locales de usuarios (computadoras portátiles o de escritorio), en correos electrónicos (incluyendo archivos adjuntos), en sistemas de gestión de documentos (SGDEA, Sharepoint, etc.)	Alto	Por medio del ADiUCR se debe mantener centralizada toda la información institucional, evitando las islas de información en las distintas Unidades y asegurando la cadena de custodia.

Fuente: Elaboración propia a partir de los resultados de la aplicación de la *Digital continuity self-assessment tool.* 2023.

En la Universidad de Costa Rica, hay un marcado desconocimiento en la identificación de los sistemas y la información digital que posee. Existe información crítica y datos restringidos que deben ser resguardados, pero no se han identificado la totalidad.

Otro aspecto que pone en riesgo la preservación de la información, es que, en general, se considera que hay conocimiento sobre en cuáles sistemas informáticos y dispositivos se encuentra almacenada la información, pero no se conocen a fondo las características técnicas de los sistemas ni de la información (por ejemplo, los formatos de los ficheros, espacios de almacenamiento, entre otros), que son fundamentales para desarrollar un plan de preservación digital.

Además, no se puede asegurar la cadena de custodia, ya que la información es normalmente almacenada en dispositivos que no son adecuados para llevar a cabo la preservación digital sistémica, la cual requiere políticas que normalicen los procedimientos. En este sentido, es común que los objetos digitales se guarden en CD´s, dispositivos portátiles como llaves mayas (*pendrives*) o discos duros externos, correos electrónicos, la nube, computadoras personales y de escritorio, en servidores conectados a los sistemas informáticos transaccionales o en un SGDEA.

Otro aspecto fundamental a destacar es que la Universidad de Costa Rica utiliza sistemas hechos a la medida, lo cual puede aumentar el riesgo para asegurar la continuidad digital porque se depende de una tecnología específica, lo cual no permite la transmisión del conocimiento y crea dependencia para el mantenimiento. Sumado a ello, existe una menor capacidad de asimilar el cambio y por lo tanto se reduce la respuesta a este, generando mayores costos en el soporte técnico a través del tiempo. El uso de tecnologías a la medida dificultan la extracción y preservación de la información, máxime si se utilizan tecnologías que no se basan en estándares abiertos (National Archives, s.f, B-Report 2.6).

El aspecto anterior conlleva a que se siguen utilizando sistemas obsoletos para desarrollar las funciones institucionales, por lo cual resulta difícil mantenerlos funcionando adecuadamente. Además, considerando el rápido avance tecnológico, se complica el asegurar la gestión del cambio, aumentando el costo en el mantenimiento al tiempo que se complican las acciones para dar continuidad del negocio y se complejiza la extracción y uso de la información gestionada en equipos y sistemas obsoletos, aumentando el riesgo de pérdida de documentos y datos públicos.

Como se muestra en la Tabla 12, las distintas oficinas universitarias tienen bajo su custodia documentos con plazos de conservación que van de 5 a más de 30 años. Sin embargo, se detectó un alto riesgo porque existe una falta de instrumentos archivísticos desarrollados en su totalidad, para garantizar la correcta disposición final de la información (conservación o eliminación).

Específicamente, no están creadas todas las Tablas de Plazos de Conservación, en las cuales se determinen las vigencias en las cuales se deba preservar la información, asegurando su uso durante los plazos administrativos y, en muchos casos, su obligatoria preservación permanente por tratarse de documentos con valor histórico-cultural.

c. Gestión del riesgo en cuanto a la preservación digital

Tabla 13. *Gestión del riesgo en cuanto a la preservación digital en la Universidad de Costa Rica.*

Situación	Riesgo	Acciones por implementar
Los riesgos para la información personal y sensible, han sido reconocidos y gestionados; la gobernanza de la información o la gestión del riesgo está desarrollada únicamente para este tipo de información.	Medio bajo	El ADiUCR debe gestionar los riesgos para toda la información de la UCR y no únicamente la de carácter personal o sensible. Para ello se deben asignar responsabilidades específicas en la Política de Preservación Digital, como la seguridad, gestión de incidencias y la preservación de documentos y datos.
Los riesgos para la continuidad digital han sido reconocidos e incluidos en un registro de riesgos de información corporativa, pero no son gestionados activamente .	Medio bajo	El AUROL debe realizar una evaluación anual de riesgos, relacionada con la preservación digital.
Los incidentes relacionados con la gestión de la información se atienden localmente en cada Unidad y la institución no ha definido procesos corporativos para la gestión de incidentes.	Medio alto	Los incidentes de información deben ser gestionados desde el ADiUCR mediante la estrategia de preservación, con la participación activa del SIRO, ya que la información universitaria va a estar centralizada.
Se realizan pruebas de preservación digital de la información solo después de cambios significativos que la puedan afectar, pero estas acciones no están planificadas.	Medio alto	La Política de Preservación Digital debe incluir el aseguramiento de la cadena de custodia ininterrumpida de la información, para mantener la integridad, fiabilidad, usabilidad y disponibilidad de los documentos y datos custodiados.
La UCR no cuenta con procesos de gestión de cambio institucional, sino que los cambios específicos se establecen por cada caso en particular.	Medio alto	La Política de Preservación Digital debe considerar las estrategias necesarias para gestionar los cambios que impactan la preservación digital de manera planificada (por ejemplo, la obsolescencia tecnológica de sistemas y equipos).
La UCR espera experimentar cambios en la introducción de nuevas tecnologías y cambios en la normativa para la gestión de la información.	Bajo	En la Política de Preservación Digital se debe asignar la responsabilidad al Centro de Informática de desarrollar los servicios, aplicaciones e integraciones necesarias para que los sistemas institucionales transfieran la

Situación	Riesgo	Acciones por implementar
		información al ADiUCR. Esto implica la coordinación entre la CIADi y el Centro de Informática para llevar a cabo el desarrollo futuro de tecnologías acordes con las necesidades institucionales. La CIADi debe desarrollar propuestas y modificaciones normativas para asegurar la preservación digital, las cuales deben ser aprobadas por las altas jerarquías de la UCR, es decir, la Rectoría y el Consejo Universitario.
La estrategia de TIC de la UCR incluye la normalización del entorno TI (minimizando los sistemas hechos a la medida), el uso de estándares abiertos, formatos y estructuras de datos, y aumentando la interoperabilidad entre los sistemas.	Medio bajo	Impulsar el uso de tecnologías abiertas en la UCR para facilitar la interoperabilidad de los sistemas con el ADiUCR (Resolución R-254-2014: *"Directrices para la puesta en marcha del plan de migración a Software Libre en la Universidad de Costa Rica").*
Existe normativa vigente que le indique al personal dónde guardar la información y cómo organizarla, pero no se entiende bien y se aplica de manera inconstante.	Medio bajo	Mediante el proyecto de preservación digital se realizarán las transferencias al ADiUCR, por lo cual las Unidades no deberán almacenar la información en sus sistemas ni equipos. Dichos sistemas serán de uso transaccional.
No existe normativa vigente para definir el nombre y descripción (metadatos) de los documentos y evidencias de información, pero hay buenas prácticas esporádicas en la institución.	Medio alta	En el Protocolo de Transferencia se deben definir los metadatos necesarios para la transferencia y conservación de la información. Estas acciones ayudarán a la normalización de los metadatos que se deben generar en sistemas desarrollados a futuro.
Existen tablas de plazos de retención, pero no son aplicados o actualizados de forma sistemática.	Medio bajo	La CUSED debe definir los plazos de conservación de las series documentales que no han sido evaluadas.

Fuente: Elaboración propia a partir de los resultados de la aplicación de la *Digital continuity self-assessment tool.* 2023.

Para llevar a cabo una correcta gestión del riesgo para la continuidad digital, es fundamental que las políticas de preservación digital definan procedimientos específicos, de acuerdo con la realidad institucional y los conocimientos que deben tener las personas. Además, deben establecerse los objetivos y el alcance, para describir los procesos para identificar, controlar, monitorear y revisar los riesgos (The National Archives, 2011, p 9).

Como se muestra en la Tabla 13, en la Universidad de Costa Rica se esperan cambios en el ámbito tecnológico, por lo cual se ha previsto la normalización del entorno TI, por medio del uso de estándares y formatos abiertos. Este aspecto puede ser beneficioso ya que en el futuro, podría facilitar la interoperabilidad de los sistemas.

La institución no cuenta con un repositorio digital seguro que permita definir dónde y cómo se debe guardar la información, por medio de normas archivísticas, donde por ejemplo, se incluyan esquemas de metadatos que permitan identificar los objetos digitales y sus contextos (metadatos de contexto, de descripción y de preservación).

2.4.2. Análisis del contexto y definición del archivo

Para determinar cómo debe ser el Archivo Digital que requiere implementar la Universidad de Costa Rica, resulta fundamental conocer el contexto en el que se desarrollan las funciones que dan como resultado los documentos de archivo y la información necesaria para continuar con la operativa universitaria.

De esta manera, se aplicó el instrumento para la Identificación del Tipo de Archivo, llamado "Gestión de Objetos Digitales en las Unidades de la Universidad de Costa Rica" (Anexo 2), a las mismas 14 unidades universitarias a las que se les envió la *Digital continuity self-assessment tool*, obteniendo los siguientes resultados (Tabla 14):

Tabla 14. *Identificación del tipo de archivo.*

Ámbito	Resultado o conclusión	Observaciones
Propósito y funciones del Archivo Digital	La Universidad de Costa Rica requiere la implementación de un Archivo Digital, el cual tenga la capacidad de cumplir con las disposiciones vigentes que permitan la preservación digital a largo plazo y el aseguramiento de la Cadena de Custodia de la información.	Actualmente la UCR no cuenta con un Archivo Digital que permita la preservación de la información a largo plazo, así como el aseguramiento de la Cadena de Custodia. Los documentos de archivo y las evidencias de información que se generan en soporte electrónico a raíz de las funciones que desarrolla la UCR, no cuentan con un mecanismo eficaz para asegurar su autenticidad, integridad, fiabilidad y usabilidad a lo largo del tiempo que sean requeridos. Por esta razón, la creación del Archivo Digital, debe considerarse como un objetivo estratégico institucional, que permita asignar los recursos necesarios para su implementación y mantenimiento.
Dimensiones que debería tener el Archivo Digital	El Archivo Digital propuesto para la UCR, debe disponer de capacidad para dar acceso a distintos perfiles de usuarios y deberá prever un crecimiento progresivo de los usuarios que permite.	La cantidad de usuarios estimada para iniciar el funcionamiento del Archivo Digital, dependerá de un plan piloto de implementación, según la cantidad de unidades académicas, administrativas y de investigación, inscritas que participen. Se esperaría contar con un alto volumen de objetos digitales por año, sin embargo, no se cuenta con los datos exactos de producción documental anual de cada una de las distintas unidades universitarias.
Relativo a la seguridad en las operaciones diarias que se requieren regular para el Archivo Digital	El Archivo Digital debe contar con las funcionalidades necesarias para establecer controles eficientes, entre los que se definan perfiles y roles de acceso, los cuáles permiten mantener la seguridad e integridad de la información.	Se deben aplicar restricciones de acceso para los documentos que se reciban por medio de las transferencias de las distintas unidades, según los protocolos establecidos. Estas restricciones de acceso deben aplicarse ya que pueden encontrarse datos de acceso restringido o datos sensibles que no pueden estar abiertos al público en su totalidad. La información que sea de acceso irrestricto, deberá estar disponible en todo momento.
Soluciones tecnológicas y aspectos sobre el proceso de implementación	El Centro de Informática debe proporcionar la infraestructura tecnológica que requiere el Archivo Digital, además se propone el uso de *software* libre especializado.	Debido a la diversidad y complejidad de las aplicaciones tecnológicas utilizadas en la UCR, se requiere de un trabajo especializado, en el que debe involucrarse el Centro de Informática, pues actualmente se da el uso de *software* libre y propietario dentro de las Unidades. Por lo que el Archivo Digital, debe tener la capacidad de recibir transferencias de información en ambos casos y ofrecer una solución integral que permita la preservación a largo plazo de toda la información que requiere la institución para el cumplimiento de las funciones que desarrolla.

Fuente: Elaboración propia a partir de: Castillo-Solano y Umaña-Alpízar, 2018.

Cabe resaltar que de las 14 unidades encuestadas, se recibieron respuestas únicamente de 7, por lo cual, se sigue denotando la falta de posicionamiento del tema de Archivo Digital en la Universidad de Costa Rica.

Las respuestas obtenidas muestran que las Unidades tienen conocimiento de las clases documentales que gestionan, donde predominan los documentos textuales, los cuales son producidos por el 100% de los encuestados, seguidos por las fotografías y los videos. Los documentos de audio son los que se producen en menor cantidad.

Otro aspecto que es conocido por los encuestados es el nivel de restricción que posee la información que está bajo su custodia. Por esto, indican que el 100% de las Unidades posee documentos de acceso público. El 71,4%, indica que poseen otros documentos que contienen datos sensibles, es decir, información relativa al fuero íntimo de la persona, como por ejemplo los que revelen origen racial, opiniones políticas, convicciones religiosas o espirituales, condición socioeconómica, información biomédica o genética, vida y orientación sexual, entre otros. Además, el 57,1% señaló que custodia datos personales de acceso irrestricto, como los contenidos en bases de datos públicas de acceso general.

Con respecto a las estrategias que utilizan las Unidades para el almacenamiento de la información digital, por un lado, el 100% indicó que usan dispositivos propios (servidores propios, dispositivos almacenamiento portátiles, etc.) y, además, utilizan servidores del Centro de Informática. Por el otro lado, solo el 14,3% señaló que almacenan por medio servicios externos contratados.

Específicamente en cuanto a los dispositivos de almacenamiento, se utilizan servidores del CI (100%), discos duros externos (71,4%), computadoras personales (71,4%), la nube (85,7%) y otros dispositivos como llave maya, CD, DVD (71,4%).

También, se muestra una amplia disparidad en las respuestas específicas como la cantidad de objetos digitales generados, el espacio de almacenamiento requerido y la cantidad de usuarios que se atienden, ya que las Unidades no tienen claridad de estos datos ni existe una metodología que permita determinar estos aspectos.

2.5. Sistemas o herramientas del mercado

2.5.1. Análisis de herramientas para la preservación digital

Para desarrollar un Modelo de Preservación Digital Sistémica que sirva como base para la puesta en funcionamiento de un Archivo Digital, es fundamental analizar, de manera previa, distintas aplicaciones tecnológicas que han sido desarrolladas tanto por instituciones gubernamentales como por empresas privadas, nacionales o internacionales. Este análisis, permitirá que la Universidad de Costa Rica tenga una base para determinar si alguna de estas opciones satisface los requerimientos establecidos o si es necesario que se desarrolle una herramienta a la medida para la preservación de su información digital.

En consecuencia, se procedió a elaborar y aplicar el instrumento de "Evaluación de aplicaciones tecnológicas desarrolladas para preservación y archivo digital" (Anexo 3), para algunas de las soluciones disponibles. En este instrumento se evalúan las principales características y funciones que poseen estos sistemas, incluyendo los requerimientos archivísticos y tecnológicos. Para ello, se han elegido aplicaciones de preservación digital que, según las empresas o instituciones encargadas de su desarrollo y/o administración, han sido basadas en el modelo OAIS.

De esta manera, a continuación se presentan, en orden alfabético, las aplicaciones analizadas:

- ARCA

Es un *software* propietario, de la empresa *Business Integrators Systems Limitada*, desarrollado como un repositorio de preservación para objetos digitales. Fue creado con base en las normas UNE-ISO 15489 y UNE-ISO 14721 para la implementación del modelo OAIS. La compañía indica que se brinda el soporte tecnológico para llevar a cabo la custodia, acceso, difusión, interoperabilidad y preservación de la información digital (Business Integrators, 2022).

Al estar basado en el modelo OAIS, el sistema permite la creación de paquetes de información SIP, AIP y DIP, y la firma digital para los paquetes AIP. Permite el almacenamiento de los objetos digitales tanto de forma local, es decir, en servidores de los clientes, como en la nube (Business Integrators, 2022).

- Archivematica

Es un *software* libre de código abierto, creado por la empresa Arterfactual Systems. Se ha desarrollado para cumplir con las normas internacionales ISO 14721 (modelo OAIS), Dublin Core, METS, PREMIS.

Dentro de sus funciones principales, se encuentran: el procesamiento de objetos digitales, desde que son introducidos en el sistema hasta su publicación acorde al modelo funcional ISO-OAIS; monitorear y controlar los micro-servicios de ingesta y preservación; generar paquetes SIP, AIP y DIP e integrar otras herramientas tecnológicas para preservar la información digital (Artefactual Systems, 2022).

Con respecto a este último punto, Archivematica se puede utilizar como una herramienta de *backend* para la creación de los paquetes archivísticos, a través de su integración con otras aplicaciones como AtoM o ArchivesSpace, que funcionen como *frontend*. Archivematica es compatible con CONTENTdm, Islandora, LOCKSS, DuraCloud, OpenStack, Archivists' Toolkit, BitCurator, BagIt, PRONOM, entre otros.

- ArchivesSpace

Desarrollado por la empresa Lyrasis, es un *software* de código abierto, está basado en estándares internacionales como ISAD-G (EAD), ISAAR-CPF (EAC-CPF), CSV, MARCXML, Dublin Core (OAI-PMH). Sus principales funciones son "la administración de archivos, como el acceso; descripción y disposición de los materiales procesados, incluidos los contenidos analógicos, híbridos y nacidos en formato digital; gestión de autoridades (agentes y sujetos) y derechos; y servicio de referencia." (ArchivesSpace, 2022).

El sistema como tal no cumple con el modelo OAIS, pero se ha podido integrar con otras aplicaciones como Archivematica para cumplir con dicho modelo, y en conjunto con DSpace como *software* de repositorio, por ejemplo, en el caso de la Librería Histórica de Bentley, de la Universidad de Michigan (Ochoa-Gutiérrez, Sáenz-Giraldo & Tirado-Tamayo, 2021, p.11).

- DSpace

Es una plataforma *open source,* perteneciente a la empresa Lyrasis. Permite a las organizaciones capturar y describir material digital utilizando un módulo de flujo de trabajo de envío o una variedad de opciones de ingesta programática; también permite distribuir los activos digitales de una organización a través de la *web,* a través de un sistema de búsqueda y recuperación, y preservar los activos digitales a largo plazo (DSpace, 2022).

Según Ochoa-Gutiérrez, Sáenz-Giraldo & Tirado-Tamayo (2021, p.14), DSpace "es el software de repositorio más utilizado en repositorios institucionales, pero no es clara la evidencia respecto a sus posibilidades frente a la implementación de modelos de preservación digital como OAIS", sin embargo, puede ser integrado con otras aplicaciones como Archivematica y Fedora.

- DuraCloud

Consiste en un servicio pago de almacenamiento en la nube, a través de *Amazon Simple Storage (S3)*, para preservación digital, así como para acceder y compartir datos. Para ello brinda herramientas y soporte de transferencia de información a la nube. También permite realizar copias de seguridad y su sincronización.

Realiza informes del estado de los datos almacenados, para detectar si sufrieron algún problema en su integridad. Permite la integración con otros sistemas como DSpace o Archive-It. Como tal, DuraCloud no puede ser utilizada como un archivo digital, sino como una herramienta para el almacenamiento de objetos digitales (DuraCloud, 2022).

- Exlibris Rosetta

Este sistema es propiedad de la empresa ExLibris. Es una solución para la conservación y gestión de objetos digitales de bibliotecas, archivos, museos y otras instituciones, con alojamiento local o en la nube. Está basada en normas internacionales como el modelo OAIS y los estándares PREMIS y METS. Su principal función es la gestión y preservación de objetos digitales de extremo a extremo (*end-to-end*) (Rosetta, 2022).

- Fedora (*Flexible Extensible Digital Object Repository Architectur*e)

Plataforma de repositorio digital *open source*, perteneciente a la empresa Lysaris. Permite la gestión y difusión de contenido digital, el acceso y la conservación. Se utiliza para la gestión de colecciones grandes o complejas de materiales históricos, culturales y datos científicos. Permite la integración con otras aplicaciones como Hydra, Samvera, Islandora y DSpace (RODA, 2022).

- ICA-AtoM (*Access to Memory*)

Es un software libre de código abierto, basado en estándares de descripción archivística y esquemas de metadatos (ISAD-G (EAD), ISAAR-CPF (EAC-CPF), ISDIAH, ISDF, Dublin Core, MODS DACS. Además, puede ser integrado con otras aplicaciones como Archivematica.

Sus principales funcionalidades son: agregar registros de ingresos, descripciones archivísticas, registros de autoridades, entre otras; navegar a distintos niveles (objetos, instituciones, personas, entre otras); administrar ingresos, donadores, unidad de almacenaje, titulares de derechos; importar/exportar en formatos CSV y XML, de descripciones archivísticas, autoridades, entre otros; exportar descripciones en varios esquemas como EAD, Dublin CORE, EAC, MODS, entre otras. (Díaz-Majada, 2020, p.17-18).

- LibSafe

Programa informático propietario de la empresa Libnova Digital Preservation. Se indica que esta plataforma implementa la ISO 14721 - OAIS, para la gestión de colecciones de datos y ficheros digitales, desde la ingesta hasta la recuperación de la información (Libnova, 2010-2016).

Entre sus funcionalidades están la comprobación de objetos al ingestar (permisos, validez de los ficheros, entre otras), generar múltiples copias de seguridad, la gestión de formatos y metadatos, permite hacer auditorías de integridad, la búsqueda, visualización y recuperación de la información.

- Preservica

Es un *software* de preservación digital a largo plazo de objetos digitales, dirigido a entidades de industria, gobierno e instituciones culturales. Esta plataforma está basada en la norma ISO 14721, del modelo OAIS.

A través de Preservica se puede realizar la ingesta de los objetos digitales desde otras plataformas como SharePoint, Outlook, Gmail, PastPerfect, DSpace, entre otros. Además, lleva a cabo la preservación digital por medio de la migración de formatos post-ingesta, para mantenerlos usables, mediante otras aplicaciones como DROID, para la identificación de formatos (Preservica, 2022-c, p. 5-6).

- RODA

Esta plataforma se define como un repositorio digital de código abierto, el cual pertenece a la empresa *Free Software Foundation, Inc*. Se desarrolló para cumplir con las unidades principales del modelo OAIS y permite la ingesta, gestión y acceso a varios tipos de objetos digitales. También está basado en estándares como METS, EAD, Dublin Core y PREMIS (RODA, 2022-a).

Algunas de sus funcionalidades son la pre-ingesta (creación de SIP), ingesta (recepción de paquetes SIP y conversión a AIP), administración y acceso a los objetos digitales (SIP, AIP, DIP), la aplicación de acciones de preservación (conversión de formato, *checksum*, entre otras), la estadística de los datos y el registro de riesgos (RODA, 2022-b).

Tabla 15. *Resumen de la evaluación de aplicaciones tecnológicas.*

Nombre	Tipo de Software		Código abierto	Soporte y mantenimiento	Estándares internacionales	Firma digital	Gestiona paquetes SIP, AIP, DIP (OAIS)	Metadatos para paquetes de información	Interoperabilidad
	Libre	Propietario							
ARCA		X	-	X	X	X	X	X	X
Archivematica	X		X	X	X	-	X	X	X
ArchivesSpace	X		X	X	X	-	-	-	X
DSpace		X	X	X	X	-	-	X	X
DuraCloud		X	X	X	-	-	-	X	X
ERA		X	-	X	X	-	X	X	-
Exlibris Rosetta		X	-	X	X	-	X	X	X
Fedora		X	X	X	-	-	-	-	X
ICA-ATOM	X		X	X	X	-	-	X	X
LibSafe		X	X	X	X	-	-	-	X
Preservica		X	-	X	X	-	X	X	X
RODA	X		X	X	X	-	X	X	-

Fuente: Elaboración propia. 2023.

2.5.2. Pruebas en línea de herramientas para la preservación digital

A continuación, se presenta un análisis general de cuatro de las herramientas anteriores, las cuales cuentan con opciones de prueba en línea, con el propósito de ahondar en sus funcionalidades. Cabe destacar que las dos primeras (Archivematica y Preservica), se establecen como herramientas que funcionan para dar el tratamiento de preservación digital basado en el modelo OAIS, por lo cual se incluyen procesos de ingesta, almacenamiento y consulta de la información.

Los otros dos programas informáticos (AtoM y ArchivesSpace), también se promocionan como herramientas para dar solución a la preservación digital, sin embargo, funcionan principalmente como *front-ends,* es decir, para ser la interfaz que se muestra al usuario y por medio de las cuales se puede realizar la descripción archivística y el acceso de los objetos digitales que serán sujetos de preservación.

Las pruebas de las herramientas se presentarán en orden alfabético.

Archivematica:

Es una herramienta de *software libre*, a cargo de la compañía Artefactuals Systems Inc. Se desarrolló para cumplir con el modelo OAIS de la Norma ISO 14721, y con estándares como METS, PREMIS, Dublin Core, entre otros.

Sus principales funciones son procesar objetos digitales desde que son introducidos en el sistema hasta su publicación, acorde con el modelo funcional ISO-14721 OAIS; monitorear y controlar los microservicios de ingestión y preservación a través del panel de control; generar paquetes AIP e integrar otras herramientas tecnológicas para preservar la información digital.

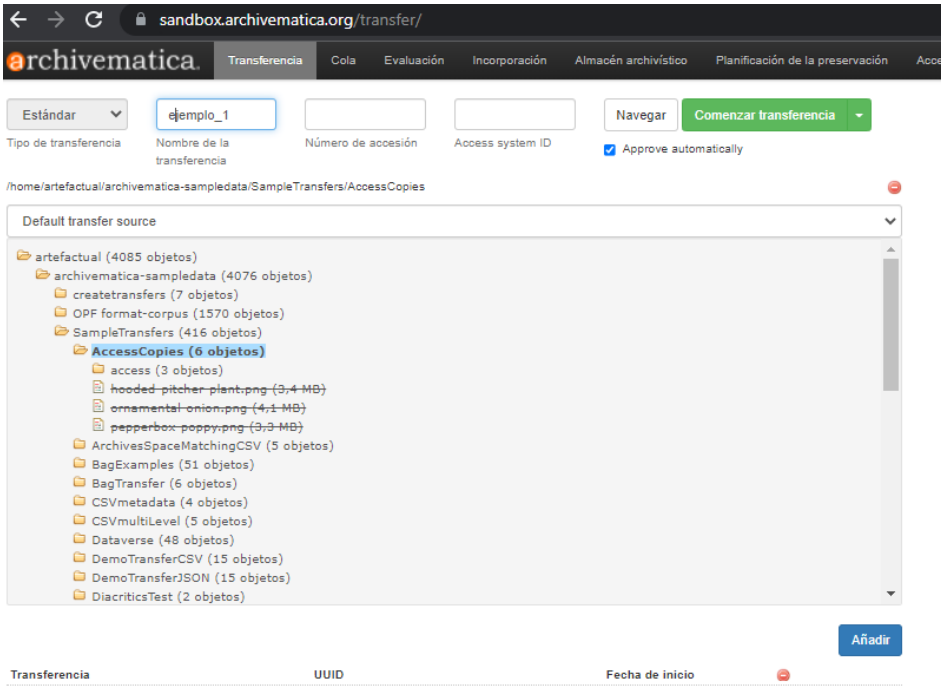
Con respecto a esta última función, Archivematica puede integrarse con otros sistemas como AtoM, DSpace, ArchiveSpace, DuraCloud, BagIt, PRONOM entre otros.

Posee una interfaz de prueba en línea para llevar a cabo la evaluación de la herramienta por medio de una *sandbox*, en un entorno controlado. Para la versión de prueba sólo se pueden realizar tareas con documentos que han sido facilitados previamente por la empresa, es decir, si se requiere utilizar documentos propios, se debe instalar la herramienta completa.

Una vez que se ingresa a la interfaz de prueba, se observa cada uno de los menús en la barra superior. Con estos se puede llevar a cabo el proceso de transferencia y administración de los documentos que conformarán el archivo digital. Estos procesos se ejecutan por medio de los *microservicios*, los cuales se componen por *trabajos*. Es posible configurar el sistema para determinar cuáles se realizan de forma manual o automática (Artefactual, 2022).

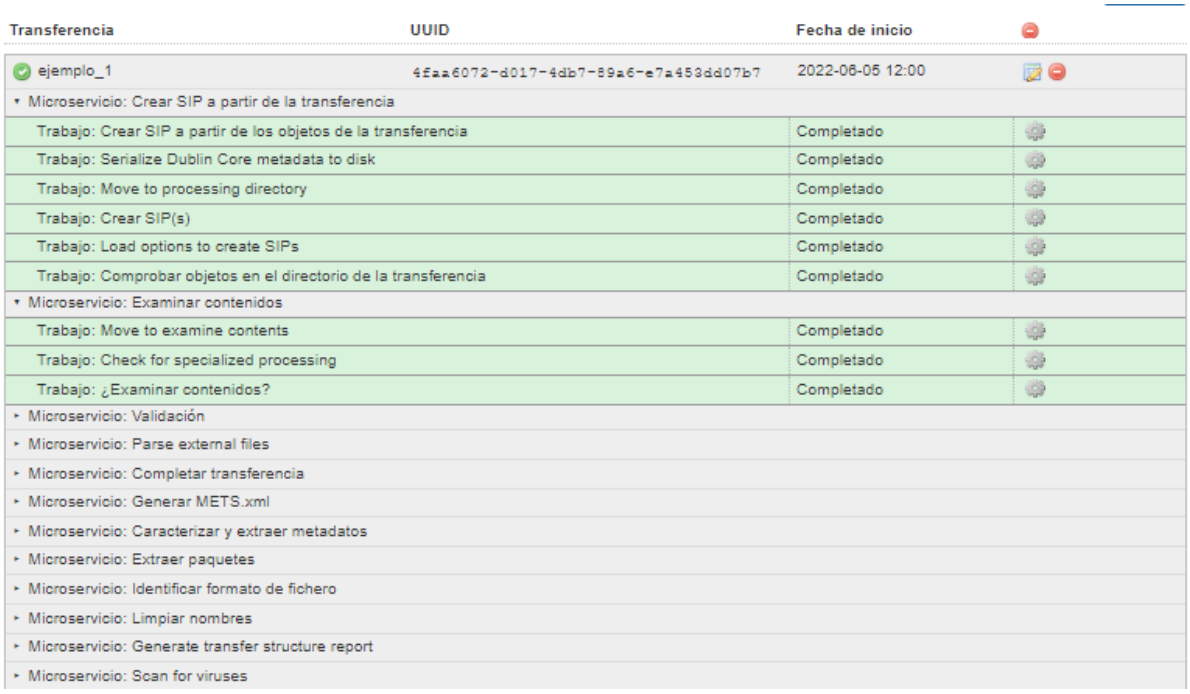
En el proceso de ingreso de los documentos se utiliza el módulo de *transferencia,* mediante el cual se ubican los documentos y se realizan los primeros microservicios (figura 13). Así, se debe añadir la carpeta de los documentos a transferir, se colocan los datos correspondientes y se comienza la transferencia. En este punto, se empiezan a ejecutar los microservicios con los cuales se crearán los paquetes SIP.

Figura 13. *Entorno de prueba de la herramienta Archivematica. Módulo de Transferencias.*



A continuación, el sistema muestra una notificación en el módulo de *incorporación*, que equivale al término *ingesta*, con lo cual se indica que los documentos han sido ingresados en el sistema (figura 14).

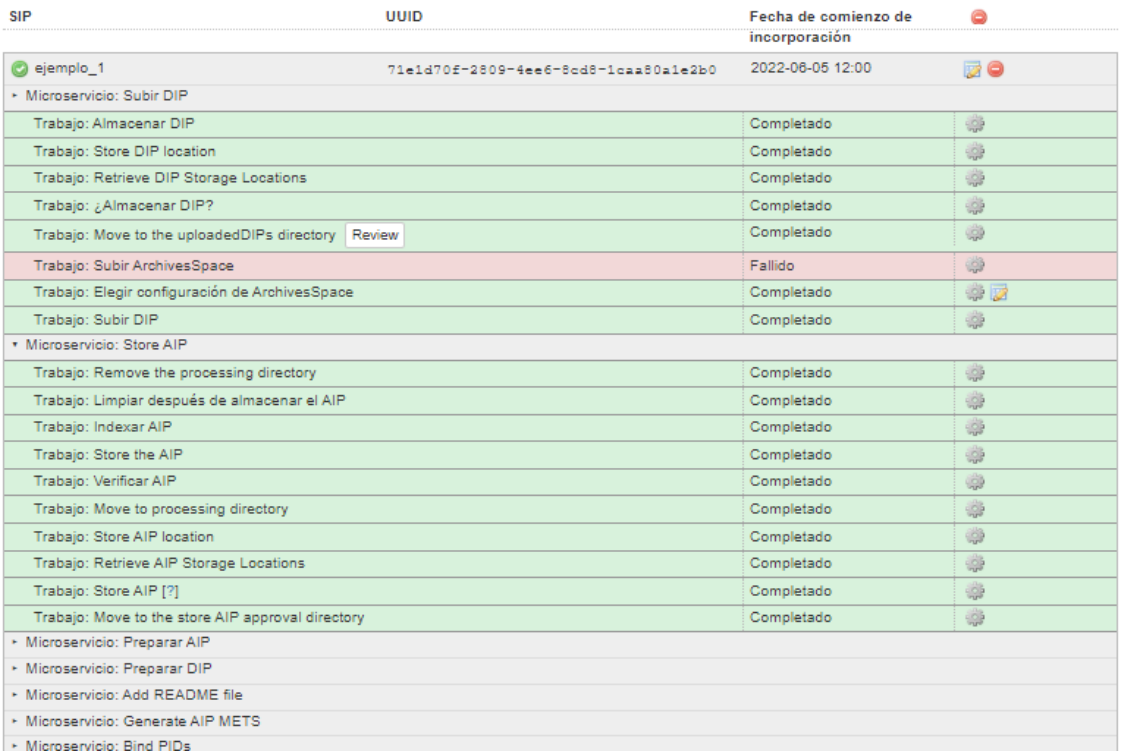
Figura 14. *Entorno de prueba de la herramienta Archivematica. Módulo de Ingesta.*



Transferencia	UUID	Fecha de inicio
ejemplo_1	4faa6072-d017-4db7-89a6-e7a453dd07b7	2022-06-05 12:00
▾ Microservicio: Crear SIP a partir de la transferencia		
Trabajo: Crear SIP a partir de los objetos de la transferencia		Completado
Trabajo: Serialize Dublin Core metadata to disk		Completado
Trabajo: Move to processing directory		Completado
Trabajo: Crear SIP(s)		Completado
Trabajo: Load options to create SIPs		Completado
Trabajo: Comprobar objetos en el directorio de la transferencia		Completado
▾ Microservicio: Examinar contenidos		
Trabajo: Move to examine contents		Completado
Trabajo: Check for specialized processing		Completado
Trabajo: ¿Examinar contenidos?		Completado
▸ Microservicio: Validación		
▸ Microservicio: Parse external files		
▸ Microservicio: Completar transferencia		
▸ Microservicio: Generar METS.xml		
▸ Microservicio: Caracterizar y extraer metadatos		
▸ Microservicio: Extraer paquetes		
▸ Microservicio: Identificar formato de fichero		
▸ Microservicio: Limpiar nombres		
▸ Microservicio: Generate transfer structure report		
▸ Microservicio: Scan for viruses		

En la figura 15, se pueden ver los distintos microservicios y trabajos involucrados en la creación y almacenamiento de los SIP y la posterior conversión y almacenamiento de los AIP.

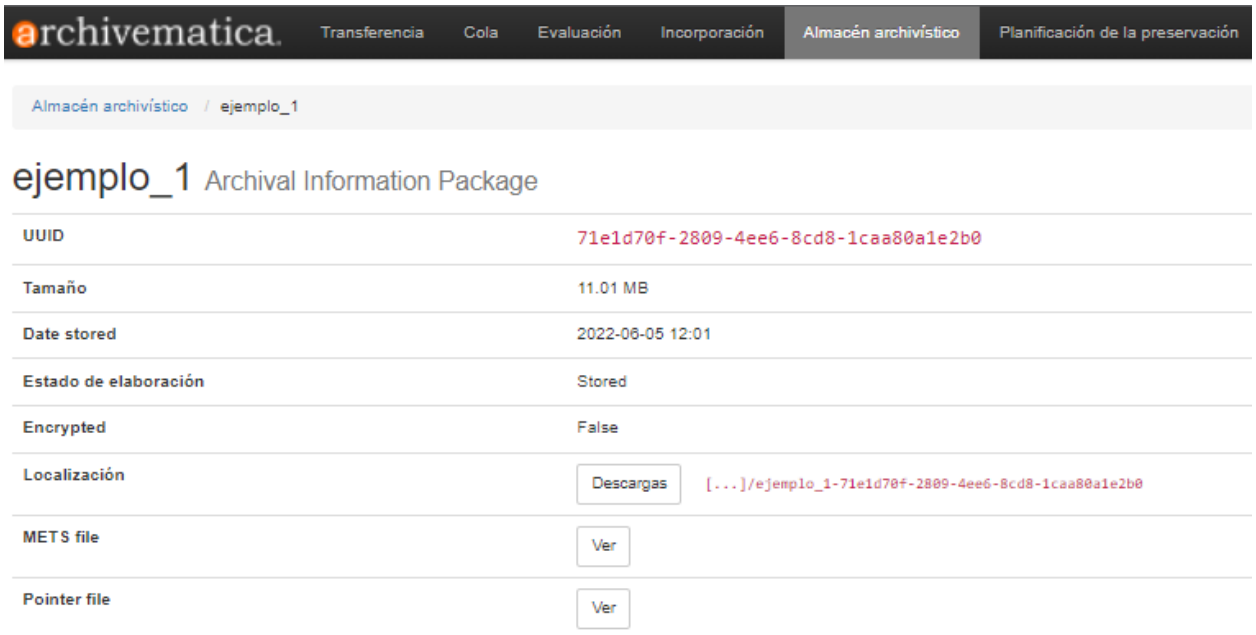
Figura 15. *Entorno de prueba de la herramienta Archivematica. Microservicios y trabajos.*



SIP	UUID	Fecha de comienzo de incorporación
ejemplo_1	71e1d70f-2809-4ee6-8cd8-1caa80a1e2b0	2022-06-05 12:00
▸ Microservicio: Subir DIP		
Trabajo: Almacenar DIP		Completado
Trabajo: Store DIP location		Completado
Trabajo: Retrieve DIP Storage Locations		Completado
Trabajo: ¿Almacenar DIP?		Completado
Trabajo: Move to the uploadedDIPs directory Review		Completado
Trabajo: Subir ArchivesSpace		Fallido
Trabajo: Elegir configuración de ArchivesSpace		Completado
Trabajo: Subir DIP		Completado
▾ Microservicio: Store AIP		
Trabajo: Remove the processing directory		Completado
Trabajo: Limpiar después de almacenar el AIP		Completado
Trabajo: Indexar AIP		Completado
Trabajo: Store the AIP		Completado
Trabajo: Verificar AIP		Completado
Trabajo: Move to processing directory		Completado
Trabajo: Store AIP location		Completado
Trabajo: Retrieve AIP Storage Locations		Completado
Trabajo: Store AIP [?]		Completado
Trabajo: Move to the store AIP approval directory		Completado
▸ Microservicio: Preparar AIP		
▸ Microservicio: Preparar DIP		
▸ Microservicio: Add README file		
▸ Microservicio: Generate AIP METS		
▸ Microservicio: Bind PIDs		

Existen otros módulos para la gestión de la información. Por ejemplo, en el módulo de *almacén archivístico* (figura 16), se pueden observar todas las transferencias que se han realizado, con algunos metadatos generales como el código de identificación único (UUID) que se le asigna a cada una, tamaño, fecha de creación, entre otros. Además, en la casilla de acciones se da la opción de *ver,* en la cual se accede a los detalles de cada transferencia.

Figura 16. *Entorno de prueba de la herramienta Archivematica. Módulo de Almacén Archivístico.*



Al acceder a la opción de descargas, se puede descargar el paquete DIP (figura 17), por medio de un fichero comprimido, en el cual se incluyen los objetos digitales originales que componen la transferencia, junto con un conjunto de documentos, incluidos un fichero XML (figura 18) en el cual se aplica el diccionario PREMIS en METS.

Figura 17. *Paquete DIP descargado del entorno de prueba de la herramienta Archivematica.*

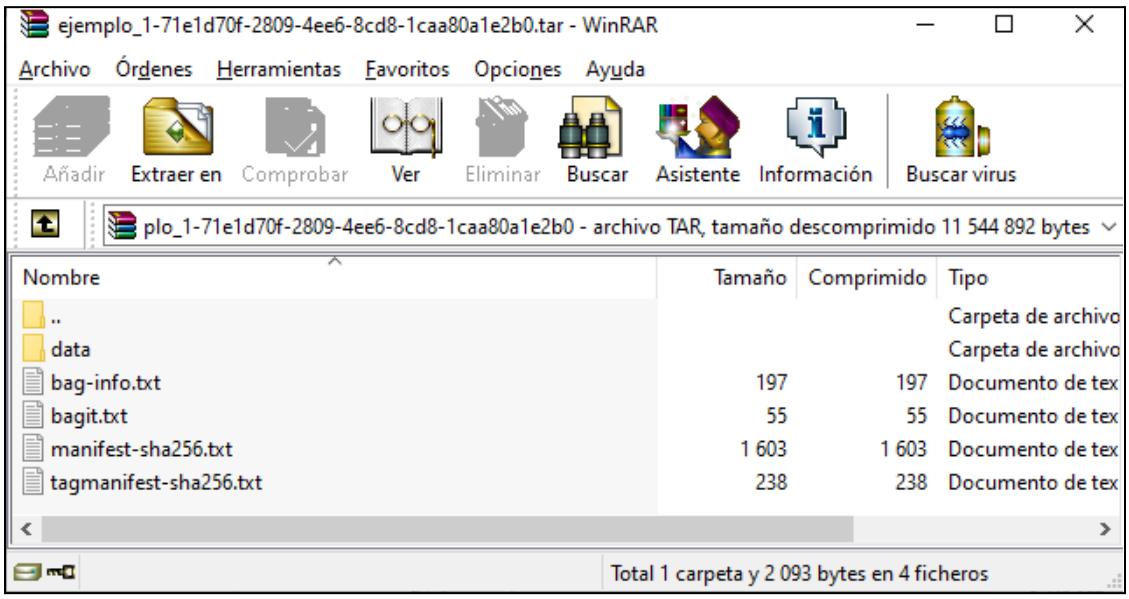
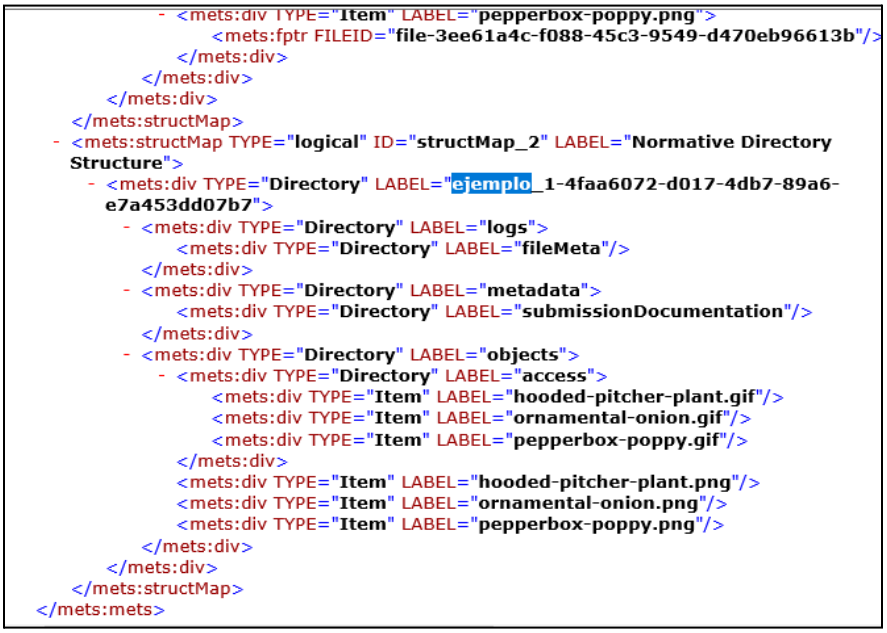


Figura 18. *Fichero XML dentro del paquete DIP descargado del entorno de prueba de la herramienta Archivematica.*



El módulo de *acceso* es utilizado para desplegar los DIP en caso que se hayan enviado a AtoM, mediante una integración de los dos sistemas. Asimismo, la interfaz de *planificación de la preservación,* permite al usuario determinar cómo Archivematica maneja los formatos, al agregar

o editar políticas de formato para la normalización, validación de formatos, flujos de trabajo, entre otros (Artefactual, 2022).

Como se indicó anteriormente, la herramienta de Archivematica tiene una mayor funcionalidad como un *back-end*, para el procesamiento y almacenamiento de los distintos paquetes de información que serán preservados.

ArchivesSpace

Sistema de código abierto desarrollado por la compañía Lyrasis. Cuenta con una demostración de prueba en línea tanto para mostrar cómo se ve y administra la cuenta de usuario externo y cómo los cambios se reflejan en una interfaz de usuario externo. Sus principales funciones son permitir el acceso y gestión de colecciones digitales, la incorporación de nuevos registros, la publicación de materiales digitales y la gestión de autoridades, lugares y derechos. También es posible la generación de metadatos EAD, MARCXML, MODS, Dublin Core, METS.

El módulo de prueba, se encuentra totalmente vacío, por lo cual se debe comenzar con la estructuración del repositorio desde cero. El sistema permite la creación de elementos de distintos niveles, entre estos: repositorios, colecciones, fondos y objetos digitales. Además, permite crear estructuras de metadatos heredables como materias, agentes de autoridad (persona, familia, entidad corporativa), entre otros.

Para este caso se creó un repositorio llamado *ejemplo de repositorio 1* (figuras 19 y 20), al cual se le pueden agregar *campos de repositorio*, que corresponden a datos del repositorio, si es público o no (opción fundamental para poder encontrarlo en la interfaz de usuario externo), organización a la que pertenece, datos de contacto, entre otros.

Figura 19. *Entorno de prueba de la herramienta ArchivesSpace. Ejemplo de repositorio 1.*

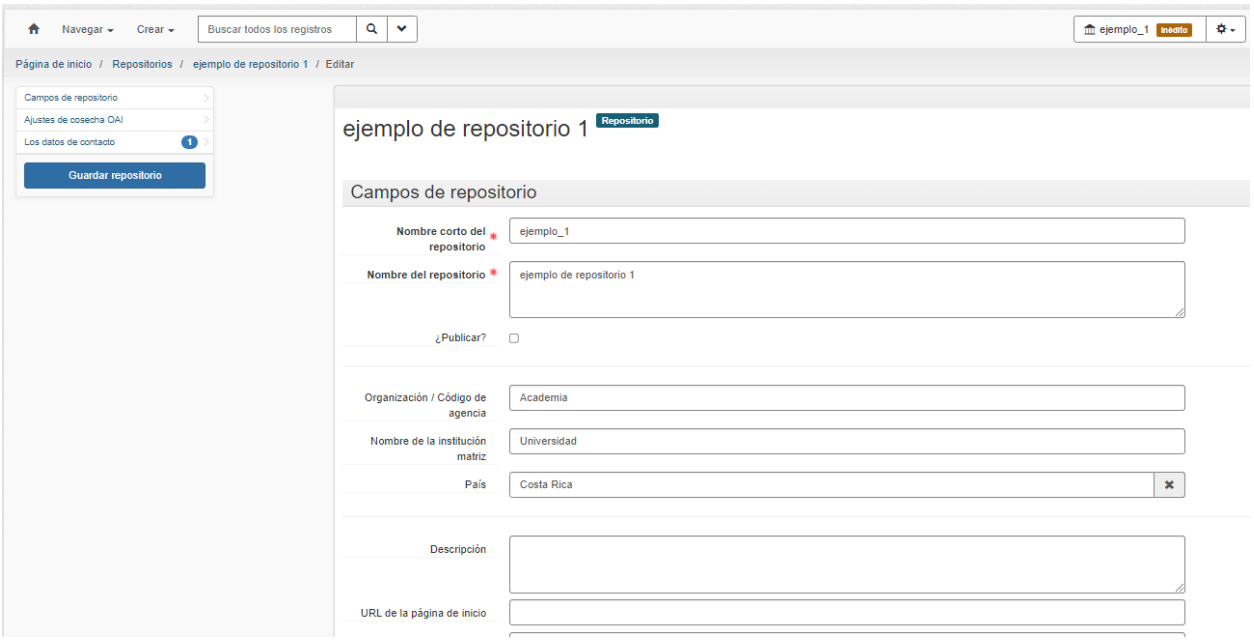
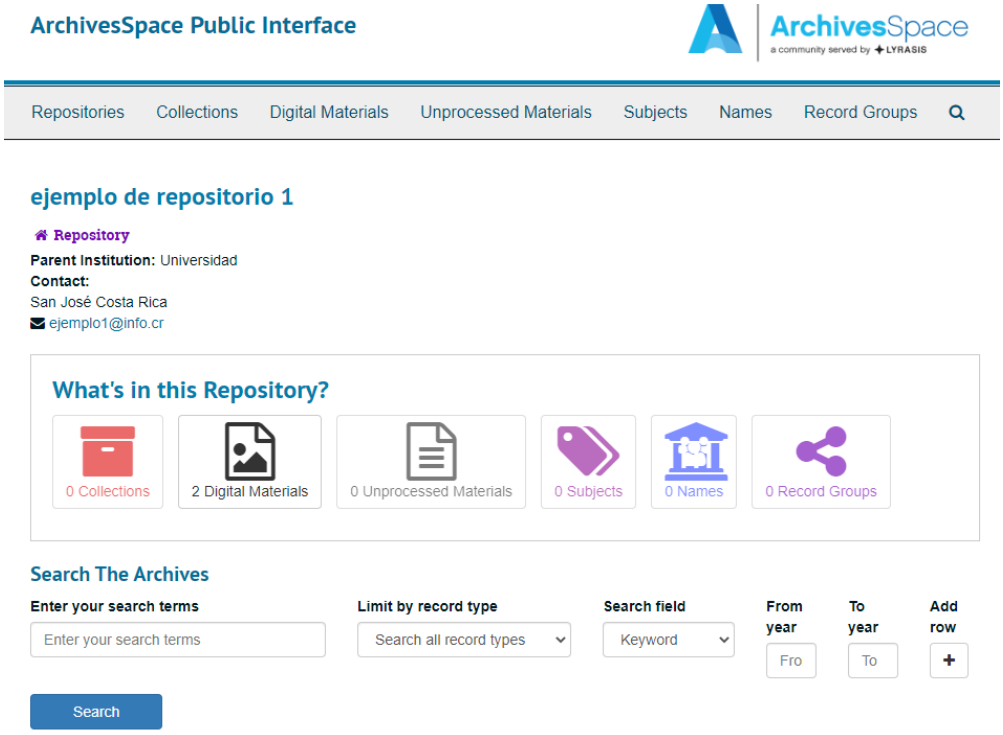


Figura 20. *Entorno de prueba de la herramienta ArchivesSpace. Ejemplo de repositorio 1.*

Dentro de este repositorio, se crearon dos objetos digitales con los nombres *documento de prueba* y *prueba_1* (figuras 21 y 22).

Figura 21. *Entorno de prueba de la herramienta ArchivesSpace. Ejemplo de repositorio 1.*

Figura 22. *Entorno de prueba de la herramienta ArchivesSpace. Ejemplo de repositorio 1.*



AtoM

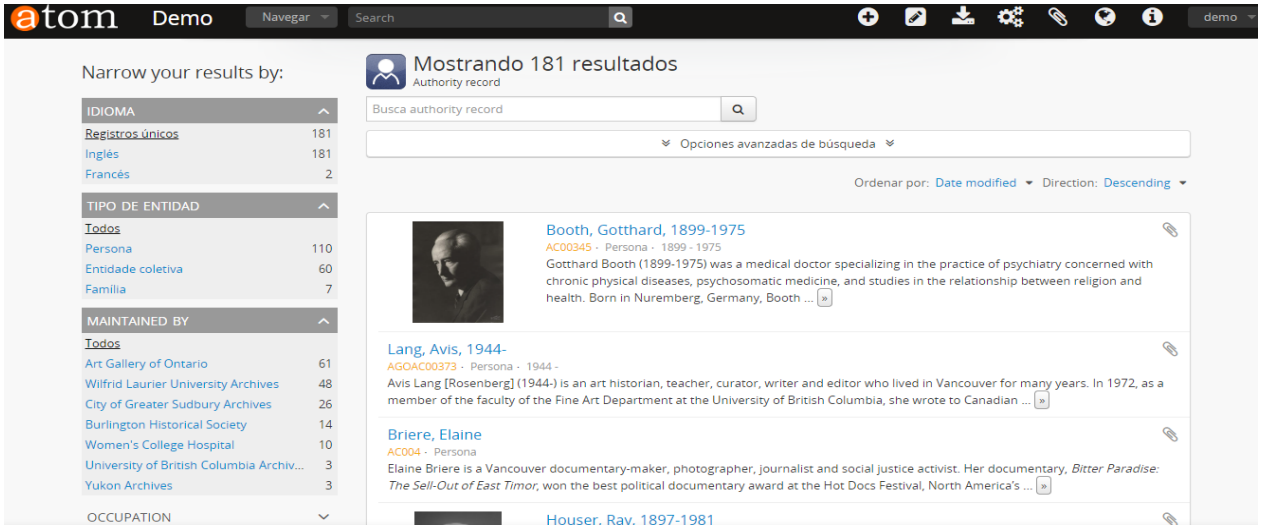
Desarrollo de *software libre*, también a cargo de Artefactual Systems Inc. permite agregar registros de ingresos, descripciones archivísticas, registros de autoridades, entre otros; navegar a distintos niveles; administrar ingresos, donadores, unidades de almacenaje, titulares de derechos, entre otros; además, importar/exportar en formatos CSV y XML, a partir de descripciones archivísticas, autoridades, de varios esquemas como EAD, Dublin CORE, EAC, MODS, entre otros.

El programa AtoM posee un módulo de prueba en línea (figura 23), en el cual se comparten ejemplos completos de colecciones de documentos, desde la perspectiva de un usuario interno del sistema, permitiendo navegar mediante distintos niveles: descripción archivística, personas y organizaciones, instituciones archivísticas, materias, lugares, objetos digitales o funciones.

Figura 23. *Entorno de prueba de la herramienta AtoM.*

A través de los distintos módulos, y con distintos perfiles de usuarios, se pueden crear, editar, eliminar o mover elementos descriptivos y objetos digitales, según corresponda. Además, al ser un sistema basado en normas de descripción archivísticas como la ISAD-G, ISAAR-CPF y la ISDF, se pueden relacionar objetos, series, fondos o instituciones en distintos niveles. También se facilita una barra de búsqueda por texto completo (figura 24).

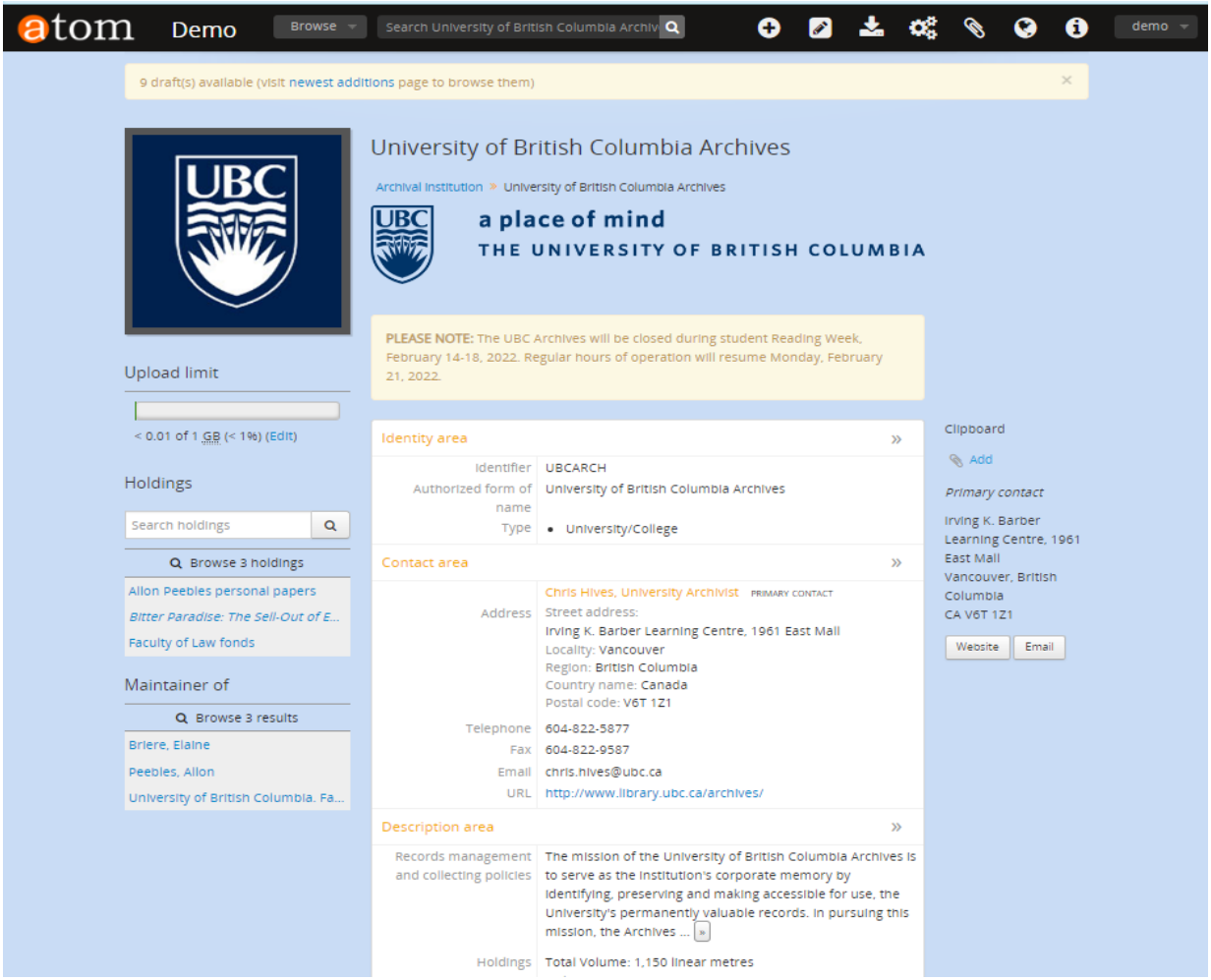
Figura 24. *Entorno de prueba de la herramienta AtoM. Barra de Búsqueda.*



Como ejemplo, se presenta la colección de la University of British Columbia Archives. En la figura 25, se presentan jerárquicamente los documentos que componen la serie documental de fotografías, que ha sido relacionada con la institución.

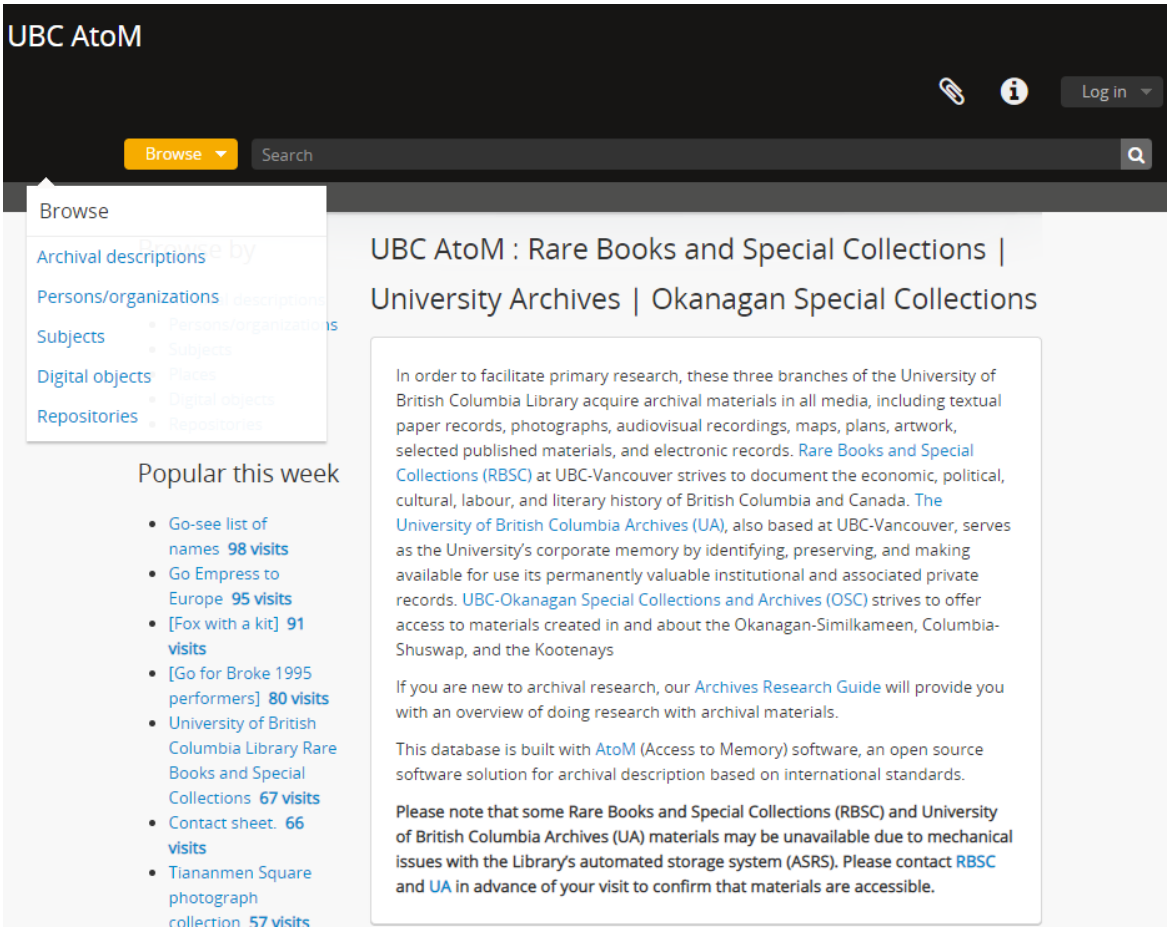
Se muestran también los distintos campos descriptivos de la serie y, en la parte inferior, las opciones para modificar la información. Al lado derecho, se facilitan opciones para importar y descargar metadatos en mediante varios esquemas, por ejemplo, Dublin Core o EAD.

Figura 25. *Entorno de prueba de la herramienta AtoM. Ejemplo University of British Columbia Archives.*



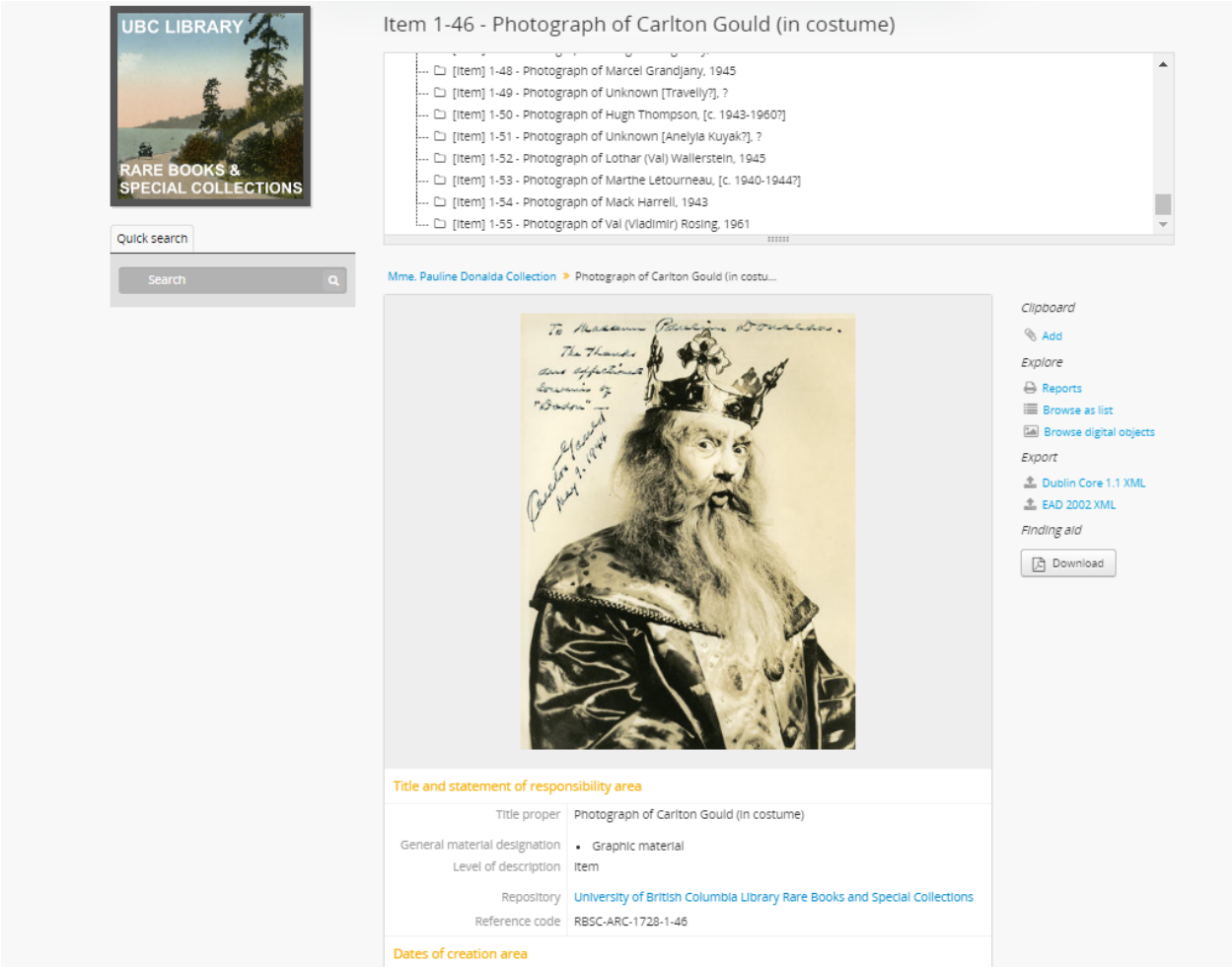
Existen perfiles de usuario externo, mediante los cuales se pueden encontrar los recursos de información creados a través del usuario interno del sistema. Así, por ejemplo, en el caso de la University of British Columbia Archives, se presenta la siguiente página *web* (figura 26):

Figura 26. *Entorno de prueba de la herramienta AtoM. Ejemplo University of British Columbia Archives.*



Navegando por medio de la página, se pueden encontrar los distintos objetos digitales que fueron ingresados al sistema, sus relaciones con otros fondos, series o documentos. Además, las descripciones que les fueron asignadas en cada nivel (figura 27).

Figura 27. *Entorno de prueba de la herramienta AtoM. Ejemplo University of British Columbia Archives.*

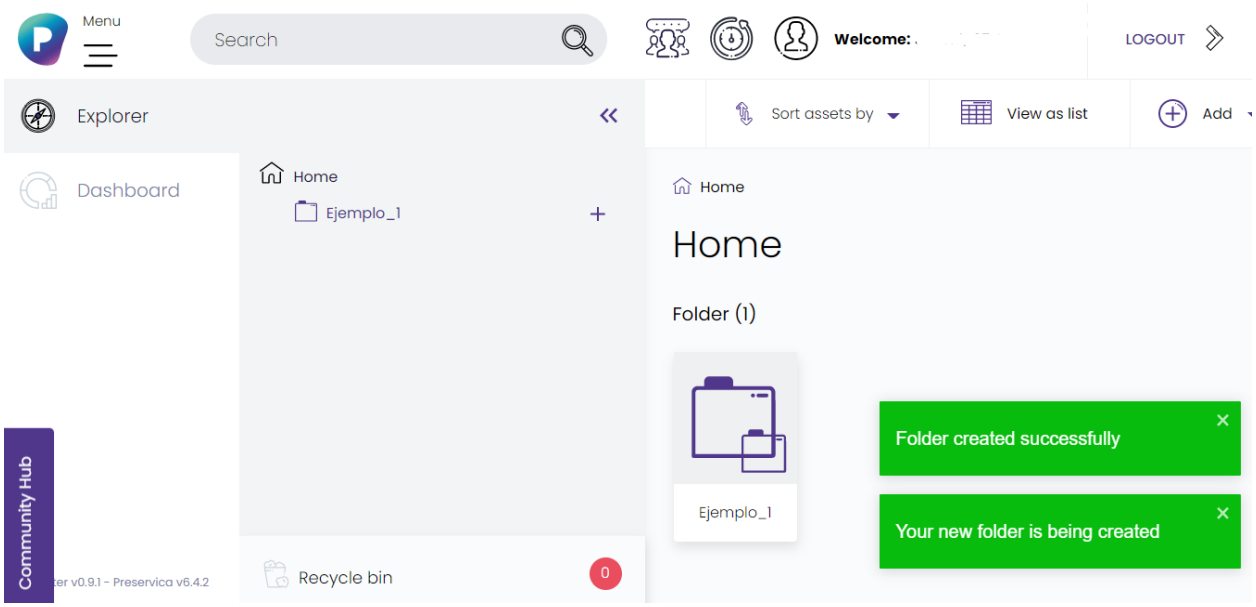


PRESERVICA

Este *software* de pago, se presenta como una solución completa para la preservación a largo plazo de los objetos digitales, alineada con el estándar ISO 14721 - OAIS (Preservica, 2022-a).

No obstante, la empresa brinda la opción de utilizar el *Preservica Starter Edition* (figura 28), con el cual se brinda un total de 5GB gratuitos de almacenamiento de forma permanente, sin la necesidad de descargar o instalar algún *software.* Es así como, mediante esta opción, se presenta el análisis de la herramienta, para conocer su interfaz y funcionamiento.

Figura 28. *Entorno de prueba de la herramienta Preservica utilizando la versión "Preservica Starter Edition".*



La interfaz de usuario interno está conformada por un menú general para configuración de la cuenta, una barra de búsqueda y datos del usuario.

Se presentan dos menús principales. En primer lugar el explorador, en el cual se visualizan las distintas carpetas que puede crear el usuario, de forma jerárquica, para almacenar los objetos digitales. La carga o ingesta de estos objetos (figuras 29 y 30), se hace mediante el botón *add* (agregar) eligiendo las opciones documento individual o comprimido, o por carpetas.

Al cargar dichos objetos digitales, es donde dependiendo del formato original, se aplican un conjunto de acciones para ejecutar: ingesta, caracterización, normalización, migración, detección de virus, identificación de formatos, entre otros.

Figura 29. *Entorno de prueba de la herramienta Preservica Starter Edition. Ingesta.*

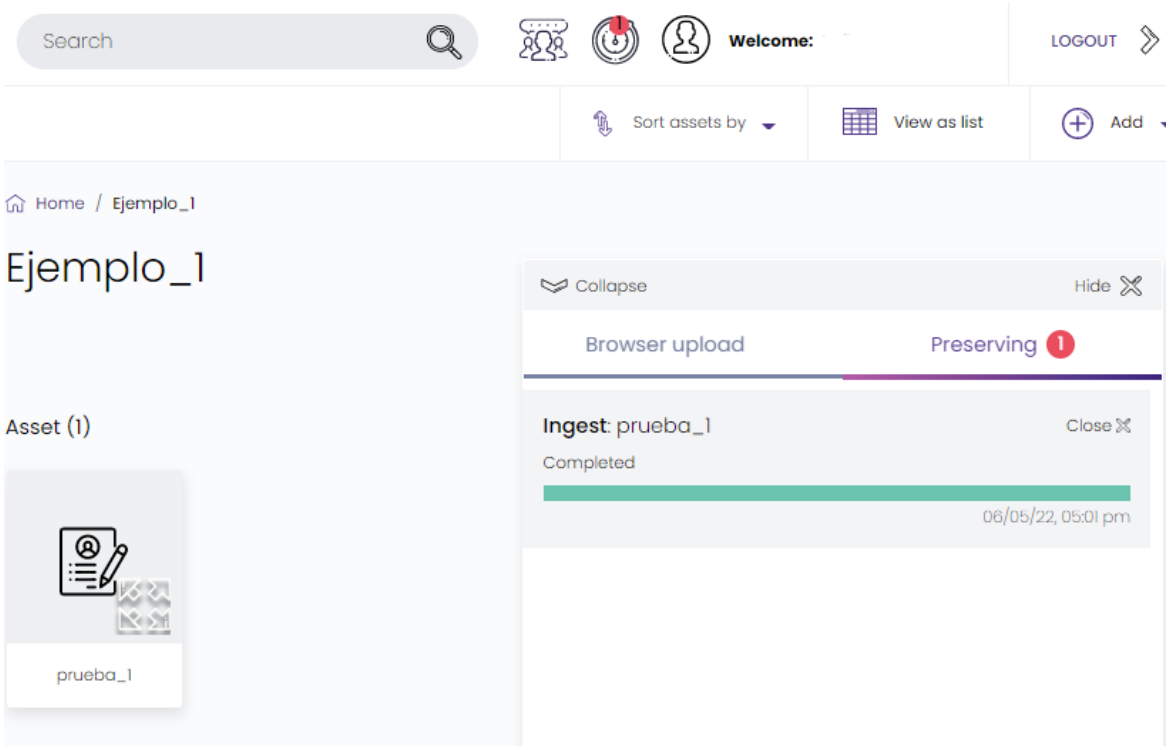
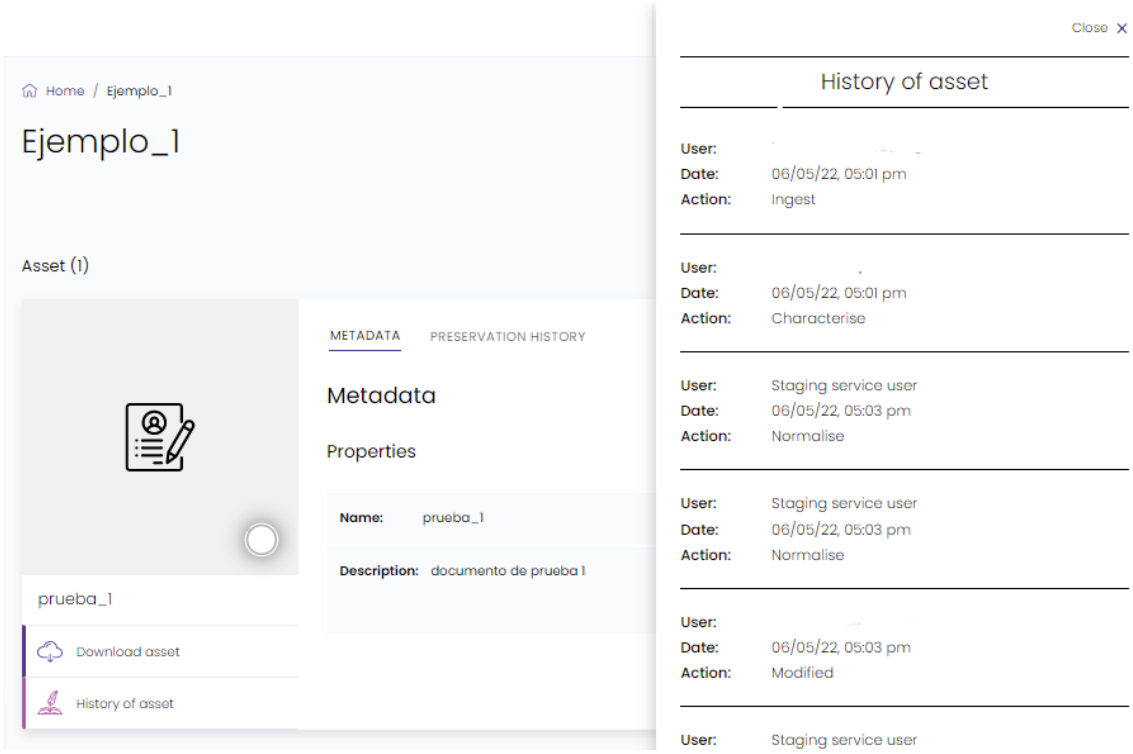
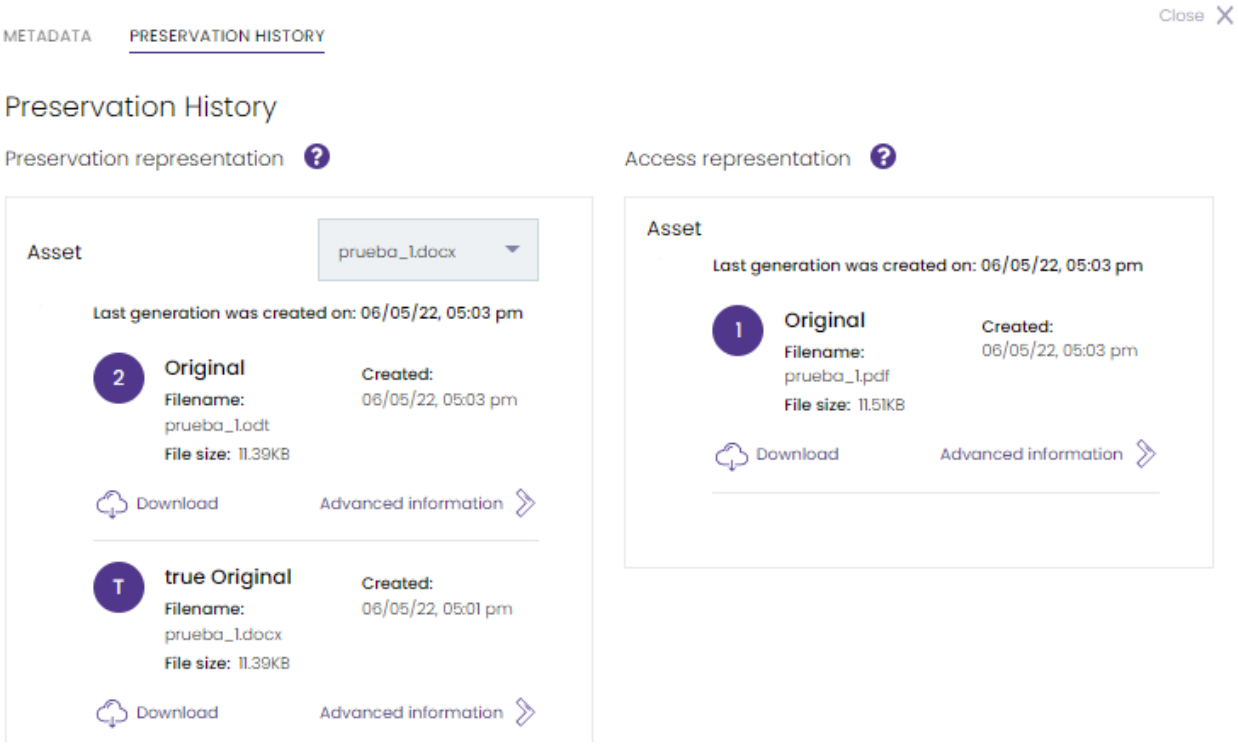


Figura 30. *Entorno de prueba de la herramienta Preservica Starter Edition. Ingesta.*



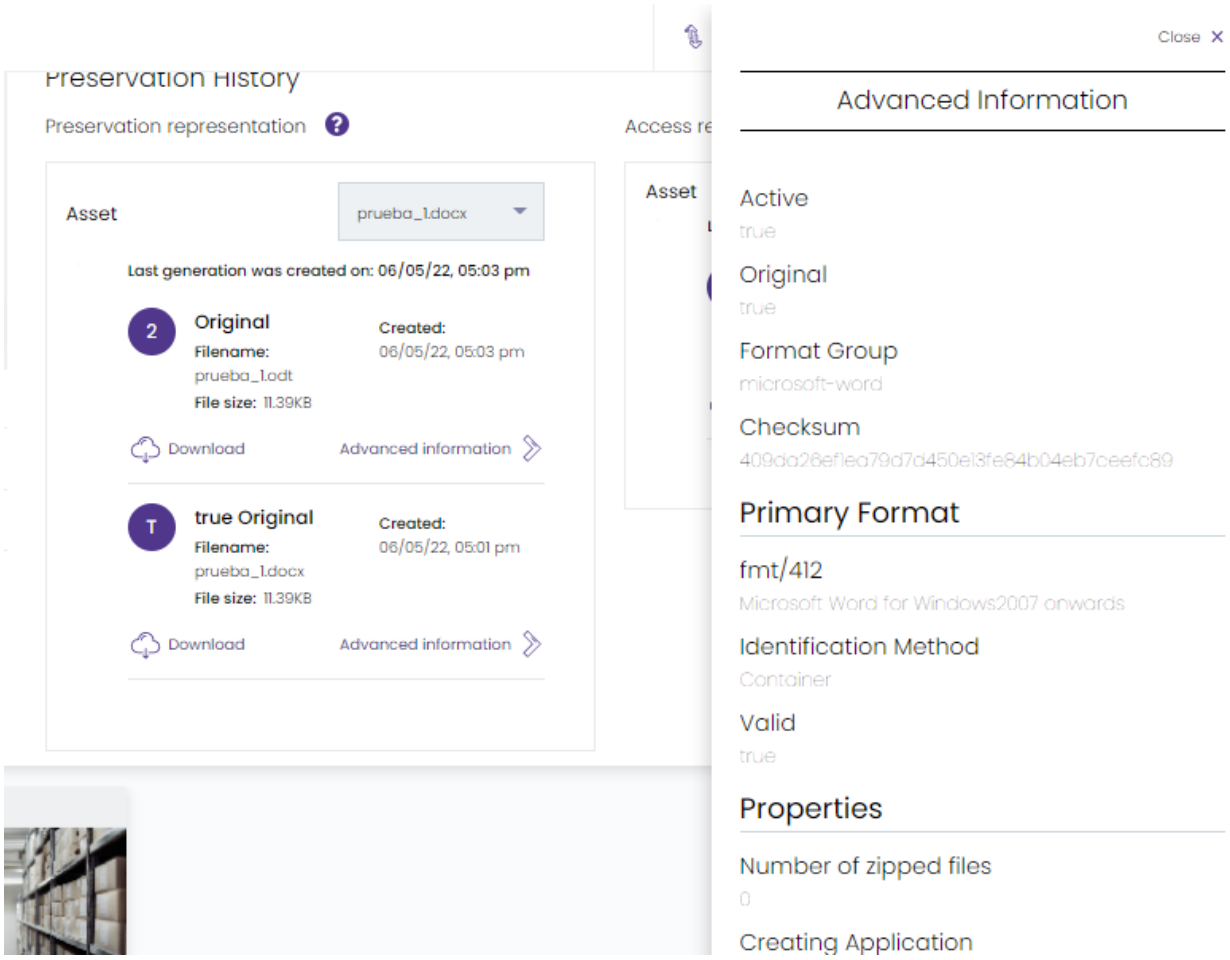
Se realizaron varias pruebas de ingesta con documentos de distintos formatos. Entre estos se encuentra el fichero *prueba_1.docx*. El sistema, realizó la migración automática a los formatos .odt y .pdf. En cuanto a los formatos .docx y .odt, el sistema indica que son objetos de representación de preservación, acotando que el .docx corresponde a un objeto *true original* (figura 31). Además, se crea una copia en formato .pdf de un peso levemente mayor (de 11,39Kb a 11,51Kb), llamado representación de acceso. Cuando se realiza la descarga del documento *prueba_1*, el sistema lo facilita mediante .pdf, a menos que se descargue específicamente el *true original* en formato .docx.

Figura 31. *Entorno de prueba de la herramienta Preservica Starter Edition. Objetos de representación de preservación.*



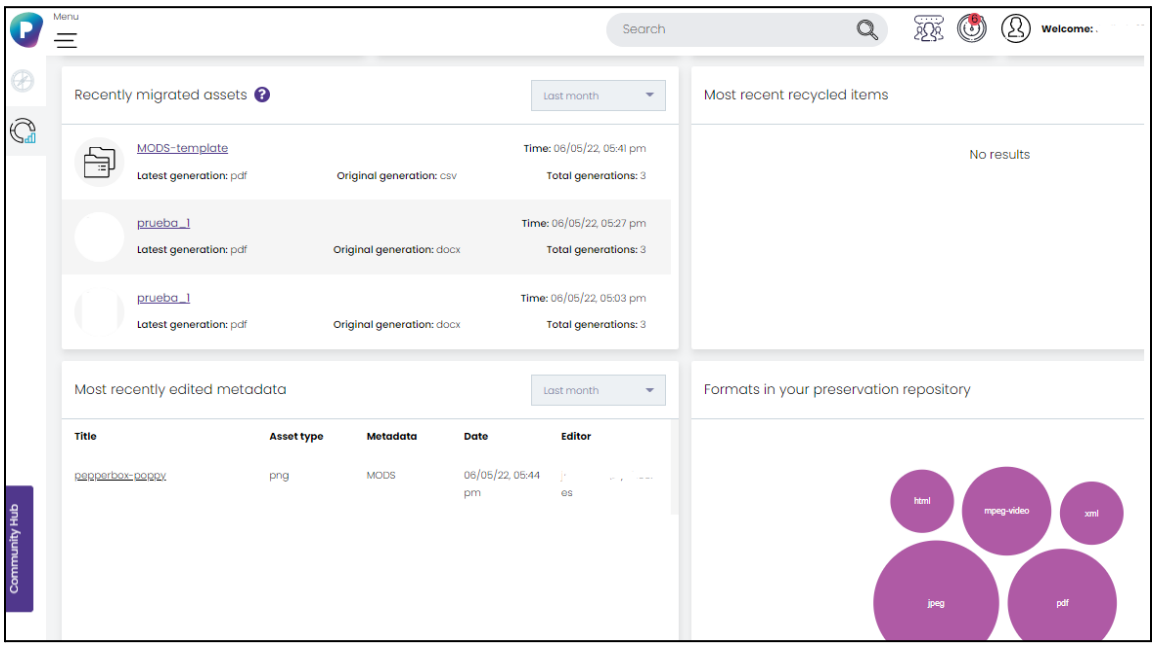
Para cada objeto digital se presenta "información avanzada" con datos como el formato, *checksum*, número de páginas, entre otros (figura 32). Además, por defecto, se pueden añadir metadatos únicamente mediante los esquemas MODS y Dublin Core (más orientados a recursos de biblioteca) aunque según Preservica (2022-b), se pueden incluir otros esquemas de metadatos como EAD.

Figura 32. *Entorno de prueba de la herramienta Preservica Starter Edition. Información avanzada.*



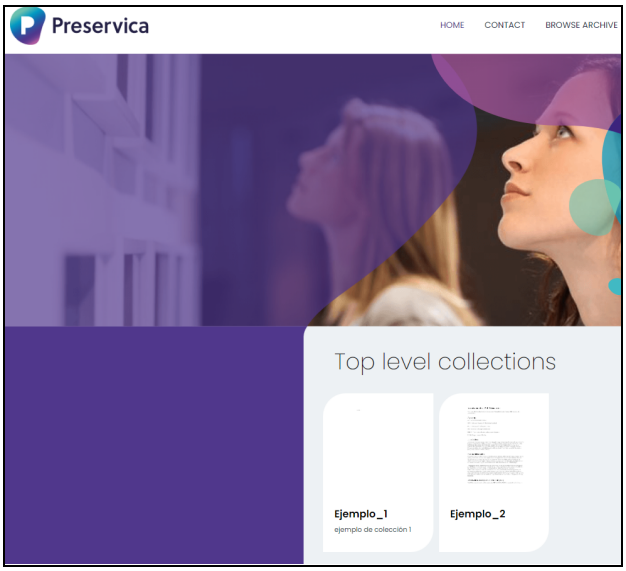
El segundo menú, es el llamado tablero o *dashboard* (figura 33), en el cual se cuantifican datos de los documentos que han sido almacenados en el sistema y el espacio utilizado y disponible con que cuenta el usuario. Sumado a ello, se presentan de forma gráfica y numérica los distintos formatos de objetos digitales que se han incorporado.

Figura 33. *Entorno de prueba de la herramienta Preservica Starter Edition. Dashboard.*



Finalmente, a través de la interfaz *dashboard* y la opción *public portal / view your portal* (figura 34), se puede observar un *front-end* donde se presentan todas las carpetas u objetos individuales, que con antelación han sido seleccionados como públicos, es decir, este es el módulo de navegación para los usuarios externos, quienes pueden visualizar y descargar la información.

Figura 34. *Entorno de prueba de la herramienta Preservica Starter Edition. Public portal / view your portal.*



3. Modelo de Preservación Digital Sistémica para el Archivo Digital.

El proyecto de creación, implementación y mantenimiento de un Archivo Digital, debe realizarse de forma planificada y precisa, con base en normativa desarrollada específicamente para la preservación digital sistémica, porque al tratarse de la gestión y preservación de la información institucional, tiene un alto impacto en todos los niveles de la organización.

Es necesario que la normativa defina los aspectos que conforman al ADiUCR. Por lo tanto, se deben especificar las acciones que deberán llevar a cabo cada una de las partes interesadas, incluyendo a la esfera política, que se refiere a las altas jerarquías tomadoras de decisiones, es decir, la Rectoría y el Consejo Universitario; a las Unidades Administrativas que desarrollarán el trabajo técnico necesario, desde la perspectiva archivística y tecnológica, es decir, el AUROL y el Centro de Informática, respectivamente; y finalmente, a la CIADi como el órgano asesor para el funcionamiento del ADiUCR.

3.1. Política de Preservación Digital

La Universidad de Costa Rica tiene actualmente vigentes las Políticas Institucionales 2021-2025, donde es posible encontrar enunciados relacionados con la gestión del conocimiento organizacional a través del uso de las TIC (Tabla 4).

Dentro de estas políticas, en cuanto al tema de preservación digital de la información, (Consejo Universitario de la UCR, 2020, p.14) resalta la siguiente:

- **Eje VII. Gestión universitaria**
    - **Política 7.4**: *Diseñará y desarrollará los mecanismos de integración de la información universitaria, de forma estandarizada, segura e interoperable, que apoyen la toma de decisiones estratégicas institucionales*.
        - Objetivo 7.4.5: *Fomentar las buenas prácticas para la conservación y preservación del patrimonio documental y el acervo bibliográfico institucional, en formato impreso y digital*.

Esta política se encuentra aprobada al más alto nivel jerárquico de la Universidad, por lo que se debe asegurar que, una vez terminado ese periodo de vigencia (2021-2025), se continúe tomando

en consideración y plasmando la preservación digital como un objetivo primordial en las Políticas que rigen el accionar de la UCR.

Siguiendo esta línea, desde el presente Trabajo Final de Graduación, se propone la adición de otro objetivo dentro de la Política 7.4., para garantizar la preservación de los documentos en soporte electrónico, generados y recibidos por la Universidad:

> ***Objetivo 7.4.6. Asegurar los mecanismos necesarios para la preservación digital sistémica a largo plazo de la información institucional, de manera que se mantenga la Cadena de Custodia Digital Archivística, garantizando su fiabilidad, integridad, autenticidad y usabilidad durante el tiempo que sea requerido***.

Además de incluirse este nuevo objetivo dentro de las políticas institucionales, la UCR debe implementar normativa vinculante a un nivel más específico, que permita una mayor claridad sobre la Preservación Digital Sistémica y la Cadena de Custodia Digital Archivística de las evidencias de información digital institucional.

Por esta razón, se propone la elaboración de un documento marco, que cubra las necesidades normativas específicas que se requieran en la UCR para la preservación digital a largo plazo; el cual, aunque no sea designado con el nombre de "Política", para evitar la ambigüedad terminológica con respecto a la normativa utilizada en la institución, tendrá el peso y la efectividad de la Política propuesta por el modelo OAIS.

A continuación, se presenta una propuesta de la estructura que podría contemplar el marco regulatorio que desarrollen las autoridades competentes para emitir normativa vinculante respecto al tema (Tabla 16):

Tabla 16. *Estructura propuesta para la elaboración de un marco normativo para la Preservación Digital Sistémica en la UCR.*

Estructura propuesta	Descripción	Contenido
Portada	"Consiste en la primera hoja del documento y es la carta de presentación del mismo" (MTSS, 2019, p.7)	Logos Título Codificación Fecha de aprobación Versión

Estructura propuesta	Descripción	Contenido
Tabla de aprobadores y revisores	“su objetivo es validar la funcionabilidad de lo documentado, mediante el visto bueno de distintas personas involucradas e interesadas. Se debe contar con el nombre, cargos y firmas de todas las personas involucradas” (MTSS, 2019, p.9-10)	Elaborado por Revisado por Aprobado por Autorizado por
Índice	“relaciona secuencialmente los apartados temáticos que integran la redacción del procedimiento, con su respectiva numeración a lo largo del documento para facilitar su localización” (MTSS, 2019, p.9-10)	Índice o Tabla de contenido
Antecedentes	“Consiste en la base jurídica, legal, económica, social, entre otras, que sustentan la creación de la política, en ella se debe mencionar los principales documentos jurídicos y administrativos que pueden ser leyes, normas, directrices, decretos ejecutivos, códigos, manuales de instructivos, políticas, entre otros, que dan soporte y razón de ser, al documento que se está presentando” (MTSS, 2019, p.11)	Antecedentes
Presentación de la normativa	Declaración	Misión Objetivos Principios Actualización
	Texto de la normativa: “se debe estipular los principios que van a orientar la toma de decisiones, éstos se deben basar en criterios y declaraciones para así lograr los resultados esperados por la unidad administrativa responsable” (MTSS, 2019, p.12)	Definición del Archivo Digital
		Conservación de la información
		Comisión Institucional del Archivo Digital
		Responsabilidades de la administración - Sostenibilidad financiera - Recurso humano
		- Requisitos de los sistemas de información - Planes de transferencia y consulta
		Prevención de pérdidas por desastre: - Respaldos de información (copias de seguridad)

Estructura propuesta	Descripción	Contenido
		- Actuación en caso de desastre
		Seguridad y Acceso: - Protección de derechos - Restricciones de acceso de usuarios - Disponibilidad de la información - Planes de migración
Glosario	"permite construir una recopilación de definiciones o explicaciones de palabras que se encuentran dentro del documento y que se categoricen de difícil comprender. Se debe ordenar de manera alfabética" (MTSS, 2019, p.12)	Términos que se consideren necesarios para la comprensión de la norma.
Control de cambios	"Con el propósito de controlar las ediciones de las políticas institucionales, es necesario registrar el número de modificaciones, las fechas, los apartados, hojas modificadas, la razón de origen del cambio y quién o quiénes realizan la modificación" (MTSS, 2019, p.12)	Cuadro de control de cambios y versiones.
Anexos	"espacio para adjuntar cualquier documento relacionado a la declaración de la política" (MTSS, 2019, p.12)	Anexos que se consideren necesarios para la norma.

Fuente: elaboración propia a partir de: MTSS, 2019; AENOR, 2015-b; y Serra-Serra, 2013-d.

Según esta propuesta de estructura, la sección más importante por completar es la del texto de la normativa, por lo cual a continuación se plantean algunas líneas base (Tabla 17) para el futuro desarrollo de los enunciados que compondrán la normativa vinculante, que debe ser creada por el órgano competente.

Tabla 17. *Propuesta de líneas base para la elaboración de normativa relacionada con preservación digital en la UCR.*

Tema		Línea base propuesta
Definición del Archivo Digital		El Archivo Digital de la Universidad de Costa Rica es el responsable de la preservación a largo plazo y acceso a los documentos de archivo, datos y otras evidencias de información digitales que se producen en la UCR en el ejercicio de sus funciones.
Conservación de la información		Preservar los documentos, datos y otras evidencias de información que se producen en formato digital en la UCR, garantizando las características de autenticidad, integridad, fiabilidad y acceso a lo largo del plazo que sean requeridos; con el fin de apoyar la toma de decisiones, fortalecer la transparencia y la rendición de cuentas de la Universidad, así como preservar la memoria institucional y colocarla al servicio de la comunidad universitaria y nacional en general.
Comisión Institucional del Archivo Digital		Es el órgano asesor con la capacidad de establecer los requisitos estratégicos, legales, técnicos, tecnológicos y funcionales para lograr un adecuado funcionamiento del Archivo Digital de la UCR. La Comisión Institucional de Archivo Digital está compuesta por los representantes, designados por la Rectoría, de las siguientes unidades: - Rectoría - Vicerrectoría de Acción Social - Oficina Jurídica - Centro de Informática - Archivo Universitario Rafael Obregón Loría (AUROL) - Escuela de Historia
Responsabilidades de la administración	*Sostenibilidad financiera*	La Universidad de Costa Rica dispondrá de los recursos financieros necesarios para asegurar la adecuada preservación y el oportuno acceso a largo plazo de los documentos de archivo y otras evidencias de información digitales, tomando en cuenta aspectos como mantenimiento, custodia, comunicación, capacitación, difusión, sistemas de información y otros equipos necesarios para el funcionamiento del Archivo Digital.
	Recurso humano	La UCR pondrá a disposición los recursos humanos necesarios para el

Tema		Línea base propuesta
		mantenimiento y funcionamiento del Archivo Digital, asegurando que el personal que tenga responsabilidades o tareas vinculadas al Archivo Digital, disponga de la formación pertinente en preservación digital. Cabe destacar que este recurso humano es diferente al designado para la Comisión Institucional de Archivo Digital, pues este es un órgano asesor; el Archivo Digital por su parte, requiere personal dedicado al funcionamiento y administración diarias.
Interacción de los Archivos	*Requisitos de los sistemas de información*	El Centro de Informática de la UCR deberá ser el responsable de desarrollar los servicios, aplicaciones e integraciones necesarios para el funcionamiento del Archivo Digital, así como las actualizaciones y mejoras necesarias que la evolución de las tecnologías de la información y la comunicación permitan.
	Planes de transferencia y consulta	Se deberán negociar los planes de transferencia de los documentos de archivos, los datos y otras evidencias de información que se producen las distintas unidades académicas, de investigación y administrativas de la UCR, siendo el Centro de Informática de la UCR, responsable de desarrollar los medios necesarios para lograr la interoperabilidad entre los sistemas, de manera que se lleve a cabo el traslado de la información entre los archivos manteniendo la Cadena de Custodia ininterrumpida.
Prevención de pérdidas por desastre	*Respaldos de información (Copias de seguridad)*	El Archivo Digital de la UCR deberá acatar las normas institucionales respecto al tema de respaldos de información, entre ellas las que se encuentran vigentes actualmente: - Directrices de Seguridad de la Información de la Universidad de Costa Rica (2015): *Capítulo 8 Resguardo y protección de la información*. - Marco de gobierno y gestión de TI de la UCR (2021): administración de respaldos de información y la implementación del plan de ejecución de respaldos y recuperación de información de TI. - Procedimiento para la realización de respaldos y pruebas de recuperación de datos. - Procedimiento para la realización y custodia de respaldos.
	Actuación en caso de desastre	En caso de desastre, se habilitarán los medios dispuestos por la UCR, en general, y del Centro de Informática, los cuáles en conjunto con los respaldos de información, permitan mantener a salvo y recuperable el fondo documental institucional

Tema		Línea base propuesta
		custodiado en el Archivo Digital.
Seguridad y Acceso	*Seguridad*	El Centro de Informática de la UCR, debe velar por el cumplimiento de las condiciones de seguridad de los documentos de archivo, datos y cualquier otra evidencia de información que se encuentre resguardada en el Archivo Digital, aplicando la normativa vigente institucional. En el caso del acceso a dispositivos físicos (por ejemplo, cuartos de servidores) debe asegurar la aplicación de controles sobre los permisos de ingreso.
	Protección de derechos	La Universidad de Costa Rica debe asegurar la protección de los derechos de todas las partes involucradas, incluyendo el marco legal nacional e institucional, y las disposiciones que las unidades productoras soliciten a la hora de realizar los convenios de transferencia. Se incluye aquí la protección de derechos de autor.
	Restricciones de acceso de usuarios	El Archivo Digital de la UCR debe contar tablas de acceso a nivel de serie documental. Estas tablas especifican las restricciones de acceso de manera clara, tanto a los paquetes AIP como los DIP, lo cual incluye la delimitación de usuarios con acceso a la información de contenido, como para usuarios finales, que realizan consultas de información. Se deben respetar la legislación y normas tanto nacionales como institucionales respecto al acceso público y restringido, datos personales de acceso irrestricto y de acceso restringido, así como datos sensibles que se encuentren en el fondo documental preservado por el Archivo Digital.
	Disponibilidad de la información	El Archivo Digital de la UCR, deberá contar con los servicios y funciones necesarios para dar acceso a la información a los usuarios que realicen solicitudes, siempre y cuando las restricciones de acceso lo permitan.
	Planes de migración	Contar con un plan de migración, acorde a las evoluciones tecnológicas del mercado y los requerimientos técnicos, que permita mantener el fondo documental accesible para la comunidad universitaria y nacional, de manera que la información siga manteniéndose usable a lo largo del tiempo que sea necesaria.

Fuente: elaboración propia a partir de: Castillo-Solano y Umaña-Alpízar, 2018; Serra-Serra, 2013-d; y AENOR, 2015-b.

3.2. Modelo de requisitos para el Archivo Digital

3.2.1. Marco Estratégico para la Preservación Digital

La propuesta para el desarrollo y la implementación de un Archivo Digital para la preservación sistémica del patrimonio documental de la Universidad de Costa Rica, está basada en la norma internacional UNE-ISO 14721, en la que se propone el uso del Modelo OAIS, para la creación de un repositorio digital seguro, con funcionalidades específicas de preservación.

3.2.1.1. Archivo Digital de la Universidad de Costa Rica (ADiUCR)

El ADiUCR es la entidad administrativa encargada de la transferencia y la preservación de la información digital generada y recibida en la Universidad de Costa Rica a raíz de la ejecución de sus funciones sustantivas (docencia, investigación y acción social), facilitativas y administrativas, en el repositorio de preservación digital sistémico.

El Archivo Digital formará parte del Sistema de Archivos de la UCR (SAU). Además estará a cargo del Archivo Universitario Rafael Obregón Loría (AUROL), quien se desempeñará como el responsable ejecutivo del ADiUCR y velará por su funcionamiento y por la gestión de su recurso humano, tecnológico y económico, en coordinación con la Rectoría y según los análisis realizados por la Comisión Institucional de Archivo Digital (CIADi).

El ADiUCR, se entenderá como un conjunto de personas, políticas y programas tecnológicos (figura 35), que trabajan en conjunto para lograr la preservación digital a largo plazo, y por lo tanto, no debe verse como una entidad aislada o como una simple plataforma tecnológica.

Figura 35. *Componentes fundamentales del ADiUCR.*

Fuente: elaboración propia. 2022.

3.2.1.2. Comisión Institucional de Archivo Digital (CIADi)

La CIADi es el órgano colegiado multidisciplinario, creado por la Rectoría, quién ejerce como ente asesor sobre la estrategia y planificación del ADiUCR, y quién se encargará de recomendar al AUROL los recursos necesarios para el correcto funcionamiento del ADiUCR, mediante análisis objetivos y actualizados.

La CIADi (Rectoría de la UCR, 2022, p.2) está conformada por los representantes de:

- El Archivo Universitario Rafael Obregón Loría (quién preside el órgano colegiado).
- La Rectoría.
- El Centro de Informática.
- La Sección de Archivística de la Escuela de Historia.
- La Vicerrectoría de Acción Social.
- La Oficina Jurídica.

Los miembros de la CIADi serán elegidos por un periodo de 4 años prorrogables.

La CIADi puede definir un calendario anual para establecer las sesiones ordinarias a realizarse. Además, será posible realizar sesiones extraordinarias para atender necesidades específicas relacionadas con la preservación digital, cuando se considere necesario.

En todos los casos, sus decisiones se tomarán por mayoría simple. Además, la CIADi podrá invitar a otros órganos de la UCR y agentes externos a la institución, como asesores para la toma de decisiones específicas, sin embargo, estas personas invitadas tendrán voz pero no voto.

La CIADi se establece como el SIRO (*Senior Information Risk Owner*) y, por lo tanto, se debe asegurar de que el riesgo para la continuidad digital está siendo gestionado de forma eficiente y efectiva, y que haya un enfoque multidisciplinario para la gestión de riesgos de información en una organización (The National Archives, s.f.-e).

Las funciones de la CIADi son las siguientes:

- Generar las propuestas normativas para la creación, organización y mantenimiento del ADiUCR. Estas normas deberán ser aprobadas por el órgano superior correspondiente para que puedan ser puestas en marcha de forma oficial a nivel universitario.
- Emitir lineamientos para asegurar la adecuada preservación digital.
- Analizar las ofertas del mercado para la adquisición o desarrollo de las herramientas tecnológicas necesarias para poner en funcionamiento el *software* del ADiUCR.
- Recomendar el presupuesto necesario para el correcto funcionamiento del ADiUCR, el cual será presentado al AUROL para ser incluido en su Plan Anual Operativo.

3.2.1.3. Recurso Humano

Para lograr un adecuado funcionamiento y posicionamiento del ADiUCR, la Universidad de Costa Rica debe asegurar la disposición del personal necesario, el cual debe contar con la formación académica y profesional requerida en materia de preservación digital, desde la ciencia archivística y desde TI.

Además, se debe garantizar la capacitación constante de las personas que trabajen de manera directa con el ADiUCR, para permitir a los profesionales mantenerse actualizados y enfrentar los retos que implica la preservación digital sistémica en la UCR. Para esto, puede establecerse una planificación anual de formación.

Para llevar a cabo la administración del ADiUCR, se designará un funcionario responsable llamado *Senior Responsible Owner* (SRO), quien es responsable de que un programa o proyecto, en este caso el ADiUCR, alcance sus objetivos, entregue los resultados proyectados y obtenga los beneficios requeridos dentro de las políticas establecidas (Gobierno de Reino Unido, s.f.), la persona que se desempeñe como SRO debe ser funcionario del AUROL y será el encargado de ejecutar las siguientes funciones (figura 36):

Figura 36. *Funciones del SRO con relación al ADiUCR.*

Fuente: elaboración propia a partir de Castillo-Solano y Umaña-Alpizar, 2018, p.167.

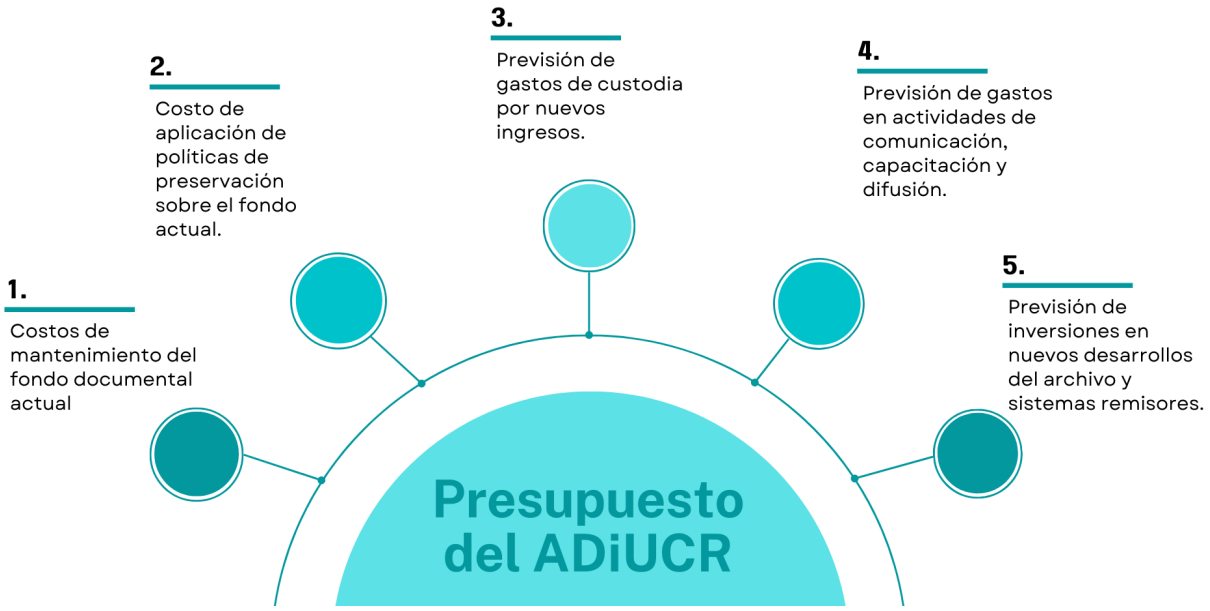
3.2.1.4. Presupuesto

Dentro de la normativa vinculante sobre preservación digital sistémica que apruebe la Universidad de Costa Rica, se deben asegurar los recursos financieros que permitan el funcionamiento y mantenimiento del ADiUCR.

Los recursos económicos que se dispongan para el ADiUCR, serán incluidos e implementados desde el Plan Anual Operativo del AUROL. Así mismo, la recomendación del presupuesto

requerido será presentada por la CIADi al AUROL, y podrá contener (aunque no exclusivamente)los siguientes aspectos (figura 37):

Figura 37. *Aspectos básicos a incorporar en el presupuesto del ADiUCR.*



Fuente: elaboración propia a partir de Serra-Serra, 2013-d, p.9.

3.2.1.5. Requisitos para las transferencias entre sistemas

Para recibir las transferencias de las distintas Unidades de la UCR, el ADiUCR deberá contar con una solución informática constituido por dos repositorios digitales, los cuáles deben "estar en las condiciones de recibir los documentos e información de los diferentes sistemas con los que cuenta la institución" (Castillo-Solano y Umaña-Alpizar, 2018, p.167).

Además, para llevar a cabo las transferencias, debe existir aprobación por parte del AUROL (como coordinador del SAU), apegado tanto a las Tablas de Plazos de Conservación e Informes de Valoración aprobadas por la CUSED, así como con el Protocolo de Transferencia establecido.

Los dos repositorios en los que se recibirán las transferencias documentales serán los siguientes:

1. Repositorio administrativo.
2. Repositorio de preservación permanente.

El Centro de Informática de la UCR, tendrá la responsabilidad de “supervisar y autorizar los servicios, aplicaciones e integraciones para las transferencias y/o comunicación entre los sistemas existentes” (Castillo-Solano y Umaña-Alpizar, 2018, p.168), de forma que se logre mantener la Cadena de Custodia Digital Archivística de manera ininterrumpida durante las transferencias documentales al ADiUCR.

3.2.1.6. Prevención y actuación en caso de desastre

Para lograr hacer frente a un desastre de manera adecuada, se debe contar con un plan de contingencia para lograr la continuidad de sus servicios y la protección de la información esencial. En el caso del ADiUCR, para lograr mantener la integridad de la información, se deberán acatar las disposiciones institucionales con respecto a seguridad y respaldos de información, así como los planes de continuidad de servicios, entre ellas:

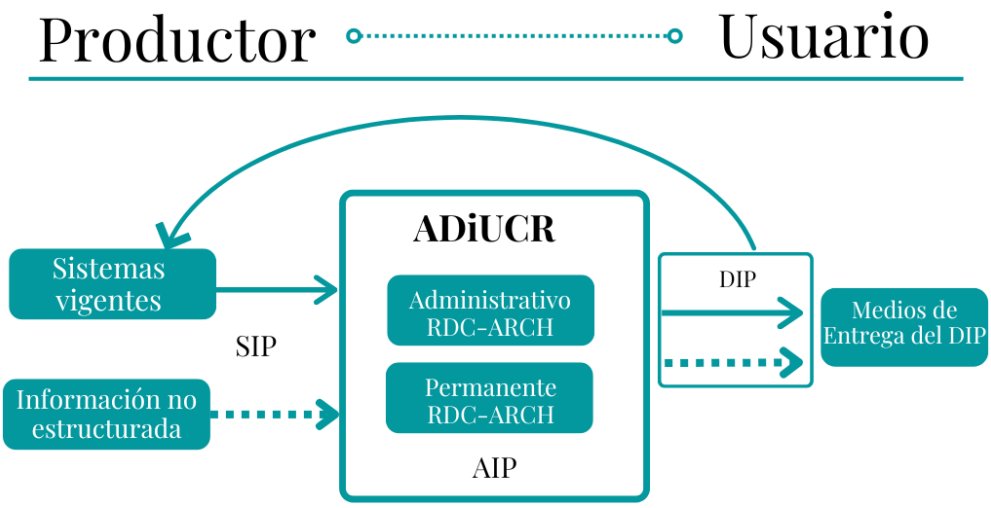
- Directrices Técnicas de Seguridad de la Información de la Universidad de Costa Rica (2015)
- CI-AGS-P01 Procedimiento para la realización de respaldos y pruebas de recuperación de datos (s.f.)
- CI-AGS-P11 Procedimiento para la realización y custodia de respaldos (2021)
- Metodología del Proceso de Continuidad de Tecnologías de la Información y Comunicación (2019)
- Lineamiento General para la Gestión de Seguridad de la Información en los Sistema de Información (2020)
- Marco de Gobierno y Gestión de TI de la Universidad de Costa Rica (2021)

3.2.2. Modelo Funcional del Archivo Digital

El Modelo Funcional “identifica los requisitos clave que el Archivo Digital debería considerar cuando la institución desarrolle la estrategia de preservación. Los requisitos funcionales caracterizan los elementos que se deben incluir en el repositorio digital” (Castillo-Solano & Umaña-Alpízar, 2019, p.199).

El ADiUCR tendrá un Modelo Funcional basado en la *Norma UNE-ISO 14721: Sistemas de transferencia de datos e información espaciales Sistema abierto de información de archivo (OAIS)*, según se muestra en la Figura 3, del apartado 1.4.9. OAIS de este documento (figura 38).

Figura 38. *Resumen del modelo funcional para el ADiUCR.*



Fuente: elaboración propia. 2023.

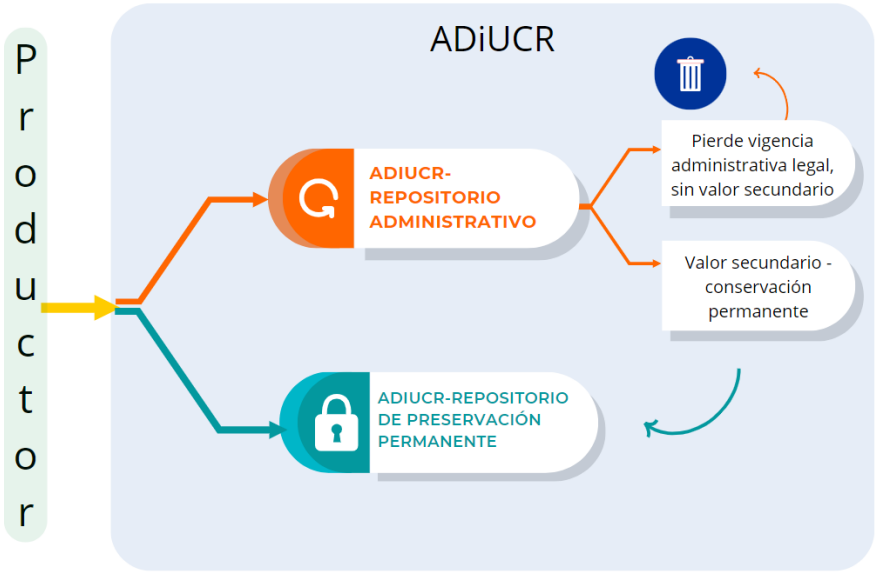
Para el caso de la Universidad de Costa Rica, se propone que el ADiUCR cuente con una misma aplicación informática compuesta por dos Repositorios Digitales de Confianza Archivísticos (RDC-ARCH) para la preservación digital (figura 39). Estos repositorios, almacenarán la información en distintos contextos de la siguiente manera:

- **Repositorio administrativo**: en este repositorio se mantendrán documentos que tienen un uso administrativo y pueden o no tener valor secundario, pero tienen un uso frecuente. Mientras se encuentren en este repositorio, pueden darse cambios en los expedientes, por ejemplo, añadir más documentos; dichos cambios deben quedar registrados en una bitácora de trazabilidad. Una vez cumplida su respectiva vigencia, debe darse su disposición final, según las Tablas de Plazo de Conservación, es decir, los documentos serán transferidos de forma automática al repositorio de preservación permanente o serán eliminados.
- **Repositorio de preservación permanente**: a este repositorio se trasladará, al cumplir con la vigencia establecida, la información que ha sido declarada de conservación permanente en la respectiva Tabla de Plazos de Conservación y que no será modificada.

También se transferirá la información que estuviera preservada en el repositorio administrativo y que según su plazo de vigencia deba trasladarse para su conservación permanente. En este repositorio, no podrán realizarse cambios ni se permitirá la eliminación de la información.

A continuación se muestra una representación gráfica de los dos tipos de repositorios que forman parte del Archivo Digital:

Figura 39. *Repositorios con los que debe contar el ADiUCR.*



Fuente: elaboración propia. 2023.

Considerando el Modelo Funcional del Archivo Digital propuesto en el Modelo OASIS, de la Norma UNE-ISO 14721, a continuación se presentan las entidades funcionales que formarán parte del modelo del ADiUCR:

1. Entidad funcional de Ingreso.
2. Entidad funcional de Almacenamiento de Archivo.
3. Entidad funcional de Gestión de Datos.
4. Entidad funcional de Administración.
5. Entidad funcional de Planificación de la Conservación.
6. Entidad funcional de Acceso.

Cada una de estas entidades, desempeñan un papel en cuanto a los flujos de información dentro de un Archivo OAIS. A continuación, se explica cada una de ellas.

3.2.2.1. Ingreso

Esta entidad funcional provee los servicios y las funciones que se requieren para aceptar los Paquetes de Información de Transferencias (SIP) que envían los productores, así como preparar los contenidos para el Almacenamiento y Gestión en el Archivo (AENOR, 2015-b, p.41).

Es importante resaltar que las transferencias recibidas por el Archivo Digital, provenientes de sistemas institucionales o de una instancia universitaria, incluso de un ente externo a la institución (por ejemplo, mediante donaciones), en algunos casos requieren un Protocolo de Transferencia específico, de manera que haya claridad en el uso de las herramientas, el procedimiento a seguir y las responsabilidades que adquiere cada parte interesada.

Algunas de las funciones de Ingreso con que debe contar el ADiUCR, son las siguientes (AENOR, 2015-b, p.45-46):

- Permitir recibir los paquetes archivísticos mediante el método *Push* o *Pull*, o interfaces programáticas, según la naturaleza de la información a transferir.
- Contar con mecanismos tecnológicos para recibir la transferencia desde los sistemas de producción.
- Confirmar al productor la recepción de los paquetes.
- Validar la transferencia exitosa del SIP (almacenamiento temporal) y detectar errores presentes en las transferencias.
- Contar con la capacidad de almacenamiento necesario para recibir los paquetes SIP, y conservar los subsecuentes paquetes AIP que se deben generar.
- Transformar SIP en AIP.
- Permitir la conversión automatizada de formatos de fichero.
- Extraer la Información Descriptiva desde los AIP, de manera que pueda incluirse en la base de datos del Archivo.
- Incluir metadatos para apoyar las búsquedas y recuperaciones del AIP.
- Coordinación de actualizaciones y gestión de datos.

De esta manera, el ADiUCR debe cumplir los siguientes requisitos de la Entidad Funcional de Ingreso (Tabla 18):

Tabla 18. *Requisitos de la entidad funcional de Ingreso para el ADiUCR.*

Entidad Funcional	Función	Requisito	Agente
Ingreso	Recepción de la Transferencia	Contar con capacidad de almacenamiento adecuado (para la información, copias de seguridad, copia remota, entre otras)	Sistema ADiUCR
		Contar con mecanismos para recibir la información desde el Productor.	Sistema ADiUCR
		Permitir la carga desde otros sistemas informáticos institucionales o desde otros medios (ficheros gestionados fuera de sistemas informáticos)	Sistema ADiUCR
		Aceptar la transferencia legal de custodia para la Información de Contenido en el SIP	Sistema ADiUCR
		Capacidad de implementar controles especiales de acceso a los contenidos	Sistema ADiUCR
		Enviar un acuse de recibo de un SIP al Productor	Sistema ADiUCR
		Permitir reenviar un SIP, en caso de errores resultantes de la transferencia del SIP	Sistema ADiUCR
	Aseguramiento de la Calidad	Validar la transferencia exitosa del SIP en el área de almacenamiento temporal	Sistema ADiUCR
		Implementar controles para documentar e identificar cualquier error en la transferencia, tanto de los ficheros como en la lectura/escritura del soporte	Sistema ADiUCR
	Generación del AIP	Transformar el SIP en AIP	Sistema ADiUCR
		Permitir la conversión de formato de ficheros	Sistema ADiUCR
		Solicitar informes para producir la Información Descriptiva que completa el AIP	Sistema ADiUCR
		Permitir el envío de SIP o AIP para auditoría a la Administración, y recibir de vuelta un informe de auditoría	Sistema ADiUCR
	Generación de Información Descriptiva	Capturar la Información Descriptiva de los AIP	Sistema ADiUCR
		Extraer Información Descriptiva desde otras fuentes (bases de datos, otros sistemas, entre otros)	Sistema ADiUCR

Entidad Funcional	Función	Requisito	Agente
		Incluir metadatos para apoyar las búsquedas y recuperaciones de AIP	Sistema ADiUCR
	Coordinación de Actualizaciones	Transferir los AIP a Almacenamiento de Archivo y la información de descripción a Gestión de Datos	Sistema ADiUCR
		Realizar una solicitud de almacenamiento y enviar una confirmación de almacenamiento cuando la transferencia se completa y verifica	Sistema ADiUCR
		Transferir la Información de Descripción de los nuevos AIP almacenados en el ADiUCR, a Gestión de Datos	Sistema ADiUCR
		Enviar una solicitud de actualización de la base de datos, es decir, actualizar el fondo cada vez que ingrese un nuevo AIP	Sistema ADiUCR
		Proporcionar una respuesta de actualización de la información de la base de datos indicando el estado de la actualización	Sistema ADiUCR

Fuente: Elaboración propia a partir de AENOR, 2015-b, p.44-46 y Castillo-Solano & Umaña-Alpízar, 2019.

El ADiUCR hará la Recepción de la Transferencia de los paquetes de información SIP, provenientes desde los sistemas informáticos y otras ubicaciones de almacenamiento en la que se encuentre información universitaria.

De esta forma, el ADiUCR deberá contar con las funcionalidades necesarias para recibir las transferencias de documentos, datos y cualquier otra evidencia de información, para los siguientes tres escenarios:

a. **Transferencia automatizada**: forma preferente para recibir los SIP provenientes de los sistemas de producción universitarios que se encuentran en uso. El ADiUCR debe recoger los paquetes de información de los sistemas productores, de forma directa, para asegurar tanto la creación del SIP como su recepción, y que esta se realice de forma automatizada (Serra-Serra, 2013c, p.6).

Este primer escenario será abordado mediante el método de transferencia *pull,* es decir, que el *software* del ADiUCR recoja los paquetes de información automáticamente desde el sistema productor, de manera que la intervención humana sea mínima, con lo cual se logrará automatizar la mayoría de los procesos de transferencia y asegurar en todo momento la CCDA.

Como ejemplo de transferencia automatizada, en el apartado 3.3 de esta investigación, se desarrolla el caso de la preservación digital de los documentos creados y recibidos mediante el Sistema de Gestión de Documentos Institucional (SiGeDI).

b. **Transferencia con intermediación humana**: forma preferente para la recepción de los SIP para los documentos y evidencias creados mediante herramientas ofimáticas y/o que se encuentran almacenados en sistemas de ficheros o redes locales. Para esto, se proporcionará un servicio tecnológico a los productores de la información para que puedan crear y remitir los SIP al Archivo Digital. Esta forma de ingreso debe ser recesiva a medida que se desarrollen nuevas aplicaciones que cubran los procesos no automatizados (Serra-Serra, 2013c, p.6).

Es necesario realizar una proceso previo de *autenticación* para los paquetes de información que se pretendan transferir al ADiUCR mediante este escenario. Este proceso implica que una autoridad con las competencias adecuadas, certifique que la información a transferir corresponde

a una representación suficiente del documento original, en cuanto a forma y/o contenido, de manera que sirva de prueba legal, administrativa o histórica, una vez ingresada al ADiUCR.

La autenticación permite marcar un punto de partida para asegurar la Cadena de Custodia Ininterrumpida de la información una vez que se transfiere al ADiUCR, considerando que en este escenario se plantea la conservación de información que no fue creada dentro de un sistema o ambiente seguro, por lo cual no se puede asegurar que antes de la autenticación se haya mantenido la integridad de los objetos digitales.

En cuanto a la transferencia con intermediación humana, en el apartado 3.3 se desarrolla el caso de la transferencia de las representaciones digitalizadas correspondientes a la Colección Fotográfica de la Universidad de Costa Rica, bajo custodia del Archivo Universitario.

c. **Transferencia con tratamiento previo de la documentación**: forma preferente para la transferencia de paquetes de información provenientes de sistemas obsoletos (*legacy systems*) de la UCR y documentos, datos y evidencias donados a la institución (*legacy data*).

El ADiUCR debe ser capaz de almacenar la información proveniente de sistemas obsoletos que aún contienen información con valor administrativo, legal e incluso histórico, de la Universidad de Costa Rica. Para ello, se deben crear los paquetes SIP según el Modelo OAIS, para que puedan ser recibidos y transformados en paquetes AIP dentro del *software* del ADiUCR.

3.2.2.2. Almacenamiento de Archivo

Incluye los servicios y funciones necesarios para el almacenamiento, mantenimiento y recuperación de los AIP, tales como (AENOR, 2015-b, p.42):

- Recibir los AIP desde el Ingreso, y añadirlos al almacenamiento permanente o administrativo según corresponda.
- Gestionar el almacenamiento en capas.
- Actualizar los soportes sobre los que los fondos han sido almacenados.
- Llevar a cabo controles especiales y de rutina de errores.
- Habilitar medios de prevención en caso de desastres.
- Proporcionar los AIP en el Acceso para cumplir con las solicitudes mediante el DIP.

El ADiUCR debe cumplir los siguientes requisitos de la Entidad Funcional de Almacenamiento de Archivo (Tabla 19):

Tabla 19. *Requisitos de la entidad funcional de Almacenamiento de Archivo para el ADiUCR.*

Entidad funcional	Función	Requisito	Agente
Almace-namiento de Archivo	Recepción de Datos	Recibir una solicitud de almacenamiento y un AIP procedente de Ingreso	Sistema ADiUCR
		Trasladar el AIP a un almacenamiento (permanente o administrativo) dentro del Archivo	Sistema ADiUCR
		Seleccionar los dispositivos de almacenamiento (servidores del Centro de Informática, almacenamiento en la nube, entre otros) y preparar los dispositivos	Sistema ADiUCR
		Llevar a cabo la transferencia a los dispositivos de Almacenamiento de Archivo	Sistema ADiUCR
		Enviar un mensaje de confirmación de almacenamiento a Ingreso, en el que se incluye la identificación de almacenamiento de los AIP	Sistema ADiUCR
	Gestión de Jerarquía de Depósito	Colocar los contenidos de los AIP en los soportes correspondientes	Sistema ADiUCR
		Ajustar a cualquier nivel, las medidas especiales de seguridad necesarias para garantizar la protección del AIP, según el Convenio de Transferencia	Sistema ADiUCR
		Garantizar el nivel de protección adecuado para el AIP	Sistema ADiUCR
		Supervisar los registros de errores para garantizar que los AIP no resulten dañados durante las transferencias	Sistema ADiUCR
		Proporcionar estadísticas operativas (que incluyen el inventario de dispositivos de almacenamiento disponibles, la capacidad de almacenamiento disponible y las estadísticas de uso)	Sistema ADiUCR
	Sustitución de Soportes	Brindar la posibilidad de reproducir los AIP en el tiempo	Sistema ADiUCR
		No permitir la modificación de la Información	Sistema ADiUCR
		Aplicar la estrategia de migración	Sistema ADiUCR

Entidad funcional	Función	Requisito	Agente
		Llevar a cabo un "Refrescamiento o Recopiado", una "Reproducción o Copia" y un "Reempaquetado" que sean sencillos	Sistema ADiUCR
	Control de errores	Garantizar que que ningún componente del AIP ha resultado dañado en el Almacenamiento de Archivo o durante cualquier transferencia interna de datos en el Almacenamiento de Archivo	Sistema ADiUCR
		El hardware y el software dentro del ADiUCR deben proporcionar notificaciones de los posibles errores y que dichos errores se envíen a registros de errores	Sistema ADiUCR
		Verificar de manera aleatoria la integridad de los Objetos de Datos por medio de algún mecanismo de comprobación de errores	Sistema ADiUCR
	Prevención de Desastres	Realizar copias de seguridad en una ubicación físicamente independiente	Sistema ADiUCR
		La Administración del ADiUCR debe desarrollar directivas sobre la prevención de desastres y recuperación ante desastres	Administración ADiUCR
	Suministro de Datos	Facilitar copias de los AIP almacenados a Acceso	Sistema ADiUCR
		Recibir solicitudes de AIP, en las que se pueda identificar los AIP solicitados	Sistema ADiUCR
		Facilitar el AIP en el tipo de soporte indicado o los transfiere a un área de almacenamiento temporal	Sistema ADiUCR
		Enviar un aviso de transferencia de datos a Acceso una vez ejecutada la solicitud	Sistema ADiUCR

Fuente: Elaboración propia a partir de AENOR, 2015-b, p.46-47 y Castillo-Solano y Umaña-Alpízar, 2019.

3.2.2.3. Gestión de Datos

La entidad funcional de Gestión de Datos expone los "servicios y funciones para ingresar datos, mantener y acceder tanto a la Información Descriptiva con la que se identifican y documentan los fondos de Archivo como a los datos administrativos empleados para gestionar el Archivo" (AENOR, 2015-b, p.42). Dentro de sus funciones y servicios se encuentran (AENOR, 2015-b, p.42):

- Administrar las funciones de bases de datos del Archivo (manteniendo el esquema y las definiciones de visualización e integridad referencial).
- Aplicar actualizaciones de bases de datos (cargando nueva información descriptiva o datos administrativos de Archivo).
- Presentar dudas sobre los datos de la gestión de datos, para generar respuestas.
- Producir informes derivados de las respuestas.

Tabla 20. *Requisitos de la entidad funcional de Gestión de Datos para el ADiUCR.*

Entidad funcional	Función	Requisito	Agente
Gestión de Datos	Administración de Bases de Datos	Mantener la integridad de la base de datos de Gestión de Datos, tanto de la información descriptiva de la información a preservarse en el ADiUCR, como de la información del sistema (necesaria para el funcionamiento de la aplicación tecnológica utilizada)	Sistema ADiUCR
		Definir las tablas o esquemas necesarios para llevar a cabo las funciones de Gestión de Datos	Personal ADiUCR
		Proporcionar la capacidad de crear, mantener y acceder a visualizaciones personalizadas de usuarios de los contenidos	Sistema ADiUCR
		Proporcionar la validación interna de los contenidos de la base de datos	Sistema ADiUCR
		La función Administración de Bases de Datos se lleva a cabo de acuerdo con las directivas recibidas de Administración del ADiUCR	Administración ADiUCR
	Resolución de Dudas	Recibir una solicitud de duda procedente de Acceso	Sistema ADiUCR / Personal ADiUCR
		Generar una respuesta de duda que se transmite al solicitante	Sistema ADiUCR / Personal ADiUCR

Entidad funcional	Función	Requisito	Agente
	Generación de Informes	Recibir una solicitud de informe procedente de Ingreso, Acceso o Administración	Sistema ADiUCR / Personal ADiUCR
		Generar el informe que entrega al solicitante	Sistema ADiUCR / Personal ADiUCR
		Ofrecer información descriptiva sobre un AIP concreto	Sistema ADiUCR
	Recepción de Actualizaciones de Base de Datos	Añadir, modificar o eliminar información del depósito de Gestión de Datos.	Sistema ADiUCR
		Actualizar la Información Descriptiva de los nuevos AIP (actualizar bases de datos)	Sistema ADiUCR
		Incluir actualizaciones del sistema y actualizaciones de informes	Sistema ADiUCR
		Proporcionar informes periódicos a Administración del estado de las actualizaciones	Sistema ADiUCR
		Enviar una respuesta de las actualizaciones de la base de datos a Ingreso	Sistema ADiUCR

Fuente: Elaboración propia a partir de AENOR, 2015-b, p.48 y Castillo-Solano y Umaña-Alpízar, 2019.

3.2.2.4. Administración

Esta entidad funcional, por su parte, ofrece los servicios necesarios para "el funcionamiento global del sistema de Archivo" (AENOR, 2015-b, p.42).

Es posible encontrar dentro de sus funciones (AENOR, 2015-b, p.42):

- Solicitar y negociar convenios de transferencia con Productores.
- Auditar las transferencias para asegurar que cumplan las normas del Archivo.
- Mantener la configuración de la gestión del sistema de hardware y de software.
- Contar con ingeniería del sistema para controlar y mejorar las operaciones de Archivo.
- Inventariar, elaborar informes y migrar o actualizar los contenidos del Archivo.
- Establecer y mantener normas y políticas de Archivo.
- Aportar ayuda al usuario y activar solicitudes almacenadas.

Tabla 21. *Requisitos de la entidad funcional de Administración para el ADiUCR.*

Entidad funcional	Función	Requisito	Agente
Administración	Negociación del Convenio de Transferencia	Negociar Convenios de transferencia con los Productores	Administración ADiUCR / Productor
		Negociar un calendario de transferencia de datos con el Productor	Administración ADiUCR / Productor
		Mantener un calendario de Sesiones de Transferencias de Datos esperadas	Administración ADiUCR / Productor
		Recibir plantillas de AIP/SIP y recomendaciones de personalización de Planificación de la Conservación	Administración ADiUCR
		Documentar los formatos y procedimientos para la transferencia de datos como parte de las políticas de transferencia	Administración ADiUCR
	Gestión de la Configuración del Sistema	Ofrecer ingeniería de sistemas (hardware y software), para que el sistema de Archivo pueda monitorizar continuamente la funcionalidad del sistema de ADiUCR en su totalidad, y controle los cambios	Administración ADiUCR
		Mantener la integridad y la trazabilidad de la configuración durante todas las fases del ciclo de vida del sistema	Administración ADiUCR
		Auditar las operaciones del sistema, su rendimiento y utilización	Administración ADiUCR / Sistema ADiUCR
		Envía y recibe informes sobre información del sistema a Gestión de Datos	Administración ADiUCR / Sistema ADiUCR
		Recibe estadísticas operativas desde Almacenamiento	Administración ADiUCR / Sistema ADiUCR
		Brinda información del rendimiento del ADiUCR e informes de inventarios	Administración

Entidad funcional	Función	Requisito	Agente
		de la información preservada, a Planificación de la Conservación	ADiUCR / Sistema ADiUCR
		Ofrecer información del rendimiento de ADiUCR e informes de inventario de los fondos de Archivo	Administración ADiUCR / Sistema ADiUCR
		Desarrollar e implementar planes para la evolución del sistema	Administración ADiUCR
	Actualización de la Información de Archivo	Ofrecer un mecanismo para actualizar los contenidos del ADiUCR (es decir, de los paquetes de información archivística)	Administración ADiUCR
		Recibir solicitudes de cambio, procedimientos y herramientas desde Gestión de la Configuración del Sistema	Administración ADiUCR / Sistema ADiUCR
		Facilita actualizaciones mediante el envío de solicitudes de consulta al Acceso, actualizando los contenidos de los DIP resultantes y reenviándolos como SIP a Ingreso.	Administración ADiUCR / Sistema ADiUCR
	Control del Acceso Físico	Ofrecer mecanismos para restringir o permitir el acceso físico a los elementos del ADiUCR, según las políticas de Archivo.	Administración ADiUCR
	Establecimiento de Normas y Políticas	Establecer y mantener las políticas y normas del sistema de ADiUCR	Administración ADiUCR
		Recibir información sobre presupuesto desde el AUROL	Administración ADiUCR
		Recibir información sobre políticas de preservación desde la CIADi	Administración ADiUCR
		Facilitar a la Dirección informes periódicos	Administración ADiUCR / Sistema ADiUCR
		Recibe recomendaciones, propuestas e informes de análisis de riesgos para mejorar el funcionamiento del ADiUCR, desde Planificación de la Conservación	Administración ADiUCR

Entidad funcional	Función	Requisito	Agente
		Afronta riesgos derivados de eventos no previstos y toma las decisiones adecuadas para minimizar el riesgo de incumplir los compromisos del ADiUCR (faltas de servicio no planificadas debidas a fallos en la red, errores del software, fallos de hardware, errores humanos, fallos de disco, etc.)	Administración ADiUCR / CIADi
		Crear las normas sobre estándares de formato, normas de documentación y procedimientos a seguir durante el proceso de Ingreso, las cuales deben ser aprobadas por la CIADi.	Administración ADiUCR / CIADi
		Facilitar normas aprobadas y objetivos de migración a Planificación de la Conservación	Administración ADiUCR / CIADi
		Desarrollar normativa sobre: - Gestión de migración de formatos de almacenamiento - Gestión de bases de datos - Prevención de desastres - Seguridad para los contenidos del ADiUCR Estas normativas deben ser aprobadas por la CIADi	Administración ADiUCR / CIADi
		Aplicar técnicas de control de errores a través del ADiUCR	Administración ADiUCR
	Auditoría de la Transferencia	Verificar que las transferencias (SIP o AIP) cumplen las especificaciones del Convenio de Transferencia	Administración ADiUCR
		Verificar que los SIP y AIP son comprensibles por la Comunidad Específica.	Administración ADiUCR / Productor
		Comprobar que la calidad de los datos cumple con los requisitos del ADiUCR	Administración ADiUCR
		Comprobar que se dispone de la Información de Representación e Información de Descripción de la Conservación adecuadas para asegurar que la Información de Contenido es comprensible y puede ser utilizada	Administración ADiUCR / Productor

Entidad funcional	Función	Requisito	Agente
		Facilitar un informe de auditoría para Ingreso	Administración ADiUCR
		Informar de la penalización al Productor (en caso de existir)	Administración ADiUCR
		En el caso de que se genere una nueva versión de un AIP, comprobar que se han cumplido los objetivos de la migración	Administración ADiUCR / Sistema ADiUCR
		Preparar un informe final de ingreso que se facilita al Productor y que se utiliza para negociar el Convenio de Transferencia	Administración ADiUCR
	Activación de Solicitudes	Contar con un registro de las solicitudes dirigidas a evento y compararlo periódicamente con los contenidos del Archivo para determinar si todos los datos necesarios están disponibles	Administración ADiUCR
		Generar solicitudes periódicamente, con una periodicidad definida por los Usuarios o por el suceso de un evento.	Administración ADiUCR
	Servicio al Cliente	El SRO debe crear, mantener y eliminar cuentas de Usuarios	Administración ADiUCR
		Responder a solicitudes de información general	Personal ADiUCR

Fuente: Elaboración propia a partir de AENOR, 2015-b, p.49-51 y Castillo-Solano & Umaña-Alpízar, 2019.

3.2.2.5. Planificación de la Conservación

Incluye los servicios y funciones de "control del entorno del OAIS, proveyendo recomendaciones y planes de conservación para asegurar que la información almacenada en el OAIS permanezca accesible a Largo Plazo, e inteligible, para la Comunidad Específica, incluso cuando el entorno automatizado original devenga obsoleto" (AENOR, 2015-b, p.42).

Las funciones que desempeña esta entidad funcional incluyen (AENOR, 2015-b, p.42):

- Evaluar los contenidos del Archivo.
- Recomendar actualizaciones de información archivística.
- Recomendar la migración de fondos de Archivo vigentes.
- Desarrollar indicaciones para normas y políticas de Archivo.
- Producir regularmente informes de análisis de riesgos.
- Controlar cambios en el entorno tecnológico y nuevos requisitos de servicio.
- Diseñar plantillas de Paquetes de Información y proporcionar asistencia en el diseño y en la revisión para especializar estas plantillas en SIP y AIP para transferencias específicas.
- Desarrollar planes de migración detallados, así como los prototipos de *software* y planes de prueba para esas migraciones.

En general, esta entidad funcional se encarga de mantener actualizada la normativa y la tecnología que se requiere para el funcionamiento del ADiUCR, a la vez que se asegura el acceso y usabilidad de la información durante todo el plazo que sea requerida.

Tabla 22. *Requisitos de la entidad funcional de Planificación de la Conservación para el ADiUCR.*

Entidad funcional	Función	Requisito	Agente
Planificación de la Conservación	Monitorización de Comunidad Específica	Hacer un seguimiento de los cambios en sus requisitos del servicio y en las tecnologías de producto disponibles	Personal ADiUCR
		Facilitar informes, alertas de requisitos y normas emergentes a la función Desarrollo de Estrategias y Normas de Conservación	Personal ADiUCR
		Enviar requisitos de conservación a Desarrollo de Diseños del Empaquetado	Personal ADiUCR
	Monitorización de Tecnología	Hacer el seguimiento de las tecnologías digitales emergentes, normas de información y plataformas informáticas para identificar tecnologías que podrían ser motivo de obsolescencia	Personal ADiUCR
		Capacidad de desarrollar prototipos para hacer una mejor evaluación de las tecnologías emergentes	Personal ADiUCR
		Recibir solicitudes para realizar prototipos y enviar los resultados	Personal ADiUCR
		Enviar informes, normas de datos externas, resultados de los prototipos y alertas sobre tecnología	Personal ADiUCR
	Desarrollo de Normas y Estrategias de Conservación	Desarrollar y recomendar estrategias y normas, y evaluar riesgos para que el ADiUCR haga valoraciones informadas cuando se establecen normas y políticas, así como la gestión de la infraestructura de su sistema	Administración ADiUCR / Personal ADiUCR
		Ofrecer informes de análisis de riesgos, sobre los riesgos previstos y su posible mitigación	Personal ADiUCR
		Recibir informes, alertas de requisitos y normas emergentes mediante la monitorización de Comunidades Específicas y monitorización de Tecnología	Personal ADiUCR
		Recibir políticas, procedimientos y normas de operación, información del rendimiento, informes de inventario y comentarios resumidos de los usuarios	Personal ADiUCR
		Identificar aquellos cambios que precisarían la migración de ciertos fondos de Archivo actuales o las nuevas transferencias	Personal ADiUCR

Entidad funcional	Función	Requisito	Agente
		Enviar a la Administración recomendaciones sobre la evolución del sistema y sobre los cambios en los AIP	Personal ADiUCR
		Recibir normas de datos externas y producir perfiles de esas normas, que se envían como propuestas sobre su uso potencial	Personal ADiUCR
		Recibir puntos a tratar en caso de requisitos de transferencia no previstos, y responder con recomendaciones para tratar los nuevos requisitos.	Personal ADiUCR
	Desarrollo de Diseños del Empaquetado y Planes de Migración	Producir nuevos diseños de Paquetes de Información y planes de migración y prototipos detallados, para implementar las políticas y directrices de Administración	Personal ADiUCR
		Ofrecer pautas para la aplicación de estos diseños de Paquete de Información y planes de Migración	Personal ADiUCR
		Recibir normas aprobadas y objetivos de migración desde Administración	Personal ADiUCR
		Aplicar estas normas a los requisitos de conservación y facilitar diseños de plantillas AIP y SIP a Administración	Personal ADiUCR
		Facilitar pautas de personalización y revisiones de AIP/SIP a Administración (por ejemplo, aplicar firma digital y sellado de tiempo cuando existan modificaciones en los paquetes)	Personal ADiUCR
		En caso de identificar transferencias que no están contempladas por las normas y procedimientos existentes, puede enviar puntos a tratar	Personal ADiUCR
		Recibir pautas, incluyendo nuevas normas, para satisfacer los requisitos de las nuevas transferencias.	Personal ADiUCR
		Realizar las transformaciones en el AIP según requisitos de conservación y los objetivos de migración, para evitar perder la capacidad de acceder, causada por la obsolescencia tecnológica	Personal ADiUCR
		Desarrollar nuevos diseños de AIP, prototipos de software, planes de pruebas, planes de revisión por parte de la comunidad y planes de implementación para el despliegue de los nuevos AIP.	Personal ADiUCR

Entidad funcional	Función	Requisito	Agente
		Establecer mecanismos para asegurar la integridad y autenticidad de los paquetes de información, a través de la firma digital y sellado de tiempo, algoritmos criptográficos (HASH), y bitácoras de trazabilidad, durante los procesos de empaquetado y migración	Personal ADiUCR
		Enviar el paquete de migración completo a Administración, una vez que se ha aprobado el plan de migración, los diseños de AIP asociados y el software.	Personal ADiUCR

Fuente: *Elaboración propia a partir de AENOR, 2015-b, p.51-52 y Castillo-Solano & Umaña-Alpízar, 2019*

Se debe considerar que uno de los aspectos fundamentales con respecto a la conservación, es la administración de los formatos. El rápido avance de la tecnologías y el constante surgimiento de nuevos formatos, obligan a estar atentos a la obsolescencia, tarea que debe asumir el ADiUCR.

De esta forma el Archivo Digital, debe contar con la capacidad de "identificar, administrar y normalizar los formatos que ingresan. Para ello debe tener la información propia de los formatos admitidos/permitidos en el repositorio, y la lista de los formatos no admitidos" (Castillo-Solano & Umaña-Alpízar, 2019, p.216)

Dentro de los factores de sostenibilidad con los que se debe contar para la elección de los formatos a utilizar en el ADiUCR están (Castillo-Solano & Umaña-Alpízar, 2019, p.216):

- Formatos accesibles: que sean de código abierto, sin dependencia de terceros.
- Interoperabilidad.
- Estabilidad/Compatibilidad: funcionalidad e integridad con versiones anteriores o posteriores.
- Aceptación: grado de utilización a nivel internacional.
- Estandarización: normalizados por organismos internacionales
- Mecanismos de protección técnica.
- Factores de calidad y funcionalidad: resolución.

3.2.2.6. Acceso

Esta entidad cuenta con servicios y funciones para proporcionar el "apoyo a los Usuarios para determinar la existencia, descripción, localización y disponibilidad de la información almacenada en el OAIS y permite a los Usuarios solicitar y recibir productos de información" (AENOR, 2015-b, p.42).

Las funciones de la entidad funcional de acceso son (AENOR, 2015-b, p.42):

- Comunicarse con los Usuarios para recibir solicitudes.
- Aplicar controles que limiten el acceso a información protegida específicamente.
- Coordinar la ejecución de solicitudes para que lleguen a buen término.
- Generar respuestas (Paquetes de Información de Consulta, respuestas a consultas, informes).
- Entregar las respuestas a los usuarios.

Tabla 23. *Requisitos de la entidad funcional de Acceso para el ADiUCR.*

Entidad funcional	Función	Requisito	Agente
Acceso	Coordinación de Actividades de Acceso	Ofrecer uno o más interfaces de consulta a la información que custodia el ADiUCR y permitir la descargas de copia certificadas	Sistema ADiUCR
		Definir y verificar los roles y permisos a los usuarios o sistemas, en el consumo de servicios del ADiUCR	Sistema ADiUCR
		Establecer reglas de restricción según Tablas de Acceso (datos personales, datos sensibles, información confidencial, etc.)	Administración ADiUCR / Personal ADiUCR
		Atender solicitudes de duda, que se ejecutan en Gestión de Datos y devuelven respuestas inmediatas al usuario	Personal ADiUCR / Sistema ADiUCR
		Atender solicitudes de informe, que pueden exigir varias consultas para generar informes con un formato para ser entregados al Usuario	Personal ADiUCR / Sistema ADiUCR
		Atender solicitudes, que pueden acceder bien a Gestión de Datos o a Almacenamiento de Archivo, o a ambos, para preparar un Paquete de Información de Consulta (DIP) formal: - Solicitud Ad hoc: que se ejecuta una sola vez - Solicitud Basada en Evento: se inicia por una solicitud de consulta que puede resultar en la entrega periódica de los ítems solicitados	Sistema ADiUCR
		Enviar solicitudes de consulta para obtener los DIP necesarios para realizar sus funciones de actualización	Sistema ADiUCR
		Determinar si están disponibles los recursos para realizar la solicitud, asegurar que el usuario esté autorizado para acceder y recibir los elementos solicitados, y notificar al Usuario que la solicitud haya sido aceptada o rechazada	Sistema ADiUCR
		Ofrecer asistencia a los Usuarios del ADiUCR	Personal ADiUCR / ADiUCR
		Permitir realizar búsquedas por contenido y por metadatos descriptivos	Sistema ADiUCR

Entidad funcional	Función	Requisito	Agente
		Contar con una bitácora de registro de consultas	Sistema ADiUCR
	Generación del DIP	Aceptar una solicitud de consulta, recuperar el AIP de "Almacenamiento de Archivo" y mover una copia de los datos a un área de almacenamiento temporal para su posterior consulta	Sistema ADiUCR
		Transmitir una solicitud de informe a Gestión de Datos para obtener la Información Descriptiva necesaria para el DIP	Sistema ADiUCR
		Situar la respuesta DIP completada en el área de almacenamiento temporal	Sistema ADiUCR
		Notificar a la función Coordinación de Actividades de Acceso que el DIP está listo para su distribución	Sistema ADiUCR
	Entrega de Respuesta	Gestionar tanto las entregas en línea como las fuera de línea de las respuestas (DIP, respuestas a consultas, informes y asistencia) a los Usuarios	Sistema ADiUCR
		Entregas en línea: Aceptar una respuesta de Actividades de Acceso Coordinadas y prepararla para su distribución en línea en tiempo real a través de enlaces de comunicación. Identificar a los destinatarios, determinar el procedimiento de transferencia solicitado, localizar la respuesta en el área de almacenamiento temporal para que sea remitida y dar soporte a la transferencia en línea de la respuesta	Sistema ADiUCR
		Entregas fuera de línea: recuperar la respuesta de la función Coordinación de Actividades de Acceso, preparar las listas de empaquetado y otros documentos de envío y envíar la respuesta. Cuando la respuesta se ha enviado, devolver una nota de solicitud enviada	Sistema ADiUCR

Fuente: Elaboración propia a partir de AENOR, 2015-b, p.53-54 y Castillo-Solano & Umaña-Alpízar, 2019.

3.2.3. Modelo Tecnológico del Archivo Digital

3.2.3.1. Especificaciones tecnológicas básicas

Dentro del Modelo Tecnológico propuesto para el desarrollo e implementación del Archivo Digital de la Universidad de Costa Rica, se espera que, como mínimo se pueda garantizar las especificaciones sobre el servicio de recepción de documentos para ingesta y de paquetes de envío de información o SIP, conformación contenedores normalizados de información de clasificación, descripción y preservación protegidos por mecanismos criptográficos confiables y económicamente viables AIP, controles de acceso y aseguramiento de los AIP, gestión de los documentos en estructuras jerárquicas multinivel y conformación de agrupaciones documentales que respondan a criterios lógicos, legales, administrativos y de control, es decir, a nivel de serie documental, expedientes y unidades documentales compuestas, y finalmente que permita establecer contratos de consulta diferenciada mediante la generación de paquetes de consulta DIP, entre otras características.

Resulta de vital importancia, a nivel de la solución tecnológica, considerar una diversidad de aspectos en cuanto a seguridad, acceso, servicios, estructura, metadatos, alta disponibilidad, calidad de servicio, entre otros.

Por lo cual se requiere que la infraestructura tecnológica del ADiUCR, sea planificada de manera interdisciplinaria, liderada por equipos de profesionales de archivística, personal de informática, asesores legales y administrativos. También se recomienda la participación de ingenieros industriales o expertos en gestión de procesos que permitan maximizar el retorno de inversión mediante mecanismos y procesos optimizados que permitan a la institución en su totalidad incrementar su eficiencia y productividad.

En la figura 40, se detallan elementos mínimos que se van a requerir de parte de la solución tecnológica de Archivo Digital que se espera implementar en la UCR.

Figura 40. *Especificaciones mínimas que requiere la solución tecnológica del Archivo Digital de la UCR.*

Fuente: elaboración propia a partir de Castillo-Solano y Umaña-Alpízar, 2018, p.218-219.

3.2.3.2. Arquitectura tecnológica

Además de los servicios mínimos indicados en el apartado anterior, algunos requerimientos en cuanto a la arquitectura tecnológica con los que debe cumplir el ADiUCR, son (Castillo-Solano y Umaña-Alpízar, 2018, 224-225):

- Contar con un contrato de mantenimiento que permita la mejora o incorporación de:
    - nuevos procesos, atributos o características del objeto.
    - la normativa y los estándares mundiales en el tratamiento o la preservación del documento digital demanden.
    - los cambios requeridos con respecto a la tecnología.
    - la renovación de su plataforma tecnológica, acorde con los avances de la industria.
- Desarrollarse empleando el paradigma de la arquitectura orientada a servicios SOA, de modo que esté habilitado para implementar interfaces con el fin de que sea interoperable con sistemas dentro y fuera de la institución, sin incurrir en procesos de alta complejidad.
- Permitir el crecimiento horizontal y vertical, de forma escalonada hasta cumplir con las necesidades de la institución.
- Garantizar en todo momento el control de acceso a la información en custodia con la misma configuración y seguridad, independientemente de la interfaz que solicita el acceso.

De esta forma, mediante la Tabla 24, se presentan las Condiciones de Operación necesarias para implementar y mantener en funcionamiento el ADiUCR, es decir, los requerimientos tecnológicos para almacenar la información universitaria dentro de un entorno funcional protegido en todos los niveles y asegurar la continuidad del negocio en caso de desastres o fallas del sistema.

Asimismo, el Archivo Digital tendrá la capacidad de ofrecer un alto nivel de conectividad para facilitar la información a los usuarios, mediante servicios de consulta a través de los sistemas productores u otros medios digitales, facilitando los trámites administrativos y la investigación.

Tabla 24. *Requisitos sobre las Condiciones de Operación para el Modelo Tecnológico del ADiUCR.*

Condiciones de Operación	Requisitos
Sistema operativo Servicios principales necesarios para operar y administrar la plataforma de aplicaciones y proporcionar una interfaz entre el software de aplicación y la plataforma	Contar con un núcleo o Kernel, que permita: - crear y gestionar procesos - ejecutar programas - definir y comunicar señales - definir y procesar las operaciones horarias del ADiUCR - controlar los procesos de entrada y salida hacia y del entorno externo
	Incluir comandos y dispositivos con mecanismos para las operaciones a nivel de operador, como: - comparar, imprimir y visualizar el contenido de los ficheros - modificar ficheros - buscar modelos - evaluar expresiones - registrar mensajes - mover ficheros entre directorios - seleccionar datos - ejecutar secuencias de comandos - acceder a la información del entorno
	Contar con extensión a tiempo real, la cual incluye los interfaces de las aplicaciones y los sistemas de operación necesarios para apoyar esos dominios de aplicaciones que requieren ejecución determinista, procesamiento y sensibilidad. La extensión define la interfaz de las aplicaciones en los servicios básicos del sistema para entradas/salidas, acceso al sistema de ficheros y gestión de los procesos.
	Incluir la gestión de sistemas para: - definir y gestionar la asignación de los recursos de los usuarios y el acceso - la configuración y la gestión del desempeño de recursos, sistemas de ficheros, procesos administrativos, listas, perfiles de plataforma/máquina - autorización de uso de recursos - sistema de copia de seguridad

Condiciones de Operación	Requisitos
	Control del acceso al sistema de datos, las funciones, el hardware y los recursos de software por los usuarios y procesos de los usuarios.
	Crear y conservar un manual de descripción técnica del sistema de información que debe contener como mínimo: - una lista de los componentes hardware del sistema de información - la distribución e interacción de los componentes del sistema en la red de datos, así como una descripción de las conexiones y del equipamiento de seguridad - un modelo de la arquitectura de datos de los objetos de información y sus relaciones - una lista de productos de software que interactúan y documentación relacionada - una lista de las aplicaciones software personalizadas con su fichero del diseño y de la arquitectura, su código fuente o una prueba de su depósito bajo custodia, cuando sea posible.
Servicios de Red Capacidad para apoyar las aplicaciones que precisan el acceso a datos y la interoperabilidad de aplicaciones en entornos heterogéneos de red.	Contar con comunicación de datos redundante, segura y protegida entre los servidores del ADiUCR.
	Establecer comunicación entre servidores del ADiUCR utilizando el protocolo IPsec (*Internet protocol security*). Además, la comunicación con los clientes de consumo con el protocolo TLS (*Transport Layer Security*).
	Tener interoperabilidad con los sistemas basados sobre otros sistemas operativos.
	Incluir servicios de seguridad para el acceso, la autenticación, confidencialidad, integridad y controles de no repudio y la gestión de las comunicaciones entre emisores y receptores de información en una red.
	Utilizar los anchos de banda recomendados para las comunicaciones entre los componentes de la solución y hacia los clientes y la optimización de los almacenes de datos.
	Verificar las condiciones de los servicios de comunicaciones, esquemas de multi proveedor de internet, equipo activo, soportes de almacenamiento; de manera que se asegure un servicio 24x7x365, incluso en el evento de falla del ISP (*Internet Service Provider*).
Servicios de seguridad Capacidad de proteger la información sensible y tratamientos en el sistema de información	Contar con un nivel apropiado de protección para toda la información custodiada en el ADiUCR
	Incluir un servicio de identificación/autentificación para confirmar las identidades de los solicitantes para el uso de los recursos del ADiUCR, el cual puede efectuarse en el inicio de la sesión o durante la sesión.
	Prevenir el uso no autorizado de los recursos dentro del ADiUCR, por ejemplo: ejecución, lectura, escritura, modificación o borrado de un recurso de datos/información
	Permitir la configuración personalizada de control de acceso y confidencialidad al menos en tres niveles de clasificación archivística: Serie Documental, Unidad Documental Compuesta o Expediente y Documento.

Condiciones de Operación	Requisitos
	Asegurar la integridad de los datos, es decir, que no sean alterados o destruidos en modo no autorizado.
	Incluir un servicio de confidencialidad de datos, el cual asegure que los datos no estén disponibles o no sean revelados a individuos o procesos informáticos no autorizados.
	Contar con un servicio de no repudio, por medio del cual se garantice que las entidades que participan en el intercambio de información no pueden negar la participación en él.
	Implementar controles de alto nivel para el acceso físico al centro de datos, donde se restrinja el acceso solamente para los usuarios autorizados, y puedan identificarse de manera unívoca a quienes hayan tenido posibilidad de ingreso.
Condiciones físicas de los equipos	Regular el uso eficiente de la energía de los equipos utilizados.
	Garantizar al menos la operación de todos los servicios y componentes del ADiUCR, cuando haya pérdida de suministro de energía. Validar especificaciones con la norma ANSI/TIA -942.
	Se recomienda que los equipos físicos que hospedan los servicios del ADiUCR o los equipos virtuales en los que estos se ejecuten, cuenten con unidades especializadas de almacenamiento para el sistema operativo y la información a preservar.
	El poder de procesamiento, la memoria RAM y el almacenamiento local en disco serán los que defina el desarrollador o fabricante de la solución.
	Contar con un plan de mantenimiento y cambio para el hardware que se utilice para la implementación del ADiUCR .
Almacenamiento	Debe prever un espacio de almacenamiento adecuado y escalable, para suplir las necesidades de todas las unidades de la UCR.
	Debe incluir almacenamiento para documentos de gran volumen.
	Los servicios deben poder ser hospedados localmente en el centro de datos de la UCR o en la nube (según directrices y necesidad)
	Contar con almacenamiento seguro y cifrado.
	Permitir el almacenamiento de las bitácoras de trazabilidad de manera que no puedan ser borradas, regrabadas o sobreescritas.
Búsquedas de Información	El ADiUCR debe contar con una interfaz de búsqueda que permita acceder al contenido.
	Verificar si un usuario tiene acceso a un determinado documento, o recurso de información, antes de retornar la lista de contenidos de una búsqueda. Para esto se pueden definir credenciales de autenticación.

Condiciones de Operación	Requisitos
	Debe permitir a los usuarios autorizados recuperar la Información de Contenido y el IDC.
	Permitir el acceso a copias de consulta de la información almacenada, que consistirá en un breve resumen de los metadatos de descripción más relevantes, imágenes de cada página que compone el documento y un resumen de seguridad.
	Integrar instrumentos de Descripción del Archivo para identificar e investigar fondos de interés potencial.
	Contar con una base de datos relacional para la información de los objetos de descripción.
	Incluir un servicio especializado para realizar las búsquedas que utilice un motor de Índice de Texto y procesamiento de lenguaje natural.
	Contar con análisis de léxico, análisis morfológico y puntaje de clasificación mediante algoritmos para cuantificar en qué medida un determinado registro coincide con palabras clave de búsqueda.
	Permitir la búsqueda de información a distintos niveles: fondo, subfondo, serie documental o unidad documental, por medio de metadatos descriptivos y de contenido de la información preservada, y que esta sea exportada en distintos formatos de fichero, según las necesidades de los usuarios.
Continuidad del negocio	Contar con un Plan de Continuidad del Negocio que cuente como mínimo con los siguientes elementos: - Identificación de los activos. - Valoración de Riesgos. - Establecimiento de Estrategias de Continuidad. - Establecimiento de roles, responsabilidades y procedimientos. - Estrategias, Procedimientos y Tiempo Meta de Recuperación - Manual de Procedimientos de Continuidad. - Plan de pruebas con calendario de cumplimiento, proceso de análisis de resultados y mejora continua.
	Contar con un servicio de Repositorio Alterno, que permita la continuidad de las operaciones y consultas, así como la salvaguarda de los activos de información ante ciber incidentes, y como medida en caso de catástrofe.
	El sitio alterno debe estar ubicado, idealmente, a una distancia no menor de 150 Kilómetros del sitio principal y deberá contar con medios de comunicación redundantes entre ambas instalaciones.
	Cumplir con la normativa institucional relacionada con la continuidad del negocio y la continuidad de las TIC. Considerar también la aplicación de la norma ANSI/TIA -942.

Fuente: Elaboración propia a partir de AENOR, 2015-b, p.43-44 y Castillo-Solano & Umaña-Alpízar, 2019.

3.3. Estudios de caso para la implementación del Modelo OAIS en la UCR

Según el diagnóstico elaborado en el capítulo 2 de esta investigación, en la Universidad de Costa Rica se utilizan diversos sistemas informáticos productores de información, que no han sido diseñados con las características necesarias para llevar a cabo la Preservación Digital Sistémica (PDS). Además, hay repetidas prácticas de almacenamiento de información en dispositivos no seguros como discos duros externos, dispositivos USB, hasta unidades ópticas de escritura como discos compactos, entre otros.

Estos factores implican una ruptura en la Cadena de Custodia Digital Archivística, por lo tanto, se pierde la certeza de que la información se mantenga íntegra, auténtica y confiable durante el tiempo que sea requerida, de los documentos nativos digitales y los digitalizados, que cada día representan un mayor porcentaje de la producción institucional.

Por ello, en este apartado se abordan dos escenarios tecnológicos para aplicar los requerimientos presentados en la Norma UNE-ISO 14721, mediante el Modelo OAIS, con el fin de que sirva de prototipo para que sean replicados en otros sistemas informáticos que existen en la Universidad de Costa Rica.

De esta manera, en primer lugar, se aborda el caso de los documentos de archivo que se gestionan dentro del Sistema de Gestión de Documentos Institucional (SiGeDI), el cual se seleccionó por su amplio rango de utilización a nivel de las unidades administrativas, académicas y de investigación, para el cumplimiento de trámites administrativos.

En segundo lugar, se analizará la preservación digital de una muestra de la Fototeca de la UCR, que se encuentra bajo custodia por el AUROL. El objetivo es aplicar el Modelo OAIS a documentos que no están dentro de sistemas, en este caso, producto de la digitalización a partir de soportes físicos, ya que proyectos de digitalización han sido desarrollados ampliamente dentro de la institución.

Si bien se trata de dos casos diferentes, el servicio de Archivo Digital debe ser uno sólo y transversal a toda la organización, lo que brinda un escenario ideal para llevar a cabo la Preservación Digital Sistémica.

3.3.1 Sistema de Gestión de Documentos Institucional (SiGeDI)

El SiGeDI, es un sistema informático y archivístico ampliamente utilizado en la UCR, con más de 500 instancias participantes, como por ejemplo oficinas en: vicerrectorías, facultades, escuelas, institutos y centros de investigación, programas de posgrados, sedes y recintos e incluso asociaciones de estudiantes (AUROL, s.f.)

Este alto grado adopción por parte de las distintas unidades académicas, administrativas y de investigación, se debe en gran parte a los beneficios que el sistema ofrece a la Universidad (figura 41), el cumplimiento de necesidades de gestión documental, y así también en cuanto a la experiencia que ofrece al usuario sobre su funcionamiento (usabilidad, accesibilidad, adaptabilidad y uso de firma digital) (AUROL y CI, s.f., p. 6-16).

Figura 41. *Beneficios que ofrece el SiGeDI a la UCR.*

Fuente: elaboración propia a partir de AUROL y CI, s.f., p.6-7.

Si bien el SiGeDI ofrece funcionalidades necesarias para la producción, gestión y almacenamiento de documentos, (figura 42), este sistema no es un repositorio archivístico digital confiable (RCD-Arch).

Figura 42. *Características archivísticas del SiGeDI de la UCR.*

Fuente: elaboración propia a partir de AUROL y CI, s.f., p.6-7

De esta manera, como se verá más adelante, el ADiUCR viene a asegurar la Preservación Digital Sistémica y la Cadena de Custodia Digital Archivística de los documentos que se generan por medio del SiGeDI, el cual para todos los efectos se constituye en realidad como un sistema de producción.

El SiGeDI "tiene el propósito de dotar al personal universitario con un instrumento automatizado, vía web, que asegure una administración eficiente de la gestión documental desde la planificación, creación, recepción, trazabilidad, selección y demás etapas del ciclo de vida de los documentos, asegurando la aplicación de requerimientos institucionales y normas archivísticas" (AUROL y CI, s.f., p.2).

El funcionamiento del SiGeDI desde el ámbito archivístico, corresponde al Archivo Universitario Rafael Obregón Loría, mientras que el apoyo técnico informático y de mantenimiento se recibe de parte del Centro de Informática de la UCR. Este sistema inició su

funcionamiento en el año 2018, por medio de un plan piloto y la posterior implementación paulatina en distintas instancias universitarias.

Su precedente es el SisDoc (Sistema de Gestión de Documentos), que también nace como un sistema institucional de producción y gestión de documentos, pero actualmente se encuentra en estado obsoleto (*legacy system*) ya que presentó problemas de escalabilidad, disminuyendo el rendimiento conforme se aumentaba en su uso.

Este sistema permite la creación de múltiples tipos de documentos como actas, constancias, circulares, convocatorias, bitácoras de asesoría, informes, entre otros. A todas las series documentales incluidas en el SiGeDI se les ha aplicado el proceso técnico de *identificación de documentos.* Además, la CUSED les ha aplicado el proceso técnico de *valoración de documentos* por procesos, a algunas de esas series.

Sumado a esto, el SiGeDI contiene piezas documentales que deben ser archivadas en expedientes con base en el Cuadro de Clasificación por Procesos, generando unidades documentales compuestas (expedientes). Además, durante la creación de los documentos, existen múltiples borradores y documentos de trabajo en los formatos de *Microsoft Word (.DOCX)* y *Libre Office Writter (ODT)*, de los cuales se producen documentos finalizados, en formato .PDF.

Durante el proceso de creación, edición y despacho de los documentos, el SiGeDI genera metadatos a nivel de expediente y documento que permiten entender su contexto y las relaciones con otros documentos.

A nivel de expediente, se pueden recuperar los siguientes metadatos:

- Información general: Nombre del expediente, descripción, ubicación física, si pasa a expurgo y el estado del trámite.
- Datos relacionados: Fecha de creación, fecha de vencimiento, documento inicial, documento final y cantidad de documentos que conforman el expediente.

A su vez, dentro de cada expediente se encuentran los documentos que lo componen y el siguiente conjunto de metadatos:

- Identificador único, descripción, remitentes, destinatarios, bitácora del documento, archivos adjuntos, documentos relacionados, palabras clave, clasificación del documento, expediente al que pertenece y propiedades del documento (Propietario, Tipo documental, Estado, Fecha creación, Formato: *Microsoft Word*)

Como puede verse son registros en tuplas de datos con información de descripción del expediente, los cuales, al no estar normalizados por medio de un estándar, no establecen claras relaciones entre los documentos ni se puede garantizar que estas relaciones permanezcan a mediano plazo, por lo que es vital la integración de este sistema con un servicio de Archivo Digital basado en estructuras METS.

3.3.1.1. Metodología de Ingesta del SiGeDI

Para la ingesta de los documentos del SiGeDi al ADiUCR se tienen dos escenarios:

1. Ingesta de los documentos producidos de forma previa, en custodia.
2. Integración continua, para la ingesta inmediata de los nuevos documentos digitales, tal y como se vayan produciendo.

Existe una serie de *requerimientos generales* que son transversales a los dos escenarios expuestos, y que deben cumplirse para todos los sistemas que transfieren información al ADiUCR..

Entre estos destaca la necesidad de que el sistema productor envíe la información de clasificación y agrupamiento de cada documento. Esta información debe especificar con claridad la estructura jerárquica multinivel, incluyendo la información mínima requerida para crear los elementos en AdiUCR si no existieran. Como mínimo debe incluir:

a. Código de Referencia (Identificador único) y nombre de cada uno de los Sub Fondos documentales que componen la estructura que contiene la serie documental y que refleja el Macroproceso, Proceso y Subproceso, según corresponda. Estos datos deben estar dispuestos en una estructura anidada por nivel jerárquico, donde puede usarse un acercamiento similar para las estructuras orgánicas.

b. Identificador o Código de Referencia y Nombre de la Serie Documental y Sub Serie Documental (si existiera).
c. Identificador o Código de Referencia y Nombre de la Unidad Documental compuesta (Expediente) al que pertenece el documento.

Otro requerimiento general es que la ingesta se realizará por documento; únicamente con documentos que se encuentren en estado de finalizado, es decir, que han sido despachados a sus destinatarios para la realización de un trámite. El sistema del ADiUCR deberá permitir la personalización de las listas de acceso hasta un nivel de pieza documental, para poder determinar el acceso a información pública o si existe algún tipo de restricción por datos personales y sensibles (Castillo-Solano y Umaña-Alpízar, 2018, p.247).

Para el escenario de Ingesta de los documentos producidos de forma previa y en custodia, el sistema del ADiUCR debe contar con una funcionalidad para la ejecución del método *Pull*. Por consiguiente, el ADiUCR debe desarrollar una aplicación *middleware*, que permita establecer medios de conexión entre el repositorio seguro del Archivo Digital y cada uno de los sistemas universitarios, generando los paquetes de información que serán transferidos al ADiUCR.

Cabe resaltar que, mediante esta propuesta, el ADiUCR, en conjunto con las unidades propietarias de cada sistema, deben asumir la tarea de interconectar ese *middleware*, sin embargo, se cuenta con la ventaja que no se deberán realizar modificaciones complejas de cada uno de los sistemas, para que estos generen y envíen los paquetes SIP. Esto se vuelve aún más importante sabiendo que en la UCR existen decenas de sistemas y que algunos ya están en desuso, por lo cual invertir en realizarles modificaciones podría ir en detrimento del uso de los recursos institucionales, mientras que los agentes de *middleware* pueden fácilmente reutilizar componentes en cada iteración, maximizando la eficiencia del proceso.

Es necesario que dentro de la información que se captura del sistema SiGeDI, se pueda recuperar datos de creación, modificación, entre otros, que permitirán entender cuál fue el contexto de creación y uso de la información.

Sin embargo, es fundamental que el ADiUCR sea capaz de interpretar todos los metadatos e información que capture y proceda a registrarla con base en la norma de descripción archivística ISAD-G e ISAAR-CPF, mediante los esquemas EAD y EAC, respectivamente y el diccionario

de Metadatos de Preservación PREMIS, realizando los procesos que permitan conservar el contexto de creación mencionado, la estructura de clasificación, agrupamiento y relaciones y las propiedades significativas, específicamente las relacionadas con contenido, autenticidad y autoría, ubicándose en los nodos correspondientes de la estructura METS del AIP empleando las codificaciones y los conjuntos de metadatos indicados.

El escenario de *Integración Continua* aplica para la ingesta inmediata de los nuevos documentos digitales tal y como se vayan produciendo, tanto para SiGeDI como para todos los otros sistemas que se encuentren produciendo activos y evidencias digitales. ADiUCR debe proveer una interfaz programática segura bajo la arquitectura de *REST* que permita el uso de mecanismos abreviados y sencillos de baja carga, de modo que pueda existir una integración completa.

Como mínimo ADiUCR deberá exponer controladores para 3 procesos, a saber:

- Autenticación/Autorización: Este proceso deberá otorgar un token perecedero al sistema solicitante que identifique el usuario que está solicitando la acción y permita validar si cuenta con los permisos en el objeto asegurado que le habiliten a realizar las acciones que va a intentar. Este token deberá perder su valor inmediatamente tras su uso o tras un determinado tiempo, que será establecido por los administradores del ADiUCR de acuerdo a lo que la institución considere seguro y conveniente.

- Ingesta de documentos: Este proceso deberá realizar la ingesta, para lo que el sistema productor deberá enviar el token de autorización, la información de clasificación y agrupamiento, la información de descripción, la información de contexto de creación y el documento mismo.

El controlador deberá como mínimo revisar la integridad del documento y la validez de sus firmas digitales (si las hubiere), deberá comprobar que no existen amenazas informáticas ligadas a la carga útil, tales como virus y malware, revisar y validar la calidad de la información recibida, localizar o crear las estructuras de clasificación y agrupamiento, recibir y procesar el contexto de creación, la estructura de clasificación, agrupamiento y relaciones y extraer las propiedades significativas, específicamente las relacionadas con contenido, autenticidad y autoría, y darles persistencia en los nodos correspondientes de la estructura METS del AIP empleando las codificaciones y los conjuntos de metadatos supra indicados.

Finalmente deberá devolver al sistema SiGeDI un reporte de todas las etapas (superadas o no) y un identificador universal de recurso, con el que SiGeDI reemplazará el localizador universal de recurso que actualmente sirve para localizar el fichero físico del documento, éste deberá desaparecer y no deberá volver a utilizarse este método por estar expuesto a toda forma riesgos, informáticos y humanos.

- Consulta de documentos: Este proceso será el que utilice SiGeDI para mostrar a sus usuarios los documentos cuando le sean solicitados, recibirá un identificador universal de recurso y el token de autorización, que representa al usuario que hace la solicitud y con éste llevará a cabo una revisión de control de acceso para verificar que este usuario tiene acceso al documento que solicita, así como a la calidad de los datos que puede ver, tomando la determinación de entregar una copia anonimizada o íntegra según sea el caso.

El controlador de consulta de documentos creará el paquete de difusión de información (DIP), de acuerdo al contrato de consumo que ADiUCR mantiene con SiGeDI y devolverá los metadatos y el documento en una forma en que SiGeDI pueda interpretarlos de forma nativa.

Esta API REST deberá publicarse de forma segura protegiendo el tráfico con TLS y una lista controlada de orígenes IP que pueden hacer consumo de la interfaz, en todos los casos los paquetes que se envían y reciben estarán expresados por la notación JSON y deberán ser tecnológicamente neutras, de manera que permitan interoperar con lenguajes y soluciones disímiles.

El desarrollo y mantenimiento de las API REST de ADiUCR, así como los agentes *middleware* serán de la responsabilidad del proveedor de software de Archivo Digital, tanto si se realiza un desarrollo local como si se adquiere un producto comercial para tal fin.

Es recomendable que la CIADi se mantenga alerta de los cambios de la tecnología que podrían ocasionar la necesidad de renovar o añadir nuevas interfaces programáticas, como el cambio de protocolo de aseguramiento de TLS del año 2022 que desactivó permanentemente la versión 1.1 o la irrupción de nuevos mecanismos como el prometedor sistema de llamada a procedimiento remoto de código abierto desarrollado inicialmente en Google gRPC.

3.3.1.2. Protocolo de Transferencia: ADiUCR y SiGeDI

El Protocolo de Transferencia es el acuerdo en el que se plantean los detalles de la transferencia por parte del sistema productor al Archivo Digital. Permite establecer las series documentales y las características técnicas informáticas y archivísticas necesarias, para llevar a cabo la preservación de la información. También incluye las propiedades significativas, los derechos que se ceden al transferir los documentos y las responsabilidades de ambas partes.

A continuación, se presenta el caso para la transferencia de los documentos del SiGeDI al ADiUCR (Tabla 25):

Tabla 25. *Protocolo de Transferencia de expedientes del SiGeDI al ADiUCR.*

PROTOCOLO DE TRANSFERENCIA
DE DOCUMENTOS ELECTRÓNICOS AL ADiUCR
Número PT-1-2023

Versión 1.0 Fecha: agosto de 2023 Autores: Jéssica Barahona Chavarría y Jorge Luis Mora Cerdas

Datos identificativos

Identificador	UCR-ADiUCR-SIGEDI-01-2023
Órgano productor o custodio	Productor: Instancias universitarias que utilizan el SiGeDI. Custodia dentro del SiGeDI: AUROL y Centro de Informática (CI).

Alcance

Alcance documental (series documentales)	Todas las series documentales que contengan documentos en estado de *finalizados* que se generen o ingresen al SiGeDI.
Alcance tecnológico (sistemas de información):	Sistema de Gestión de Documentos Institucional (SiGeDI).

	Fecha de inicio de operatividad: 2018. Versión 1. Base de datos: ORACLE. Sistema Operativo: Puede ejecutarse en cualquier sistema operativo por medio de un navegador *web.* Lenguaje de programación: .NET.
Alcance orgánico (órganos productores o custodios):	Productor: instancias universitarias que utilizan el SiGeDI. Custodio: SiGeDI (AUROL y CI).
Alcance cronológico:	2018 - en adelante
Duración del protocolo y fecha de revisión:	5 años o hasta que haya alguna modificación en el modelo de datos o la plataforma tecnológica. Próxima revisión: Junio del 2028.

Parámetros de Ingreso

Canal de transferencia:	Método: Pull Transferencia automatizada: el ADiUCR recogerá los paquetes SIP y los manifiestos o inventarios de transferencia, por medio de una aplicación *middleware.*
Formatos de fichero admitidos:	Documentos finalizados en formato PDF. Se debe mantener la firma digital original de cada documento.
Metadatos descriptivos obligatorios:	- Descripción de los documentos mediante la norma ISAD (G), codificados en el estándar EAD 2002. Nota: posteriormente al ingreso, se deben incorporar los metadatos para registros de autoridad, planteados en la norma ISAAR-CPF, codificados en el estándar EAC.
Estructura del contenedor de transferencia (SIP):	Se deberá crear un SIP para cada documento a transferir, según los formatos admitidos indicados en este protocolo. Cada paquete SIP será un fichero en formato XML,utilizando la estructura METS, con los siguientes

	elementos: ● Elemento <mets:metsHdr> con la información de encabezado del XML. ● Un único elemento <mets:dmdSec> con los metadatos descriptivos del documento, contenidos en el mismo documento METS, codificados en EAD. ● Elementos <mets:amdSec>: metadatos técnicos <techMD> (sobre Objetos PREMIS); metadatos <rightsMD> (sobre Derechos PREMIS) y metadatos <digiprovMD> (sobre Eventos PREMIS y Agentes PREMIS). ● Un elemento <mets:fileSec> con un elemento <fileGrp> que contiene un <fContent>, que contendrá el documento a transferir, codificado en Base64. Debe contener el número característico *hash* de la firma digital del documento, calculado con base al algoritmo criptográfico SHA 256, incluido como un atributo. En el caso de que se exceda el tamaño máximo soportado por el fichero XML, se definirá un elemento <FLocat>, dentro del elemento <fileGrp>, para designar una ubicación de fichero única, por medio de una URL u otro elemento parecido. ● La información de estructura de almacenamiento (Fondo, Subfondo, Serie y Expediente) será capturada por medio del elemento <mets:structmap>, capturando los metadatos del Cuadro de Clasificación del SiGeDI. Cada SIP se enviará firmado electrónicamente, con firma XAdES-T enveloping.
Verificaciones del ADiUCR	Deberá verificar automáticamente, antes de autorizar el ingreso del SIP al sistema: - Que el origen de la transferencia es de confianza y está autorizado. - Que cada fichero esté libre de virus. - Que todos los ficheros del SIP corresponden con sus respectivos números característicos (*hash*), incluidos en el manifiesto. - Que los ficheros corresponden a los formatos

	indicados en este protocolo. - Que el METS de cada fichero contiene los metadatos obligatorios en el estándar descriptivo indicado. - El repositorio verifica la identidad del emisor, verifica la autenticidad e integridad del SIP, mediante la firma digital, toma el fichero del SIP, con base en la sección <mets:fileSec> , verifica su integridad y lo procesa para ingreso como AIP, con las verificaciones de cumplimiento y seguridad señaladas previamente. En caso del incumplimiento de cualquiera de estos requisitos se realizará la notificación al encargado para su rectificación.
Normalización de formatos	Se recibirán los documentos en la versión de formato PDF que genera el SiGeDI, con la respectiva firma digital.
Metadatos que va a añadir el ADiUCR	Añadirá al AIP los siguientes metadatos: - Metadatos tecnológicos relativos al 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: 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 de 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 participantes en el proceso de ingreso en la sección METS <amdSec> dentro de la unidad semántica correspondiente del esquema PREMIS.

	- Sellado electrónico del AIP con certificado electrónico del ADiUCR mediante firma tipo XAdES XL en conformidad con el estándar y sellado de fecha y hora de la autoridad competente y de confianza.

Propiedades Significativas a conservar en el ADiUCR

Relacionadas con la apariencia	Asegurar las características del objeto digital que permitan la representación inteligible del documento.
Relacionadas con las funcionalidades	En los casos posibles, mantener las funcionalidades de hiperenlaces insertadas en el texto de los documentos PDF.
Relacionadas con el contexto	Se preservará la información de procedencia digital, las relaciones con otros objetos digitales, su cadena de custodia y el historial de cambios autorizados.
Relacionadas con la autenticidad/significación/valor	El Archivo Digital deberá extraer las propiedades significativas de autenticidad e integridad:, 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, y se conservan en el metadato PREMIS respectivo. Se asegurará la integridad de la información mediante la firma XAdES del AIP.

Plazos de conservación

Plazo de conservación de las propiedades significativas de apariencia	Se deben eliminar junto con los paquetes AIP, de acuerdo con el plazo de conservación respectivo.
Plazo de conservación de las propiedades significativas de funcionalidades	Se deben eliminar junto con los paquetes AIP, de acuerdo con el plazo de conservación respectivo.
Plazo de conservación de las propiedades significativas de contexto	Se deben eliminar junto con los paquetes AIP, de acuerdo con el plazo de conservación respectivo.
Plazo de conservación de las propiedades significativas de autenticidad	Se deben eliminar junto con los paquetes AIP, de acuerdo con el plazo de conservación respectivo.

Plazo de conservación total	Cada paquete archivístico se conservará de acuerdo con la Tabla de Plazos de Conservación, según la vigencia establecida en la serie.

Derechos que se ceden

Derechos de difusión y acceso	Los documentos serán de acceso público, a menos que existan restricciones de acceso y/o datos personales o sensibles. Se recomienda aplicar un proceso de anonimización, por medio de una copia, en la cual no estén disponibles los datos personales o sensibles de las personas. Es decir, el Archivo Digital genera una copia anonimizada a partir del documento íntegro (el cual no se modificará); la copia será facilitada a los distintos usuarios según el nivel de acceso correspondiente.
Derechos de uso (propiedad intelectual)	El ADiUCR podrá emitir copias auténticas de los documentos, aplicando el nivel de acceso respectivo.
Derechos de modificación para preservación	Es permitido modificar la representación del formato de las series documentales, con el objetivo de mantener el acceso y combatir la obsolescencia tecnológica. No se permitirá la modificación del contenido de los documentos.

Con la firma de este protocolo, las partes firmantes se obligan a:

Por el Archivo Universitario Rafael Obregón Loría y el Centro de Informática	Por el Archivo Digital de la Universidad de Costa Rica
- Transferir al ADiUCR, con la periodicidad indicada en este protocolo, todos los documentos en estado de *finalizados*, generados por medio del SiGeDI, junto con los documentos adjuntos, en caso de existir. - Realizar la transferencia mediante el canal y en el formato, estructura y metadatos que se indican en este protocolo.	- Aceptar las transferencias de todos los documentos en estado de *finalizados*, generados por medio del SiGeDI, junto con los documentos adjuntos, en caso de existir que se ajusten a la periodicidad, formato, estructura y metadatos que se indican en este documento. - Conservar de forma íntegra, auténtica y accesible los documentos transferidos desde

- Ceder, sobre la documentación transferida, los derechos que se indican en este documento. - Acceder a los documentos mediante el canal proporcionado por el ADiUCR, de acuerdo con su política de acceso definida en este documento.	el SiGeDI, durante el plazo que se indica en este documento. - Notificar a la CIADi cualquier modificación realizada sobre los documentos conservados. - Asumir el coste de conservar los documentos de forma íntegra, auténtica y accesible durante el ciclo de conservación expresado en este documento. - Aplicar sobre los documentos transferidos el procedimiento de acceso de acuerdo con los derechos sobre la documentación que se indican en este documento.
[Cargos firmantes] [Lugar y fecha de firma]	[Cargo firmante] [Lugar y fecha de firma]

Fuente: Elaboración propia con base en Castillo-Solano y Umaña-Alpízar (2018, p.248-258).

3.3.2. Fototeca de la Universidad de Costa Rica

La Fototeca de la Universidad de Costa Rica, tomada en consideración en esta investigación como ejemplo de serie documental no textual, representa una valiosa y abundante fuente de información tanto para la comunidad universitaria como para la sociedad costarricense, cuyo potencial no ha sido explotado en su totalidad.

Las fotografías representan "una fuente documental sobresaliente, un registro visual de primera magnitud en un determinado contexto espacio-temporal, que resulta atractivo para el estudio del patrimonio cultural y para la puesta en marcha o estudio de cualquier intervención de conservación y restauración" (Universidad de Navarra, 2023, p.3).

Se puede considerar que las fotografías tienen la capacidad de capturar y transmitir información visual tanto a nivel de patrimonio material (sobre objetos tangibles: obras de arte, arquitectura, etc.), así como de patrimonio inmaterial (tradiciones, artes del espectáculo, usos sociales, rituales, actos festivos, entre otros) (Universidad de Navarra, 2023).

De esta manera, independientemente del soporte en el cual se encuentran las fotografías, se debe considerar que "la conservación es uno de los objetivos principales de cualquier fondo

fotográfico, junto con la difusión. Toda entidad cultural que posee un fondo fotográfico debe asumir responsablemente la correcta custodia de este material, garantizando la conservación del patrimonio cultural que alberga" (Foix, 2003, p.17).

En el caso de la Universidad de Costa Rica, la serie documental Fotografías fue valorada por la CUSED, de acuerdo con la Tabla de Plazos de Conservación y Eliminación de Documentos para Series Comunes en la UCR CUSED-TPC-2018, actualizada en octubre del 2021.

De esta manera, la valoración de esta serie se representa en la Tabla 26:

Tabla 26. *Valoración de la serie documental Fotografías.*

Serie documental	**Contenido**	Vigencia Administrativa-Legal			Valor Científico Cultural
		Unidad	Archivo Central	AUROL	
Fotografías	Imágenes alusivas al quehacer universitario como retratos, edificaciones, actividades académicas, de investigación, acción social, estudiantiles, administrativas, entre otras, relacionadas con el contexto universitario.	1 año	0 años	Permanente	SÍ

Fuente: Elaboración propia a partir de CUSED, 2021-2, p.31.

Mediante este extracto de la Tabla de Plazos, se observa que la serie documental de fotografías se considera de valor científico cultural, por lo que su conservación es permanente. Según esta Tabla, la serie debe ser almacenada por un plazo de 1 año en las unidades productoras, posterior al cual se deben transferir al AUROL.

Además, algunos criterios para la preselección de las fotografías que se deben transferir al AUROL para su conservación permanente son las siguientes (CUSED, 2021-2):

- Se deben eliminar: duplicados, desenfocadas (en caso de que solamente se cuente con una imagen de la actividad, lugar o personaje, y ésta es visible aunque desenfocada, se debe conservar), reiterativas, fuera del contexto institucional, dañadas de alguna forma (digitales)

- Cuando exista edición de fotografías: dos archivos de las fotografías en formatos jpg o tif: Alta resolución (impresión) y Baja resolución (optimizadas para web).
- Metadatos que debe contener: Fecha, Lugar, Personajes, Nombre de la actividad, Persona que tomó la fotografía.

El AUROL, ha realizado un trabajo de preservación exhaustivo con las transferencias de colecciones fotográficas que ha recibido desde las distintas unidades de la UCR, aplicando procesos de:

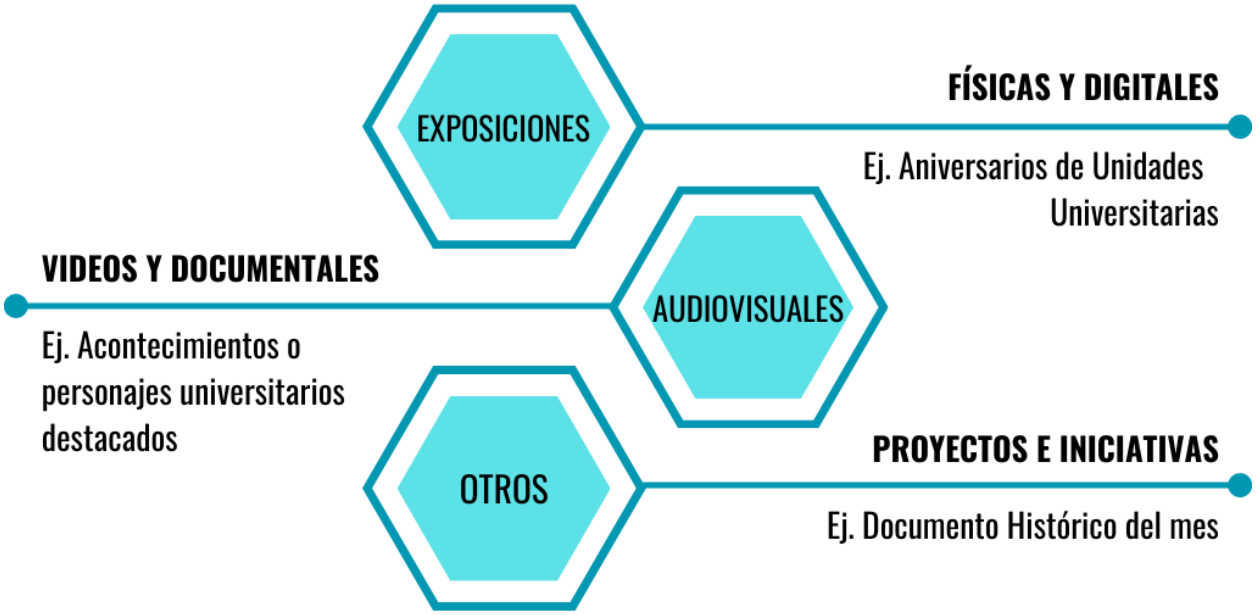
- Conservación preventiva: colocación de las fotografías en sobres especiales de papel libre de ácido, así como almacenamiento en cajas diseñadas a la medida, también libres de ácido, las cuáles se mantienen en un depósito con temperatura controlada..
- Descripción documental: obteniendo como producto inventarios basados en normas internacionales como por ejemplo ISAD-G.
- Digitalización: escaneo de las fotografías que se encuentran en soporte físico.

Estos esfuerzos se realizan como parte de las funciones que desempeña el AUROL, para lograr la difusión del patrimonio documental universitario, tal y como se establece en el artículo 6 del Reglamento del Sistema de Archivos de la Universidad de Costa Rica en sus incisos “e. Rescatar, custodiar y difundir el patrimonio documental universitario”, y “f. Garantizar el acceso a la información archivística universitaria” (Consejo Universitario de la UCR, 2008, p.2).

Gracias a esto, la serie documental “Fotografías”, se encuentra a disposición de la comunidad universitaria, esto puede observarse a través de las consultas que recibe el AUROL. Así por ejemplo, en el año 2021 se recibieron 32 consultas sobre fotografías y en el año 2022, se recibieron 25.

Las fotografías custodiadas por el Archivo Universitario de la UCR, son un insumo fundamental en procesos de difusión, siendo utilizadas en exposiciones, videos y otros proyectos (figura 43).

Figura 43. *Uso de la serie documental Fotografías para difusión en la UCR.*



Fuente: Elaboración propia. 2023.

Sin embargo, los métodos utilizados para tener a disposición de los usuarios la información contenida en esta serie documental (es decir para brindarles acceso), se basa en la necesidad de que exista en primera instancia una solicitud, la cual posteriormente será atendida. Así, como indica el profesor Dr. Daniel Flores (2022), se requiere que la UCR, como institución de educación superior y cultura, favorezca la transparencia activa, al ofrecer y difundir información de interés público, a través de canales formales de comunicación sin la necesidad de que medie ninguna solicitud previa.

Para lograr este tipo de difusión, la implementación del ADiUCR resulta fundamental, ya que en su modelo funcional se aplica la entidad "Acceso", mediante la cual se ofrecerán interfaces de consulta a los fondos de información del ADiUCR.

Actualmente, el AUROL posee bajo su custodia para conservación permanente, fotografías de las siguientes procedencias:

- Archivo Universitario Rafael Obregón Loría (AUROL)
- Centro Infantil Laboratorio (CIL)
- Colección Emma Gamboa Alvarado (donación)
- Colección Fernando Baudrit Solera (donación)

- Consejo Universitario
- Danza Universitaria (Danza U)
- Escuela de Enfermería
- Escuela de Química
- Facultad de Ciencias Agroalimentarias
- Facultad de Ciencias Económicas
- Facultad de Medicina
- Facultad de Odontología
- Oficina de Asuntos Internacionales y Cooperación Externa (OAICE)
- Oficina de Comunicación Institucional (OCI)
- Oficina de Planificación Universitaria (OPLAU)
- Oficina de Recursos Humanos (ORH)
- Oficina de Registro e Información (ORI)
- Oficina Ejecutora del Programa de Inversiones (OEPI)
- Programa de Atención Integral de Salud (PAIS)
- Programa de Investigaciones en Desarrollo Urbano Sostenible (ProDUS)
- Semanario Universidad
- Unidad de Programas Deportivos, Recreativos y Artísticos (UPDRA)
- Vicerrectoría de Acción Social (VAS)
- Vicerrectoría de Docencia (VD)
- Vicerrectoría de Investigación (VI)

La difusión de la colección fotográfica de la UCR, es una obligación que no se debe seguir posponiendo. Sin embargo, para proteger las imágenes digitales y lograr su acceso y disponibilidad a largo plazo, así como para ofrecer un servicio más completo a los usuarios (metadatos, formatos accesibles, fiabilidad, etc.), es necesario transferirlas al ADiUCR, de manera que se aplique a ellas el modelo OAIS.

Cabe destacar que una vez implementado el ADiUCR, la información producida en las unidades, será transferida inmediatamente al Archivo Digital, por lo cual, se requiere que la CUSED modifique las Tablas de Plazos con respecto a las Vigencias Administrativas Legales, en las unidades productoras.

Como muestra para esta investigación, a continuación se presenta el caso de la colección fotográfica de la Unidad de Programas Deportivos Recreativos y Artísticos (UPDRA). Se trata de una colección compuesta por 732 fotografías, a la cual ya se le aplicó la descripción archivística, por lo que cuenta con un inventario completo. También se encuentra digitalizada y almacenada en los servidores del AUROL.

Como puede observarse, se trata de una colección que está lista para su difusión a la comunidad universitaria y a la sociedad costarricense, la cual puede utilizarse como modelo para la ingesta de documentos de archivo no textuales al ADiUCR, y que además no se encuentran dentro de sistemas de información.

3.3.2.1. Metodología de Ingesta de la colección fotográfica UPDRA

Para la ingesta, en el caso de la colección fotográfica de la UPDRA, el ADiUCR debe contar con una funcionalidad para la ejecución del método *Push*, de forma que en lugar de generar los paquetes de información SIP, se realizará una carga por medio de lotes, través de un *agente de sincronización* que interprete la estructura física de almacenamiento para crear o actualizar la estructura lógica de clasificación en términos de la estructura jerárquica multinivel, sin intervención humana. Estos grupos o lotes, deben pasar por la validación del ingreso en el ADiUCR e irán directo al almacenamiento convertidos en AIP, proceso realizado ya estando dentro del ADiUCR.

El agente de sincronización deberá capturar los metadatos descriptivos de las fotografías a partir de la hoja de cálculo de inventario existente e inferir la información de clasificación de acuerdo con la estructura del directorio donde se encuentren ubicadas las fotografías (Castillo-Solano y Umaña-Alpízar, 2018, p.246).

Cabe destacar que los inventarios generados en el AUROL, para las fotografías (y otras series documentales), están basados en la norma ISAD-G, para mantener la normalización de los campos descriptivos. Este aspecto es favorable porque se puede planificar la inferencia de la información de los inventarios, por medio del establecimiento de las equivalencias o *crosswalks* de los campos descriptivos de la ISAD-G con la EAD.

Sumado a ello, el inventario se realizó a nivel de pieza documental, es decir, cada una de las fotografías de la UPDRA fueron descritas en una fila única en la hoja de cálculo, lo que facilitará la recuperación de los metadatos descriptivos.

Las fotografías de la UPDRA, se puede acceder hasta un nivel de pieza documental, ya que son de acceso público y no existen restricciones por datos personales ni sensibles.

El desarrollo y mantenimiento del agente de sincronización será responsabilidad del proveedor de *software* de Archivo Digital, tanto si se realiza un desarrollo local como si se adquiere un producto comercial para tal fin.

3.3.2.2. Protocolo de transferencia: ADiUCR y colección fotográfica UPDRA

Tabla 27. *Protocolo de Transferencia de la colección fotográfica de la UPDRA al ADiUCR.*

PROTOCOLO DE TRANSFERENCIA
DE DOCUMENTOS ELECTRÓNICOS AL ADiUCR
Número PT-2-2023

Versión 1.0 Fecha: agosto de 2023 Autores: Jéssica Barahona Chavarría y Jorge Luis Mora Cerdas

Datos identificativos

Identificador	UCR-ADiUCR-CF-UPDRA-01-2023
Órgano productor o custodio	**Productor**: Unidad de Programas Deportivos Recreativos y Artísticos (UPDRA) **Custodia**: AUROL

Alcance

Alcance documental (series documentales)	Colección fotográfica.
Alcance tecnológico (sistemas de información):	No se encuentra en un sistema automatizado. Las fotografías digitalizadas se encuentran en los servidores del AUROL.

Alcance orgánico (órganos productores o custodios):	**Productor**: Unidad de Programas Deportivos Recreativos y Artísticos (UPDRA) **Custodia**: AUROL
Alcance cronológico:	1990-2006
Duración del protocolo y fecha de revisión:	5 años o hasta que haya alguna modificación en el modelo de datos o la plataforma tecnológica. Próxima revisión: Junio del 2028.

Parámetros de Ingreso

Canal de transferencia:	Método: *Push.* Transferencia con intervención humana: Se realizará la ingesta por lotes. En este caso, no se requiere de la creación de un SIP. El ADiUCR contará con la funcionalidad de aplicar los controles y validaciones necesarios antes de generar el AIP.
Formatos de fichero admitidos:	TIFF (formato en el que se encuentran digitalizadas las fotografías).
Metadatos descriptivos obligatorios:	- Descripción de los documentos mediante la norma ISAD (G), codificados en EAD 2002. Nota: posteriormente al ingreso, se deben incorporar los metadatos para registros de autoridad, planteados en la norma ISAAR-CPF, codificados en el estándar EAC.
Estructura del contenedor de transferencia (SIP):	En este caso no se crearán SIP como paquetes contenedores para la transferencia, pero se deberán asegurar los siguientes elementos en la creación del paquete AIP, en formato XML, utilizando la estructura METS: ● Elemento <mets:metsHdr> con la información de encabezado del XML. ● Un único elemento <mets:dmdSec> con los metadatos descriptivos del documento, contenidos en el mismo documento METS, codificados en EAD. ● Elementos <mets:amdSec>: metadatos técnicos <techMD> (sobre Objetos PREMIS); metadatos

	<rightsMD> (sobre Derechos PREMIS) y metadatos <digiprovMD> (sobre Eventos PREMIS y Agentes PREMIS). En <mets:amdSec> <techMD> también incluir los metadatos ANSI/NISO Z39.87-2006(R2017), codificados mediante el esquema MIX en XML. ● Un elemento <mets:fileSec> con un elemento <fileGrp> que contiene un <fContent>, que contendrá el documento a transferir, codificado en Base64. ● La información de estructura de almacenamiento (Fondo:UCR, Subfondo: Fototeca, Colección: UPDRA) será capturada por medio del elemento <mets:structmap>, capturando los metadatos del Cuadro de Clasificación inferidos de las carpetas compartidas donde se encuentran las fotografías.
Verificaciones del ADiUCR	El ADiUCR deberá verificar automáticamente, antes de autorizar el ingreso de las fotografías al sistema: - Que el origen de la transferencia es de confianza y está autorizado. - Que cada fichero esté libre de virus. - Que los ficheros corresponden a los formatos indicados en este protocolo. - Que el METS de cada fichero contiene los metadatos obligatorios en el estándar descriptivo indicado. - El repositorio verifica la identidad del emisor. En caso del incumplimiento de cualquiera de estos requisitos se realizará la notificación al encargado para su rectificación.
Metadatos que va a añadir el ADiUCR	Añadirá al AIP los siguientes metadatos: - Metadatos tecnológicos relativos al formato y características de los ficheros ingresados, en la sección METS <amdSec>dentro de la unidad semántica correspondiente del esquema PREMIS. - Metadatos de los eventos de 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 participantes en el proceso de ingreso en la sección METS <amdSec>dentro de la unidad semántica correspondiente del esquema PREMIS. - Sellado electrónico del AIP con certificado electrónico del ADiUCR mediante firma tipo XAdES XL en conformidad con el estándar ETSI TS 101 903 y sellado de fecha y hora de la autoridad competente y de confianza.

Propiedades Significativas a conservar en el ADiUCR

Relacionadas con la apariencia	Documentos TIFF, se preserva la apariencia completa durante el plazo de vigencia. Para los documentos en XML, la apariencia no es una propiedad significativa.
Relacionadas con las funcionalidades	No aplica
Relacionadas con la autenticidad/significación/valor	La firma del paquete, o bien los metadatos de evento en el AIP. La autenticidad de la procedencia se derivará a la firma de archivo del AIP. Se conservará, como metadato de preservación, 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. Se deben conservar los datos EXIF (*Exchangeable Image File Format*) disponibles de cada fichero.

Plazos de conservación

Plazo de conservación de las propiedades significativas de apariencia	Conservación Permanente.
Plazo de conservación de las propiedades significativas de funcionalidades	No aplica.
Plazo de conservación de las propiedades significativas de autenticidad	Conservación Permanente.

Plazo de conservación total	Conservación Permanente.

Derechos que se ceden

Derechos de difusión y acceso	Los documentos son de acceso público en el mismo momento que son transferidos al ADiUCR. Se puede visualizar: • Todos los documentos TIFF. • Todos los datos contenidos en documentos XML.
Derechos de uso (propiedad intelectual)	Podrá emitir copias auténticas de los documentos que tengan permitido el acceso público. En todo caso se deberá respetar lo dispuesto en la Ley 6683 Ley de Derechos de Autor y Derechos Conexos.
Derechos de modificación para preservación	Es permitido modificar la representación del formato de la serie de fotografías, con el objetivo de mantener el acceso, en el plazo determinado en este protocolo. Toda modificación será notificada antes y después de su ejecución.

Con la firma de este protocolo, las partes firmantes se obligan a:

Por el Archivo Universitario Rafael Obregón Loría	Por el Archivo Digital de la Universidad de Costa Rica
- Transferir al ADiUCR todas las imágenes de la colección fotográfica de la UPDRA. - Realizar la transferencia mediante el canal y en el formato, estructura y metadatos que se indican en este protocolo. - Ceder, sobre la documentación transferida, los derechos que se indican en este documento. - Acceder a los documentos mediante el canal proporcionado por el ADiUCR, de acuerdo con su política de acceso definida en este documento.	- Aceptar las transferencias de todas las imágenes de la colección fotográfica de la UPDRA que se ajusten a la periodicidad, formato, estructura y metadatos que se indican en este documento. - Conservar de forma íntegra, auténtica y accesible todas las imágenes de la colección fotográfica de la UPDRA, durante el plazo que se indica en este documento. - Notificar a la CIADi cualquier modificación realizada sobre los documentos conservados. - Asumir el coste de conservar los documentos de forma íntegra, auténtica y accesible durante el ciclo de conservación

	expresado en este documento. - Aplicar sobre los documentos transferidos el procedimiento de acceso de acuerdo con los derechos sobre la documentación que se indican en este documento.
[Cargo firmante] [Lugar y fecha de firma]	[Cargo firmante] [Lugar y fecha de firma]

Fuente: Elaboración propia con base en Castillo-Solano y Umaña-Alpízar (2018, p.248-258).

3.3.3. Organización de los documentos en el ADiUCR

Resulta fundamental organizar de manera sistemática la información que estará bajo la custodia del Archivo Digital, para asegurar y facilitar su mantenimiento, uso y disposición, durante el tiempo que sea requerida. Para ello, el ADiUCR debe implementar el Cuadro de Clasificación por Procesos de la Universidad de Costa Rica, para asegurar que la información mantiene una estructura lógica adecuada, que refleje la ejecución de las funciones respectivas, las cuales se prueban por medio de los documentos de archivo y datos.

Cabe destacar que en la UCR, el Cuadro de Clasificación por Procesos se ha desarrollado de forma parcial, en los cuales se reflejan 7 macroprocesos, los cuales se resumen a continuación (Tabla 28):

Tabla 28. *Macroprocesos y procesos identificados en la UCR reflejados en el SiGeDI.*

Macroproceso	Procesos
A. Gestión estratégica	A.1 Gestión de órganos colegiados A.2 Gestión de la Calidad A.3 Gestión de la identidad A.4 Gestión de las comunicaciones A.5 Gestión de Congresos Universitarios A.6 Gestión de Proyectos de Ley A.7 Gestión de los Reglamentos Generales de la Universidad de Costa Rica A.8 Elaboración o modificación de normativa institucional
B. Gestión de acción social	B.1 Gestión de proyectos de acción social
C. Gestión de docencia	C.1 Gestión de proyectos docentes C.2 Gestión de desarrollo curricular

Macroproceso	Procesos
	C.3 Desconcentración y/o descentralización de carreras en sedes regionales C.4 Autoevaluación y gestión de la calidad y excelencia académica con fines de mejoramiento, certificación, acreditación o equivalencia sustancial de carreras de grado C.5 Gestión de cátedras conmemorativas, temáticas e internacionales C.6 Gestión del recurso docente C.7 Gestión de solicitudes de información del expediente académico del docente C.8 Evaluación Académica
D. Gestión de investigación	D.1 Promoción y gestión de programas, proyectos y actividades de investigación D.2 Cooperación y financiamiento de la investigación D.3 Gestión de transferencia del conocimiento innovador D.4 Registro de marcas
E. Gestión estudiantil	E.1 Admisión E.2 Permanencia E.3 Graduación E.4 Validación de estudios universitarios
F. Gestión administrativa	F.1 Contratación administrativa F.2 Gestión del Presupuesto en Universidad de Costa Rica F.3 Gestión Documental F.4 Gestión de bienes institucionales F.5 Gestión de importaciones F.6 Promoción y facilitación de servicios de tecnología de la Información y telecomunicaciones F.7 Asesoría Jurídica F.8 Gestión de Servicios Contratados F.9 Trasiego de documentos F.10 Gestión para el cobro de deducibles por infracciones de tránsito F.11 Gestión de mantenimiento de maquinaria y equipo F.12 Asesoría Técnica para la adquisición de Aires Acondicionados F.13 Gestión del acceso vehicular y áreas de estacionamiento F.14 Gestión de la seguridad universitaria F.15 Servicio de Transporte Universitario F.16 Mantenimiento vehicular F.17 Autorización de conducción de vehículos institucionales F.18.1 Marchamo F.19 Abastecimiento de combustible F.20 Asesoría Técnica para adquisición de vehículos F.21 Revisión de emisión de gases. F.22 Gestión del Servicio de transporte externo F.23 Gestión de la infraestructura institucional F.24 Gestión de la participación de personal universitario en eventos internacionales F.25 Gestión de Nombramientos y Juramentaciones F.26 Fiscalización de la Gestión Universitaria

Macroproceso	Procesos
G. Gestión de estudios de posgrado	G.1 Gestión de desarrollo curricular G.2 Admisión Integral G.3 Permanencia G.4 Graduación G.5 Validación de estudios universitarios G.6 Gestión de permiso-beca Sistema de Estudios de Posgrado-CONARE G.7 Gestión de becas en programas de posgrado con financiamiento complementario G.8 Autoevaluación con fines de mejoramiento y acreditación de programas de posgrado

Fuente: Elaboración propia a partir de información suministrada por la Sección de Normalización del AUROL (2023).

Al respecto, el SiGeDI cuenta con la funcionalidad de clasificar los documentos generados y recibidos, de acuerdo con dicho instrumento de clasificación archivística, a partir del proceso del cuál se derivan. Como consecuencia de la aplicación del proceso de clasificación, el SiGeDI va conformando los expedientes de cada proceso ejecutado, con todos los documentos y sus respectivos documentos adjuntos.

Por lo tanto, el ADiUCR debe ser capaz de crearla estructura del Cuadro de Clasificación y darle persistencia en la sección de Mapa Estructural de METS para cada uno de los documentos transferidos desde el SiGeDI, para asegurar de forma confiable el orden lógico y el contexto en el cual se creó o recibió la información y la conformación de Expedientes Electrónicos con capacidad de control de integridad mediante índices electrónicos seguros.

De esta forma, según indican Castillo-Solano y Umaña Alpízar (2018, p.261-262), un Archivo Digital debe permitir conformar los expedientes electrónicos, con los siguientes componentes:

- Metadatos del expediente
- Documentos que conforman cada expediente
- Índice electrónico: el cual corresponde a un objeto digital que contiene la identificación de los documentos que componen el expediente electrónico, para reflejar su organización.
- Firma digital del índice electrónico: garantiza la autenticidad e integridad del contenido del índice y los documentos que conforman el expediente electrónico y su estructura.

Sin embargo, para el caso de las fotografías que se custodian en el AUROL, estas han sido agrupadas como colecciones, es decir, no se han organizado archivisticamente como producto de la ejecución de una función dentro de un proceso administrativo, por lo cual, no es posible aplicarles estrictamente todos los niveles del Cuadro de Clasificación Institucional. Así, el ADiUCR, debe permitir la organización de este tipo de documentos, infiriendo la información de Clasificación según la estructura de las carpetas compartidas donde se encuentren almacenadas.

3.3.4. Esquema de metadatos

En el ADiUCR, se utilizará la estructura METS para la representación de los metadatos de cada uno de los paquetes archivísticos, es decir, para la transferencia (SIP), el almacenamiento en el ADiUCR (AIP) y el consumo de la información (DIP).

En este sentido, se utilizarán primordialmente las 5 primeras secciones de METS, como se muestra a continuación (figura 44 y Tabla 29):

Figura 44. *Estructura de METS para el ADiUCR.*

Fuente: Elaboración propia, 2023.

Tabla 29. *Estructura de METS para el ADiUCR.*

Sección de METS	Elemento METS	Descripción	Tipos de metadatos	Elementos METS
Cabecera METS (METS Header)	**<metsHdr>**	Incluirá los metadatos que describen el propio documento METS (documento XML que representa el paquete archivístico), como su fecha de creación y datos del *agente* o persona que lo realizó.	Sobre fecha de creación del documento METS, fecha de última modificación y estado	<metsHdr>
			Nombre de uno o más agentes	<agent>
Metadatos Descriptivos (Descriptive Metadata Section)	**<dmdSec>**	En esta sección se incluirán los metadatos descriptivos del documento de archivo que se transfiere, según los esquemas EAD (equivalencias ISAD-G) y EAC (equivalencias ISAAR-CPF).	Contiene un enlace a metadatos externos	<mdRef>
			Contiene los metadatos internamente	<mdWrap>
Metadatos Administrativos (Administrative Metadata Section)	**<amdSec>**	En esta sección se deben incluir los metadatos PREMIS, dentro de la estructura de los metadatos administrativos METS.	Metadatos técnicos	<techMD>
			Metadatos sobre derechos de propiedad intelectual	<rightsMD>
			Metadatos sobre la procedencia digital	<digiprovMD>
Sección Archivo (File Section)	**<fileSec>**	Contiene los documentos a preservar en el ADiUCR. Se incluye la codificación del documento en Base64.	Reúne todos los archivos que conforman una misma versión electrónica del objeto digital.	<fileGrp>
				<FContent>
				<FLocat>
Mapa Estructural (Structural Map Section)	**<structMap>**	Se incluirán los metadatos que permitan recuperar el Cuadro de Clasificación Documental.	Estructura jerárquica para navegar a través del objeto digital	

Fuente: Elaboración propia a partir de Library of Congress, 2016.

a) Sección de encabezado: Cabecera METS (*METS Header*)

En el caso de la Cabecera METS, contendrá aquellos metadatos sobre el propio documento METS. Para ambos casos, tanto para el caso del SiGeDI y de la colección fotográfica de la UPDRA, estudiados en esta investigación, se utilizarán los siguientes metadatos:

- Fecha de creación del documento METS
- Fecha de última modificación
- Estado
- Agentes

Tabla 30. *Elementos de la Cabecera METS.*

Elemento METS	Atributos	Observaciones
<metsHdr>	CREATEDATE	Fecha y hora en que se creó el documento METS
	RECORDSTATUS	Estado del documento METS. Ej: “COMPLETO”
<agent>	ROLE	Toma sus valores de un vocabulario controlado[2]. Ej. “ARCHIVISTA”, “CREADOR”, “CUSTODIO”, “EDITOR”, “OTRO”
	TYPE	Toma sus valores de un vocabulario controlado. Ej. "INDIVIDUAL," "ORGANIZACIÓN" y "OTRO"

Fuente: Elaboración propia a partir de Library of Congress, 2016.

b) Metadatos Descriptivos (*Descriptive Metadata Section*)

Para lograr la conservación adecuada de la información y su respectivo acceso y uso, es necesario la utilización de normas archivísticas que describen el contexto y el contenido de los documentos.

Así, es requerida la descripción del fondo y las series documentales y piezas documentales que lo conforman. Dicha descripción multinivel es planteada mediante la Norma ISAD (G), (elaborada por Consejo Internacional de Archivos), con la cual se busca “representar el contexto y la estructura jerárquica del fondo y las partes que lo integran” (ICA, 2000, p.19).

[2] El vocabulario controlado debe crearse específicamente para el ADiUCR

Con esta descripción se lograrán establecer relaciones entre distintos documentos conservados en el Archivo Digital, ya sea dentro de una misma serie documental o entre distintas series. Esto mejorará el acceso y el uso de la información por parte de los usuarios y facilitará la gestión de los trámites universitarios.

Además, la norma ISAAR-CPF, se utiliza para desarrollar los "registros de autoridad de archivos que proporcionan descripciones de entidades (instituciones, personas y familias) asociadas a la producción y a la gestión de archivos" (ICA, 2004, p.8).

Ambas normas se complementan, ya que permiten describir tanto la información en diferentes niveles, como a los productores de la propia información, con lo cual se puede asegurar la conservación de su contexto de creación y facilitar su preservación, acceso y uso. Estas normas han sido utilizadas para la creación de instrumentos tradicionales de descripción archivística como guías, inventarios, catálogos, entre otros.

Para la implementación del ADiUCR, se deberán convertir los campos descriptivos establecidos en las normas ISAD (G) y la ISAAR-CPF, al ambiente tecnológico, a través del uso de los esquemas de metadatos EAD (*Encoded Archival Description*) y EAC (*Encoded Archival Context*) respectivamente, los cuales consisten en esquemas XML de descripción archivística codificada, con metadatos que sirven como equivalencias (*crosswalks*) entre ambos.

Para capturar los metadatos para la transferencia de información digital, se requiere establecer las equivalencias o *crosswalks* entre los términos que plantean cada una de las anteriores normas.

Equivalencias de la Norma ISAD (G) a EAD:

A continuación, mediante la Tabla 31, se plantean la equivalencia de metadatos del SiGeDI, ISAD (G) y EAD. Para utilizaron los metadatos que fueron expuestos en la sección 3.3.1 Sistema de Gestión de Documentos Institucional, de esta investigación.

Mediante estas equivalencias, se plantea la necesidad de que al realizar la transferencia de documentos al ADiUCR, se puedan capturar todos los metadatos descriptivos que se generan actualmente en el SiGeDI.

Tabla 31. *Equivalencias de la Norma ISAD (G) a EAD para el SiGeDI.*

SiGeDI	ISAD (G)	EAD	Características del dato
Identificador único	3.1.2. Título	<unittitle>	tipodocumental-oficina-número consecutivo-año Ejemplo: Circular-AUROL-5-2023
Fecha de creación	3.1.3. Fecha del documento	<unitdate>	AAAA-MM-DD/HH:MM:SS
Remitentes	3.2.1. Nombre(s) del productor(es)	<origination>	Nombre completo del remitente (unidad administrativa o académica).
Asunto	3.3.1. Alcance y contenido	<scopecontent>	Se suministrará la información que se agrega al campo “asunto” al crear el documento en el SiGeDI.
Documentos relacionados	3.5.3 Unidades de descripción relacionadas	<relatedmaterial>	Corresponde a los documentos indicados en el campo "Documentos relacionados”.
Archivos adjuntos	3.5.3 Unidades de descripción relacionadas	<separatedmaterial>	Corresponde a los documentos indicados en el campo “Archivos adjuntos".
Destinatarios	No aplica	<relations>	Corresponde al nombre de la persona (s) a quienes se remite el documento.
Bitácora del documento	No aplica	<odd>	Corresponde al texto del campo “Bitácora del documento".

Fuente: Elaboración propia a partir de ICA (2000), Library of Congress. (s.f.-C) y SAA (2019).

En el caso de la Colección Fotográfica de la UPDRA, el inventario fue desarrollado con base en la norma ISAD (G), por lo que también resulta factible realizar la equivalencia de los campos descriptivos de dicho inventario al esquema EAD, como se muestra a continuación:

Tabla 32. *Equivalencias de la Norma ISAD (G) a EAD para la Colección Fotográfica de la UPDRA.*

ISAD (G)	EAD	Características del dato
3.1.1. Código de referencia	<unitid> con countrycode y repositorycode	CRC-UCR-AUROL-Fototeca-sigladelaunidad-númeroimagen Ejemplo: CRC-UCR-AUROL-Fototeca-UPDRA-0002
3.1.2. Título de la fotografía	<unittitle>	consecutivoimagen_Título de la fotografía Ejemplo: 1_Campeonato de Judo
3.1.3. Fecha de creación de la fotografía	<unitdate> con atributo @datechar	AAAA-MM-DD/HH:MM:SS
3.1.4. Nivel de descripción	<archdesc> y <c> como atributo de nivel	Unidad documental simple
3.1.5. Volumen y soporte del documento	<physdescstructuredtype>	Se debe recopilar la información de cada campo descriptivo
3.2.1. Nombre del fotógrafo	<origination>	apellido1-apellido2_nombre
3.2.3. Historia archivística (Procedencia)	<custodhist>	Dato de procedencia de las fotografías, en este caso se transfirieron desde la UPDRA
3.2.4. Forma de ingreso	<acqinfo>	Transferencia
3.3.1. Contenido	<scopecontent> <p>	Incluir el texto del campo descriptivo correspondiente
3.3.2. Evaluación documental	<appraisal> Según el Informe de valoración CUSED-TPC-2018	Conservación permanente
3.4.1. Condiciones de acceso	<accessrestrict>	Acceso libre

ISAD (G)	EAD	Características del dato
3.4.2. Condiciones de reproducción	<userestrict>	Ejemplo: Reproducción libre
3.4.4. Características físicas y requisitos técnicos (Estado de conservación)	<phystech>	Ejemplo: Bueno/malo/regular
3.4.5. Instrumento de descripción	<otherfindaid>	Inventario de la colección fotográfica de la UPDRA
3.6.1. Notas	<odd><note> <p>	Incluir el texto del campo descriptivo correspondiente
3.7.1. Notas del archivista	<processinfo> <p>	Incluir el texto del campo descriptivo correspondiente
3.7.2. Reglas o normas	<descrules> <p>	Incluir el texto del campo descriptivo correspondiente
3.7.3. Fechas y estado de la descripción	<processinfo> <p> <date>	Incluir el texto del campo descriptivo correspondiente y AAAA-MM-DD

Fuente: Elaboración propia a partir de ICA (2000), Library of Congress. (s.f.-C) y SAA (2019).

Equivalencias de la Norma ISAAR-CPF a EAC:

Para conocer el contexto en el que se crea la información, es necesario establecer las relaciones entre los productores y su entorno, incluidas otras entidades y sus documentos. De esta manera, es posible mejorar los procesos de preservación y uso de dicha información.

Al respecto, la CUSED, ha creado el *Procedimiento para la Identificación Archivística en la Universidad de Costa Rica*, que contiene el "Anexo 1. Identificación de la Unidad Productora", mediante el cual el AUROL realiza los registros de autoridad de las instancias universitarias relacionadas con la producción de los documentos, como requisito para ingresar al SiGeDI.

Esta herramienta de identificación de las unidades productoras, fue desarrollada con base en la norma ISAAR-CPF, por lo cual, a continuación se proponen un conjunto de metadatos

equivalentes entre dicha norma y el esquema EAC, para establecer puntos de acceso que deben ser recuperados para transferir la información al ADiUCR (Tabla 33):

Tabla 33. *Equivalencias de la Norma ISAAR-CPF a EAC para el ADiUCR.*

Identificación unidad productora	**ISAAR-CPF**	**EAC**	**Características del dato**
No incluido en el anexo	5.1.1 Tipo de entidad	<entityType @value> <otherEntityType>	Institución Unidad administrativa, Unidad académica, Unidad de Investigación
Nombre oficial de la unidad productora	5.1.2. Forma(s) autorizada(s) del nombre	<nameEntry @status="authorized">	Nombre oficial de la unidad productora y entre paréntesis sus iniciales, de acuerdo con la Lista Normalizada de Nombres y Siglas, establecido por el Archivo Universitario. Ejemplo: Oficina de Recursos Humanos (ORH).
Fechas de creación	5.2.1 Fechas de existencia	<existDates>	AAAA-MM-DD ó AAAA
Historia administrativa	5.2.2 Historia	<biogHist>	Datos sobre el origen y evolución orgánica, jurídica y funcional de la unidad, de forma cronológica.
Estatus jurídico	5.2.4 Estatuto jurídico	<legalStatuses>	Registrar la naturaleza jurídica de la unidad de acuerdo con lo establecido en la normativa universitaria. Ejemplos: Unidad Académica (ver Estatuto Orgánico, artículo 97).

Identificación unidad productora	ISAAR-CPF	EAC	Características del dato
Dependencia jerárquica	5.3.1 Nombre(s)/Identificadores de las instituciones, personas o familias relacionadas 5.3.1 Names of related corporate bodies, persons or families 5.3.2 Naturaleza de la relación	<targetEntity> <part> <relationType>	Depende de: Ejemplo: Vicerrectoría de Administración: depende de Rectoría. Dependen de la unidad: Ejemplo: Vicerrectoría de Administración: dependen de ella Oficina de Administración Financiera. Oficina de Recursos Humanos.
Normativa	5.2.6 Atribución (es) / Fuente(s) legal (es)	<mandates>	Normativa relacionada con la naturaleza propia de cada unidad productora. En el caso de la normativa de carácter general, especificar los artículos relacionados con la unidad productora.
Funciones	5.2.5 Funciones, ocupaciones y actividades	<functions> y <occupations>	Funciones que realiza la unidad según la normativa vigente.
Estructura interna	5.2.7 Estructura(s) interna(s)/Genealogía	<structureOrGenealogy>	Áreas que conforman la estructura interna de la unidad productora.
No incluido en el anexo	5.4.1 Identificador del registro de autoridad	<recordId>	CRC-UCR-AUROL-siglaunidad-RA-consecutivo Ejemplo: CRC-UCR-AUROL-ORH-RA-1

Identificación unidad productora	ISAAR-CPF	EAC	Características del dato
Observaciones	*No incluido en la norma*	<descriptiveNote> <p>	Cualquier información que se considere necesaria y que no está mencionada en los puntos anteriores.

Fuente: Elaboración propia a partir de ICA (2004), SAA (2022), SAA (s.f) y CUSED (2018-a).

c) Metadatos Administrativos (*Administrative Metadata Section*)

En la sección de metadatos administrativos <amdSec> del esquema METS, se incluirán los metadatos de preservación digital planteados en el diccionario PREMIS, para el ADiUCR.

Cabe destacar que la distribución de los elementos del estándar METS y del diccionario PREMIS tienen correspondencia en algunos puntos, pero también hay diferencias (Caplan, P., 2009, 17). Por lo tanto, para incluir PREMIS en METS se pueden distribuir los elementos de la siguiente manera (Library of Congress, 2017, p.2):

1. Elemento PREMIS: **Objeto** en Elemento METS: **techMD**
2. Elemento PREMIS: **Derechos** en Elemento METS: **rightsMD**
3. Elemento PREMIS: **Evento** en Elemento METS: **digiprovMD**
4. Elemento PREMIS: **Agente** en Elemento METS: **digiprovMD** (si se refiere a un evento) o **rightsMD** (si se refiere a un derecho).

Por consiguiente, a continuación se presentan las unidades semánticas PREMIS que deben ser recuperados para el ADiUCR, dentro del esquema METS (Tabla 34):

Tabla 34. *Unidades semánticas PREMIS en la Sección Administrativa del estándar METS para el ADiUCR.*

Elemento METS	Unidad semántica PREMIS (O / NO, R / NR)*	Sub unidades semánticas PREMIS (O / NO, R / NR)*
1. techMD (Objeto PREMIS)	1.1 objectIdentifier (O, R)	1.1.1 objectIdentifierType (O, NR) 1.1.2 objectIdentifierValue (O, NR)
	1.2 objectCategory (O, NR)	No aplica

Elemento METS	Unidad semántica PREMIS (O / NO, R / NR)*	Sub unidades semánticas PREMIS (O / NO, R / NR)*
	1.4 significantProperties (NO, R)	1.4.1 significantPropertiesType (NO, NR) 1.4.2 significantPropertiesValue (NO, NR)
	1.5 objectCharacteristics (O, R)	1.5.2 fixity (NO, R) 1.5.3 size (NO, NR) 1.5.4 format (O, R) 1.5.7 objectCharacteristicsExtension (NO, R)
	1.7 storage (NO, R)	1.7.1 contentLocation (NO, NR) 1.7.2 storageMedium (NO, NR)
	1.13 relationship	1.13.1 relationshipType (NO, R) 1.13.2 relationshipSubType (O, RN) 1.13.3 relatedObjectIdentifier (O, R)
2. rightsMD (Derecho PREMIS)	4.1 rightsStatement (NO, R)	4.1.1 rightsStatementIdentifier (O, NR) 4.1.2 rightsBasis (O, NR)
	4.2 rightsExtension (NO, R)	No aplica
3. digiprovMD (Evento PREMIS)	2.1 eventIdentifier (O, NR)	2.1.1 eventIdentifierType (O, NR) 2.1.2 eventIdentifierValue (O, NR)
	2.2 eventType (O, NR)	No aplica
	2.3 eventDateTime (O, NR)	No aplica
	2.6 linkingAgentIdentifier (NO, R)	2.6.1 linkingAgentIdentifierType (O, NR) 2.6.2 linkingAgentIdentifierValue (O, NR)
	2.7 linkingObjectIdentifier (NO, R)	2.7.1 linkingObjectIdentifierType (O, NR) 2.7.2 linkingObjectIdentifierValue (O, NR)
4. digiprovMD / rightsMD (Agente PREMIS)	3.1 agentIdentifier (O, R)	3.1.1 agentIdentifierType (O, NR) 3.1.2 agentIdentifierValue (O, NR)
	3.2 agentName (NO, R)	No aplica
	3.3 agentType (NO, NR)	No aplica
	3.4 agentVersion (NO, NR)	No aplica

*(O-Obligatoria / NO-No Obligatoria, R-Repetible, NR-No repetible).

Fuente: elaboración propia a partir de PREMIS Editorial Committee, 2015.

En el caso específico de las imágenes, ya sean digitalizadas mediante escáneres, o bien las fotografías que han nacido en soporte digital, es decir, las captadas mediante cámaras digitales, teléfonos celulares y otros dispositivos, se deben conservar los metadatos correspondientes a sus especificaciones técnicas.

Estos metadatos serán incluidos dentro de la estructura METS del paquete archivístico en XML, en la sección <amdsec> <techMD>, mediante el estándar MIX. Se puede utilizar un atributo ID con el valor del documento a preservar, para hacer referencia a sus características técnicas desde la <fileSec>, utilizando un atributo ADMIN y de esta manera enlazar los metadatos técnicos con el documento correspondiente (Digital Library Federation, 2010, p.23).

Por lo tanto, a continuación se presentan los metadatos técnicos para las imágenes fijas digitales según la norma ANSI/NISO Z39.87-2006 (R2017) (Tabla 35). Los metadatos que se contemplan mediante el diccionario PREMIS cómo 1.1 objectIdentifier, 1.1.1 objectIdentifierType, 1.1.2 objectIdentifierValue, 1.5 objectCharacteristics, 1.5.3 size y 1.5.4 format, no se incluirán dentro de los metadatos ANSI/NISO, para evitar la duplicidad de información.

Además, los metadatos ANSI/NISO, no se establecerán como obligatorias, sino que serán opcionales, para evitar que las fotografías digitales sean rechazadas por el repositorio del Archivo Digital, en caso de no disponer de algún elemento (Calvo-López y Otárola-Sáenz, 2020, p.219-220).

Tabla 35. *Metadatos técnicos para imágenes fijas digitales de la ANSI/NISO Z39.87-2006 (R2017), en la Sección Administrativa del estándar METS para el ADiUCR.*

Unidad semántica ANSI/NISO	Subunidad semántica ANSI/NISO
6.6 Compression	6.6.1 compressionScheme
6.7 Fixity	6.7.1 messageDigestAlgorithm 6.7.2 messageDigest
7.1 BasicImageCharacteristics	7.1.1 imageWidth 7.1.2 imageHeight 7.1.3 PhotometricInterpretation 7.1.3.1 colorSpace
8.1 SourceInformation	8.1.1 sourceType

Unidad semántica ANSI/NISO	Subunidad semántica ANSI/NISO
	8.1.3 SourceSize
8.2 GeneralCaptureInformation	8.2.1 dateTimeCreated
8.3 ScannerCapture	8.3.1 scannerManufacturer 8.3.2 ScannerModel 8.3.5 ScanningSystemSoftware
8.4 DigitalCameraCapture	8.4.1 digitalCameraManufacturer 8.4.2 DigitalCameraModel 8.4.3 cameraSensor 8.4.4 CameraCaptureSettings 8.5 orientation
9.1 SpatialMetrics	9.1 SpatialMetrics 9.1.1 samplingFrequencyPlane 9.1.2 samplingFrequencyUnit
9.2 ImageColorEncoding	9.2.1 BitsPerSample 9.2.2 samplesPerPixel 9.2.4 Colormap 9.2.7 WhitePoint 9.2.8 PrimaryChromaticities
10.1 ImageProcessing	10.1.1 dateTimeProcessed 10.1.2 sourceData 10.1.5 ProcessingSoftware 10.1.6 processingActions

Fuente: Elaboración propia a partir de NISO, 2017.

Finalmente, los metadatos Exif para imágenes capturadas mediante cámaras digitales y otros dispositivos, registran detalles técnicos asociados con la fotografía digital. Para ello, emplean codificaciones de imagen basadas en formatos de imagen existentes y los archivos resultantes pueden ser leídos por muchas aplicaciones de software de imágenes (Library of Congress, 2023).

Los datos Exif se encuentran incrustados dentro de las propias imágenes y para conservarlos, el ADiUCR se debe asegurar que no existen modificaciones ni migraciones de formato en las imágenes al momento de ser transferidas, ya que se corre el riesgo de perder dichos datos.

d) Sección Archivo (*File Section*)

La sección <filesec> resulta indispensable dentro del estándar METS, ya que en esta se define el objeto digital que será transferido y almacenado en el ADiUCR.

Por ello, dentro del elemento <fileGrp>, se definirá principalmente un elemento <FContent> que contendrá el documento, codificado en Base64, de manera que el documento pueda ser incluido dentro del propio esquema METS. El incluir los documentos dentro de la misma estructura METS sirve para "intercambiar objetos digitales entre repositorios o para archivar objetos digitales" (Library of Congress, 2016).

En el caso de que el paquete archivístico que contendrá al documento exceda el tamaño máximo soportado por el fichero XML, se definirá un elemento <FLocat>, dentro del elemento <fileGrp>, para designar una ubicación de fichero única, por medio de una URL u otro elemento similar.

e) Mapa Estructural (*Structural Map Section*)

Mediante el elemento <structMap>, se determinará la clasificación documental que tendrán los documentos que se transfieran y almacenen al ADiUCR.

Es importante recalcar que el paquete archivístico representado mediante un documento XML, no incluirá como tal el Cuadro de Clasificación, sino la información que permita ubicar ese fichero dentro del Cuadro, según se haya definido por el AUROL. En el apartado 3.3.3. Organización de los documentos en el ADiUCR de la presente investigación, se muestran los macroprocesos y procesos universitarios. Sin embargo, se requiere que el ADiUCR pueda recuperar los metadatos de clasificación hasta el nivel de serie documental, ya que es a este nivel en el que se asignan los plazos de conservación de los documentos que componen cada expediente.

3.3.5. Acceso y ciberseguridad

Si bien el SiGeDI, por su reciente creación y la intervención de archivistas e informáticos en su implementación, cuenta con controles de acceso y seguridad, no todos los documentos de archivo (físicos, digitales y digitalizados) tienen las mismas condiciones, siendo que pueden estar

expuestos a riesgos y amenazas; los cuáles, tal como lo indican Castillo-Solano y Umaña-Alpízar (2018, p.273):

> (...) van desde la falsificación, modificación y pérdida, hasta el secuestro de la información por causa de infecciones debidas a software malintencionado como el "ransomware". Adicionalmente, carecen de algún tratamiento que de garantía de autenticidad o integridad; o que prevenga la obsolescencia tecnológica del soporte o del formato, por lo que no se puede asegurar su disponibilidad futura, cuando se necesite, ni cuenta con un mecanismo para hacer llegar la información al público interesado.

Para minimizar estos riesgos, en los apartados 3.2.2.6. Acceso y 3.2.3.2. Arquitectura tecnológica, se tratan los aspectos básicos de acceso y seguridad para el ADiUR. Sin embargo, a continuación se detallan algunos otros temas específicos en ambas materias.

En primer lugar, respecto al acceso, se determina que el ADiUCR deberá contar con aspectos como lo son (3.2.2.6. Acceso):

- Interfaces de consulta
- Control de acceso
- Atención de solicitudes
- Asistencia a los usuarios
- Búsquedas por contenido y metadatos
- Generación de DIP
- Entrega de respuestas
- Entre otras

La Universidad de Costa Rica, mediante el Centro de Informática, cuenta con normativa relacionada con el acceso a la información, la cual deberá ser tomada en consideración para el desarrollo de la plataforma tecnológicas del ADiUCR, como por ejemplo el documento "CI-URS-L01-2016 Lineamientos técnicos para cuentas de acceso", lineamientos mediante los que pretende "administrar adecuadamente las cuentas de acceso en los sistemas de la Universidad de Costa Rica, verificando la identidad del usuario y permitiendo la utilización personalizada de recursos y privilegios" (Centro de Informática de la UCR, 2016, p.1).

Es importante resaltar respecto al acceso, que este debe garantizarse a lo largo del tiempo que sea requerido, mientras que se protegen las características de autenticidad, integridad y propiedades significativas de los documentos y de la información que se gestiona en el ADiUCR.

En segundo lugar, dentro de la arquitectura tecnológica se definen aspectos de seguridad básicos, como por ejemplo (3.2.3.2. Arquitectura tecnológica):

- Protección ante amenazas
- Identificación/autenticación de identidades
- Controles de acceso y confidencialidad
- Integridad y confidencialidad de datos

Aunado a esto, la UCR puede considerar buenas prácticas de seguridad comprendidas en la familia de normas ISO/IEC 27000 Gestión de la seguridad de la información, como por ejemplo (ISO, s.f.):

- ISO/IEC 27000:2018 *Information technology — Security techniques — Information security management systems — Overview and vocabulary*.
- ISO/IEC 27001:2022 *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*.
- ISO/IEC 27002:2022 *Information security, cybersecurity and privacy protection — Information security controls*.

Como se observa en estas normas ISO, la ciberseguridad es un tema no solo de actualidad, sino que es de vital importancia para un Archivo Digital, puesto que como es conocido, el ADiUCR trabajará con plataformas o aplicaciones informáticas para la preservación de los objetos digitales, siendo que éstas requieren de protección especial.

La ciberseguridad se define como “la práctica de proteger sistemas críticos e información confidencial de ataques digitales, que involucran tecnología, personas y procesos” (MICITT, 2023, p.37).

Gamboa-Suárez (2020, p.1), plantea que para lograr una buena Ciberseguridad “no solo se debe basar en la prevención de ataques, sino también detección y corrección de los mismos, reduciendo los riesgos de exposición de la información, brindando confianza a los usuarios”. De

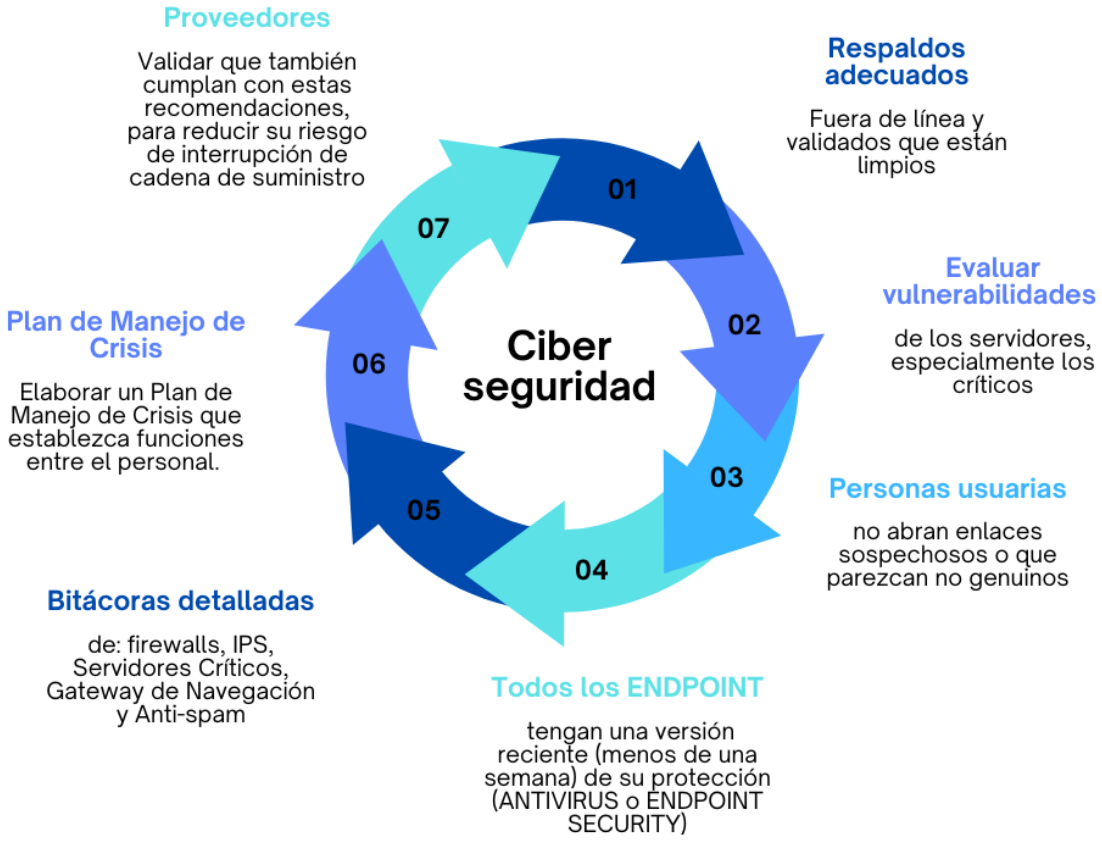
esta manera, este autor propone las siguientes categorías comunes para la ciberseguridad (figura 45):

Figura 45. *Categorías de Seguridad Informática o Ciberseguridad.*

Fuente: Elaboración propia a partir de Gamboa-Suárez, 2020, p.1-2.

Algunas buenas prácticas, con respecto a la ciberseguridad, planteadas de manera general se observan en la figura 46.

Figura 46. *Buenas prácticas de ciberseguridad ante posibles ciberataques.*



Fuente: Elaboración propia a partir de Castro-Obando, 2022, p.77.

Por su parte la UCR, desde el año 2015 implementó las "Directrices de Seguridad de la Información de la Universidad de Costa Rica". En este documento se emiten las pautas básicas para proteger la información institucional. El ADiUCR, al preservar información que pertenece a la Universidad, debe ajustarse a lo dispuesto en las directrices.

Además, el Centro de Informática de la UCR, enfoca una campaña de ciberseguridad institucional basada en la concientización y capacitación de las personas para enfrentarse a las amenazas que representa el mundo digital, para la cual ofrece material informativo sobre distintos temas. En la Tabla 36, se presentan algunos ejemplos recomendaciones que se encuentran en dichos materiales.

Tabla 36. *Temas tratados en el material informativo sobre ciberseguridad del Centro de Informática de la UCR.*

Tema	Descripción	Acciones recomendadas
Análisis de riesgo	Por medio del análisis de riesgos, una organización conoce a qué está expuesta, le permite identificar los riesgos que le podrían impedir lograr sus objetivos de negocio	Se pueden utilizar diversas soluciones como son: Firewalls, IDS, IPS, VPN, entre otros.
Buenas prácticas en entornos de tecnología de información	Medidas organizativas y de cumplimiento legal	- Identificar activos y definir responsabilidades de protección. - Crear procedimientos y responsabilidades. - Tener sistemas informáticos actualizados y una correcta gestión de parches de seguridad. - Gestión y control de sistemas antivirus y cortafuego (firewall). - Copias de seguridad. - Gestión del monitoreo. - Gestión de incidentes. - Recuperación y continuidad de servicios ante desastre.
Continuidad de servicios	El Plan de Continuidad de Servicios se encarga de impedir que una interrupción imprevista y grave de servicios, tenga grandes consecuencias para el negocio o la institución.	- ¿Qué? Definir las áreas de la organización que serán críticas. - ¿Quién?: Cuáles personas se tendrán que movilizar y en qué orden. - ¿Cuándo?: Cuáles ventanas de interrupción son tolerables y en cuánto tiempo hay que volver a la normalidad. - ¿Cómo?: Qué hacer para mitigar la contingencia, entrar en la fase de recuperación y volver a la normalidad. - ¿Dónde?: A qué lugares tendremos que acudir para poder cumplir con el plan.
Copias de seguridad y respaldos	Tienen el fin de evitar la pérdida de la información y así poder recuperarla en caso de pérdida, daño o robo.	- Elegir la información más importante o crítica. - Elegir el dispositivo de almacenamiento para las copias de seguridad. - Establecer la periodicidad con la que se debe realizar la copia de seguridad. - Dependiendo de la importancia del respaldo, el espacio físico donde se guarde éste, debe estar protegido. - Realizar copias de seguridad a dispositivos móviles como teléfonos inteligentes y tabletas que puedan almacenar información sensible e importante para la institución

Tema	Descripción	Acciones recomendadas
Dispositivos portátiles	Se deben proteger ya que su pérdida representa un impacto económico, además de poner en riesgo la información almacenada.	- Se debe llevar en ellos la información cifrada. - Proteger el teléfono celular por medio de una contraseña, un patrón numérico o de desbloqueo. - Configurar las aplicaciones para que efectúen respaldos de forma automática en la nube. - Se recomienda el uso de redes inalámbricas conocidas. - Realizar copias de seguridad periódicamente. - Instalar y actualizar anti-virus y anti-spyware
Encriptación de la información	La encriptación utiliza esquemas de cifrado con clave generada por un algoritmo. Esta clave debe ser suficientemente robusta para evitar recuperar la información por terceros no autorizados.	- Usar las claves de cifrado de la mayor longitud posible. - Cifrado en capas. - Almacenar claves de cifrado de forma segura.
Espacios de trabajo	Se deben ejecutar medidas de seguridad con respecto a la información electrónica y en papel, todo esto orientado a evitar el extravío, pérdida, fuga y/o robo de información que se podría dar sin intención del personal por desconocimiento o por personas malintencionadas	- Prevenir fallas en la seguridad de la información. - Evitar la pérdida de la documentación. - Destrucción adecuada de la información. - Almacenamiento de la información digital y física. - Uso de contraseñas seguras. - Política de escritorios limpios.
Protección ante el secuestro de información ransomware	Ransomware es un software malicioso que infecta un equipo y lo bloquea desde una ubicación remota y encripta los archivos y datos ubicados en equipos como computadoras, servidores, medios externos de almacenamiento, quitándole el control al usuario.	- Revisar detenidamente el dominio del correo electrónico del remitente. - Corroborar el nombre de la empresa o institución de la que proviene el correo. - Leer detenidamente el cuerpo del correo. - No se deje presionar. - Cuidado con enlaces falsos. - Cuando utilice enlaces contenidos en el correo, asegúrese que son sitios calificados como seguros. - No descargue archivos si no está seguro de su contenido, más si son archivos ejecutables.

Tema	Descripción	Acciones recomendadas
Tratamiento de la información digital y física	Recomendaciones generales.	- Instalar y mantener actualizado un anti-virus y anti-spyware. - Utilizar redes inalámbricas conocidas, como las del trabajo y hogar. - Instalar periódicamente parches de seguridad y actualizaciones de los sistemas operativos y aplicaciones. - Crear contraseñas seguras y robustas utilizando mayúsculas, minúsculas, números y caracteres especiales ($&#%). - Evitar repetir contraseñas utilizadas anteriormente y modificarlas periódicamente. - Evitar contestar y reenviar correos aparentemente maliciosos. - Controlar el acceso físico a equipos y componentes. - Evitar hacer clic en las ventanas emergentes y en anuncios. - Procurar usar perfiles de usuario para limitar la posibilidad de instalar programas no autorizados o de dudosa procedencia. - Desarrollar conciencia y cultura sobre los principios básicos de seguridad. - Realizar de forma periódica copias o respaldos de la información más relevante de su trabajo.
La información	Recomendaciones generales.	- Establecer acuerdos de confidencialidad con personas que manejen información institucional sensible. - Usar lineamientos de resguardo y protección de la información. - Aplicar medidas para evitar accesos no autorizados y detectar intentos de acceso a la información. - Clasificar y cifrar la información confidencial. - Hacer copias de seguridad de la información importante, confidencial y sensible. - Comprobar que las copias de seguridad funcionen correctamente.
Seguridad de sitios web	Proteger sitios web del acceso, uso, modificación, destrucción o interrupción, no autorizados.	- Utilizar sistemas de captcha. - Actualizar las plataformas y los gestores de contenidos (CMS) como Drupal, Wordpress, Joomla, entre otros. - Informar a los visitantes de que el sitio web es seguro.

Fuente: elaboración propia a partir de: Centro de Informática de la UCR, s.f.-d.

3.3.6. Nuevos enfoques para la difusión de la información preservada en el ADiUCR

- **Comunicación multidireccional del ADiUCR**

Uno de los fines de contar con un Archivo Digital, es permitir el acceso oportuno a la información y el conocimiento institucional. Para esto, además de brindar los medios para ingresar al repositorio, es necesario transmitir y difundir el acervo documental, para que el mismo pueda ser utilizado y aprovechado por las personas.

Sin embargo, se requiere que el proceso técnico archivístico tradicional de la difusión evolucione hacia un proceso de comunicación multidireccional y de transparencia activa, tanto de parte de la Universidad como organización, y del ADiUCR como parte del Sistema de Archivos de la Universidad de Costa Rica.

Una comunicación multidireccional permite un diálogo compartido, abierto y flexible que promueve "la participación activa y reflexiva de las audiencias y su colaboración mutua" (Hermann-Acosta, 2020). Este tipo de comunicación permite la generación de interrelaciones en la cuáles las partes interesadas pueden tener un rol más activo y participativo "en los procesos de construcción colectiva y colaborativa de los datos e información" (Hermann-Acosta, 2020).

La comunicación multidireccional puede llevarse a cabo en tiempo real, lo que para el ADiUCR, significaría una interacción inmediata con sus audiencias. Para esto, debe contar con interfaces de consulta con la capacidad de ofrecer a los usuarios acceso a la información que desean consultar, lo cual refuerza la necesidad de implementar la transparencia activa.

Así mismo, se requiere que el Archivo Digital cuente con los canales necesarios para brindar un espacio para recibir retroalimentación de parte de las audiencias. En el apartado *3.2.2.6. Acceso*, en la funciones de Coordinación de Actividades de Acceso y Entrega de Respuesta, se determinan requisitos como: interfaces de consulta, atención de solicitudes, ofrecer asistencia a los usuarios y permitir búsquedas.

Por lo tanto, el ADiUCR debería contar con medios que le permitan a los usuarios tener un acceso que interrelacione distintas fuentes de información. Para ello, la utilización de esquemas de metadatos es fundamental porque permitirán no solo conocer el contexto de un dato o documento, sino del conjunto de información almacenada en el Archivo Digital.

Los módulos de consulta también deberían ser capaces de interrelacionar distintas clases documentales (imágenes, audios, videos, páginas *web*, entre otros) para enriquecer la experiencia de las búsquedas, al tiempo que permita a los usuarios opinar y retroalimentar al ADiUCR sobre sus necesidades de información.

- **Metodología de la Interpretación**

Una nueva corriente que toma fuerza en el ámbito archivístico, y que ha sido probada y utilizada en otras áreas como la sociología y la antropología, es la de la Interpretación, principalmente el enfoque de la Interpretación del Patrimonio.

Debido a que los documentos con valor científico cultural se consideran parte del patrimonio documental, tanto de la UCR como del país, y son de interés para todos los ciudadanos costarricenses, el enfoque de la Interpretación podría ser aplicable para el caso del ADiUCR, ya que en él se preservarán a largo plazo este tipo de documentos con valor secundario.

Desde el punto de vista de la Interpretación, lograr que el patrimonio genere una conexión con la realidad de las personas, es fundamental para que pueda ser apropiado por ellas. De esta manera, la Interpretación del Patrimonio tiene la misión de transformar, gestionar y conservar el patrimonio material e inmaterial (figura 47):

Figura 47. *Misión de la Interpretación del Patrimonio.*

Fuente: Elaboración propia a partir de Rodríguez-Achútegui, 2023, p.20.

Para lograr esta misión, la metodología de la Interpretación cuenta con el modelo TORA, por medio del cual se indica que la Interpretación logra ser efectiva cuando tiene un tema, es organizada, es relevante y además es amena (Guerra-Rosado, 2017, p.2)

En la figura 48, a continuación se resume el modelo TORA:

Figura 48. *Modelo TORA en la metodología de la Interpretación.*

Fuente: elaboración propia a partir de Guerra-Rosado, 2017.

Si bien la información que se preservará en el ADiUCR, es producida por la ejecución de las funciones y muchas veces se desconoce su trascendencia para la construcción de la memoria y de la cultura, será trabajo de los archivistas y todo el personal a cargo de este archivo digital, lograr que el patrimonio que se resguarda sea colocado a disposición de las personas para ser aprovechado y disfrutado por ellas.

- **Herramientas para la difusión dinámica de contenidos**

Dos herramientas novedosas de las cuales puede hacer uso el AUROL y la CIADi, para promover la difusión y el acceso a los contenidos de manera dinámica desde el ADiUCR, son las redes sociales y el *storytelling*.

Las redes sociales, son una estructura que se compone por individuos y/u organizaciones, que se encuentran conectados por diversos objetivos, como por ejemplo amistad, negocios, intereses comunes, entre otros (Universitat Oberta de Catalunya, s.f.).

Por su parte, el *storytelling*, es una técnica o herramienta, por medio de la cual se cuenta una historia con un mensaje final que deja un aprendizaje o concepto (Universidad de Palermo, s.f.) y que además, permite generar un contenido emocional y dinámico con las audiencias (Hermann-Acosta, 2020).

Con la finalidad de causar un impacto en la audiencia del ADiUCR, estas dos herramientas proporcionan beneficios como (Tabla 37):

Tabla 37. *Beneficios del uso del storytelling y las redes sociales.*

Storytelling	Redes sociales
Permite conectar emocionalmente con la audiencia.	Son medios económicos que no requieren de un gran presupuesto para funcionar.
Tiene como finalidad dejar un aprendizaje.	Permiten alcanzar distintos tipos de públicos o audiencias.
Busca transformar la vida de las personas.	Permiten utilizar distintos formatos, como por ejemplo audio y video, además del textual.
Genera confianza en la audiencia y permite que la información sea recordable.	Abren otras posibilidades como las transmisiones en vivo.
Potencia el *engagement* con los usuarios.	Algunas plataformas permiten almacenar contenidos y reproducirlos la cantidad de veces que se requieran.
Promueve una comunicación multidireccional con la audiencia.	Posibilita conocer el número de personas que visualizan o interactúan con las publicaciones.
Permite informar mientras se cuentan historias, lo cual puede hacerse por medios electrónicos.	Potencializa el alcance de los contenidos.
Construye un vínculo entre el emisor y las audiencias.	Hace más amigable y homogéneo el contenido que se presenta a las audiencias.

Storytelling	Redes sociales
Logra mantener a las audiencias activas y participativas.	Logra la inmediatez en la transmisión de contenidos que se quieran difundir.

Fuente: elaboración propia a partir de Hermann-Acosta, 2020; Universidad de Palermo, s.f.; y Sánchez-Tamez, 2016.

Si bien, lo recomendable sería contar con la colaboración de expertos en el desarrollo, uso y expansión de las redes sociales, como por ejemplo un *Social Media Manager*; el SIRO (la CIADi) y SRO (persona encargada del ADiUCR), pueden capacitarse y entrenarse para lograr un desarrollo de estas herramientas, de manera que la difusión de los contenidos del acervo documental universitario llegue a muchas más personas.

Lo más importante a la hora de considerar la aplicación de alguna metodología o herramienta para la difusión de la información contenida en el ADiUCR, es cumplir con las expectativas y necesidades de los usuarios, al tiempo que se lograr tener una incidencia positiva en las audiencias para las cuáles se desarrollan los procesos que permiten un acceso ágil y eficiente de la información.

La innovación y la apertura de parte de los profesionales que trabajan con este tipo de patrimonio documental, son elementos fundamentales para cambiar la percepción y reputación de los Archivos como instituciones anticuadas y darle paso a una visión moderna y accesible como fuente de información relevante para la sociedad.

4. Conclusiones y recomendaciones

4.1. Conclusiones

1. La Universidad de Costa Rica, al contar con el Archivo Universitario Rafael Obregón Loria, el Centro de Informática y la Oficina Jurídica, ha podido ejecutar trabajos especializados en el campo de la Archivística, las TIC y el ámbito legal, respectivamente. Sin embargo, estas tres áreas del conocimiento han trabajado de manera aislada, el tema de la preservación digital, lo que ha demorado el desarrollo de un Archivo Digital en la institución.

   Es por ello que, por medio de iniciativas que se están llevando a cabo actualmente, como la conformación de la CIADi, se analiza la temática desde una visión interdisciplinaria, para incorporar la Preservación Digital Sistémica dentro de la planificación estratégica institucional, con lo cual se podrá crear normativa para asegurar la información digital a largo plazo, a través de la puesta en funcionamiento del Archivo Digital de la Universidad de Costa Rica (ADiUCR).

2. Para hacer frente al tema de la preservación digital, resultó fundamental realizar el análisis de la situación en la que se encuentra la Institución.

   Así, al aplicar la *Herramienta de autoevaluación de la continuidad digital,* como se muestra en el apartado *2.4. Evaluación de riesgos para la preservación digital de la información*, existe un conjunto de factores, que ponen en riesgo la preservación de la información a largo plazo, a causa del acelerado cambio tecnológico, que afecta directamente el uso y la preservación de la información digital.

   También, se denota que las instancias universitarias utilizan de forma extendida las TIC y que conocen la importancia de la información generada para la Institución. No obstante, se detectaron malas prácticas para la preservación de la información digital, como el almacenamiento no planificado en dispositivos portátiles y la nube, poniendo en peligro a la Institución.

   Y, al no existir lineamientos claros en cuanto a la preservación digital, cada instancia aborda de forma aislada esos riesgos tecnológicos, además que no se le ha dado la

prioridad que requiere el tema, para lograr resguardar la información, de forma segura, durante el tiempo en que se necesite.

Por lo tanto, al no existir un Archivo Digital con las características necesarias de preservación, actualmente la información institucional se encuentra bajo riesgos como la obsolescencia tecnológica y el inadecuado almacenamiento, lo cual dificulta su preservación y uso, en detrimento de la eficaz toma de decisiones y la seguridad jurídica de la Universidad.

3. Al considerar las implicaciones archivísticas, legales y tecnológicas que conlleva la Preservación Digital Sistémica, la Universidad de Costa Rica ha implementado acciones pertinentes con respecto a la necesidad de integrar un equipo interdisciplinario para abordar esta temática. De esta manera, la Rectoría creó la CIADi, la cual está conformada por profesionales en Archivística, Informática y Derecho, quienes en conjunto con la administración universitaria, trabajan en establecer las bases normativas y técnicas necesarias para la puesta en marcha del ADiUCR.

   Esta visión interdisciplinaria diversifica y valida las decisiones en materia de Preservación Digital, ya que permite abordar el tema de manera integral, para proteger adecuadamente los activos información institucional.

4. En esta investigación se presentó el modelo de Preservación Digital Sistémica para dos casos concretos: el SiGeDI y la Colección Fotográfica de la UPDRA.

   En ambos casos, para transferir la información hacia el ADiUCR, es necesario conocer cómo se organizan y describen los documentos; también los aspectos técnicos tanto de la información como del ambiente tecnológico en el que se encuentra almacenada, es decir, dentro o fuera de un sistema. Además, es necesario definir las series documentales, los formatos que se recibirán, los metadatos que deben ser recuperados, entre otros.

   Con base en estos casos, se concluye que los Protocolos de Transferencia, son esenciales para dejar claros los aspectos técnicos y legales, que implica realizar la transferencia de información hacia el ADiUCR y que estos varían significativamente si se trata de una transferencia desde sistemas informáticos o fuera de estos.

El desarrollo de Protocolos específicos, permite transferir al ADiUCR, la información desde cualquier sistema informático, así como la información no estructurada que se encuentra dispersa en la Institución, lo cual permite escalar el Modelo de Preservación Digital Sistémica, a toda la Universidad de Costa Rica.

5. En la Universidad de Costa Rica no se han elaborado ni aplicado de manera completa los instrumentos archivísticos necesarios que son indispensables para que la transferencia de información de manera normalizada, desde las instancias universitarias al ADiUCR. Entre estos instrumentos se encuentra el Cuadro de Clasificación por Procesos Institucional y las Tablas de Plazos de Conservación de cada instancia universitaria.

   Tampoco se ha normalizado la elaboración de las listas de remisión y los inventarios de los documentos, para que por medio de la descripción archivística, se pueda acceder oportunamente a la información preservada.

   Aspectos como la asignación de códigos únicos, la descripción detallada del documento de archivo e incluso el rescate de los datos Exif (para las fotografías e imágenes nacidas digitales), entre otros, forman parte de un proceso previo a la transferencia, para evitar incluir información desorganizada dentro del Archivo Digital.

6. Existe una amplia variedad de herramientas tecnológicas relacionadas con la preservación digital. Como se expuso en el apartado *2.5.1. Análisis de herramientas para la preservación digital*, se compararon algunas de esas herramientas, con el objetivo de determinar si cumplen con el modelo OAIS de la norma UNE-ISO 14721, que es la base teórica con la que se plantea la creación del ADiUCR en esta investigación.

   Si bien se realizó un análisis parcial de algunas de las herramientas tecnológicas de preservación digital disponibles en el mercado, corresponde a la CIADi y al ADiUCR realizar un estudio completo de la herramienta tecnológica que se implementará, donde se consideren los requerimientos archivísticos y tecnológicos desde una perspectiva global, incluyendo aspectos de tipo presupuestario, ya que el Archivo Digital debe ser un proyecto permanente en la Universidad y se le debe dar mantenimiento y soporte a largo plazo.

7. La información gestionada en medios digitales tiene un alto nivel de fragilidad en cuanto a su conservación, donde resulta fundamental aplicar la ciberseguridad como un eje transversal para llevar a cabo la preservación digital.

   Además, este tipo de información depende de plataformas o aplicaciones tecnológicas, que requieren de acciones de detección y protección especial ante la exposición a ataques informáticos, para mantener la confianza de que no existe pérdida o alteración en la información preservada.

   En esta línea, la Universidad de Costa Rica ya cuenta con las Directrices de Seguridad de la Información y ha ejecutado una campaña de ciberseguridad institucional para afrontar estos retos.

4.2. Recomendaciones

1. La Universidad de Costa Rica debe aunar esfuerzos de las altas jerarquías con las instancias que desempeñan funciones técnicas, para que se puedan tomar decisiones que permitan abordar la preservación digital desde una visión interdisciplinaria.

   Para lograr estos cometidos, es necesario que se incluyan los planteamientos de Preservación Digital Sistémica desde la Política Institucional quinquenal, según se propone en el apartado *3.1. Política de Preservación.* Además, es necesario que se aprueben otros lineamientos específicos de preservación digital, para definir el marco de acción del ADiUCR, las funciones y responsabilidades de cada instancia involucrada y las estrategias para asegurar el acceso y usabilidad de la información digital a largo plazo.

2. Se recomienda que la Universidad planifique las acciones para conocer periódicamente la situación de la preservación digital, de manera que se puedan identificar riesgos y oportunidades de mejora para la toma de decisiones oportuna. En este sentido, es necesario que, además de las 14 Unidades Administrativas que se incluyeron en este proyecto, se amplíe el diagnóstico a otras unidades académicas y centros de investigación.

   También, se deben seguir haciendo esfuerzos para promover dentro de la Institución, la generación de conocimiento en materia de preservación digital, para crear una cultura

institucional que tienda hacia una gestión adecuada de los objetos digitales, desde que se producen. Este aspecto debe establecerse de manera formal por medio de la normativa que emana de las altas jerarquías, pero además debe ser un proceso de convencimiento, para todas las personas de la comunidad universitaria.

3. El ADiUCR debe estar integrado por personal formado en Archivística y en Informática, ya que se requiere de labores que conjuguen ambos campos del conocimiento.

   Por ello, se deben asegurar los recursos necesarios para la formación continua de las personas que conforman el ADiUCR. Esta formación deberá ser adquirida a partir de centros educativos nacionales e internacionales, capacitados en preservación digital. También se podrá obtener a partir de entes públicos o privados que brinden soluciones certificables en esta materia.

   La formación continua, se deberá planificar estratégicamente desde el ADiUCR, de acuerdo con las necesidades técnicas y tecnológicas que se vayan detectando, con el objetivo de abordar oportunamente los riesgos asociados con la obsolescencia tecnológica y la inadecuada gestión de la información institucional.

4. Los productores de la información, deben conocer los documentos, datos y otras evidencias, que se generen como parte de la ejecución de sus funciones. En este sentido, se deberán tener claros los aspectos de tipo archivístico como la clasificación por procesos, las series documentales, los plazos de conservación, entre otros. Además, comprender aspectos tecnológicos, como los distintos formatos en que se genera la información.

   De igual manera, deberán identificar los aspectos técnicos de los sistemas productores de la información, por ejemplo, saber si generan documentos por medio de ficheros o si se almacena la información en bases de datos.

   En todos los casos, deberá existir un trabajo colaborativo entre el ADiUCR y las instancias universitarias, para definir Protocolos de Transferencia que se adapten a los requerimientos específicos de Preservación Digital Sistémica, asegurando la Cadena de Custodia Ininterrumpida.

5. La Universidad de Costa Rica, por medio de las instancias correspondientes en materia archivística, como el AUROL, el SAU-CT y la CUSED, debe asegurar la correcta aplicación de los instrumentos que se desprenden de los procesos técnicos archivísticos; de manera que cuando los documentos y otras evidencias de información sean ingresados al ADiUCR, cumplan con el nivel de organización requerido.

   En este sentido, se deben completar instrumentos archivísticos que actualmente se encuentran en proceso de elaboración, tales como el Cuadro de Clasificación por Procesos, las Tablas de Plazos de Conservación y las Fichas de Identificación de las instancias universitarias.

6. Respecto a las herramientas tecnológicas para implementar el ADiUCR, se recomienda, con base en la normativa vigente y la tendencia institucional hacia el desarrollo de nuevo conocimiento científico, valorar tanto entre sistemas o herramientas de *software* libre y también opciones propietarias, cuyo uso sea extendido y comprobado a nivel internacional; además, que estén basadas en las normas técnicas necesarias para llevar a cabo la Preservación Digital Sistémica, específicamente con el Modelo OAIS de la Norma ISO 14721, al tiempo que su uso y mantenimiento sea económicamente sostenible en el tiempo, para la Institución.

   Se plantea que sea el personal universitario quién adquiera el conocimiento relacionado con la preservación digital, en el desarrollo y/o implementación de la herramienta tecnológica. Estos profesionales serán los que formarán parte del equipo de trabajo del Archivo Digital, los miembros de la CIADi y las unidades conexas como el AUROL y el Centro de Informática. Asimismo, esta perspectiva promoverá que la Universidad tenga una mayor independencia tecnológica.

   Además, la UCR debe procurar que se desarrolle investigación científica que genere conocimiento nuevo en cuanto a preservación digital. Estas acciones permitirán conocer los planteamientos teórico-prácticos que se aplican en otros países y que pueden aportar al buen funcionamiento del ADiUCR, o bien compartir los avances que alcance la UCR con otras instituciones públicas y privadas.

7. Se recomienda que durante el proceso de desarrollo e implementación del ADiUCR en la Institución, el Centro de Informática considere dentro de sus lineamientos y de la campaña de ciberseguridad, las condiciones de Preservación Digital Sistémica y la Cadena de Custodia Ininterrumpida de la información.

   Además, se sugiere actualizar las Directrices de Seguridad de la Información aprobada en el año 2015, considerando la implementación de buenas prácticas de ciberseguridad más actualizadas, como por ejemplo, las planteadas en las normas ISO/IEC 27001:2022 y la ISO/IEC 27002:2022.

5. Referencias bibliográficas

ArchivesSpace. (2022). *Misión y principios rectores.* https://archivesspace.org/about/mission

Archivo Digital del Archivo Histórico de la Policía Nacional de Guatemala. (s.f.). *Sobre este sitio*. https://ahpn.lib.utexas.edu/es/sobre_este_sitio

Archivo General de la Nación de Colombia. (2018). *Fundamentos de preservación digital a largo plazo*. https://www.archivogeneral.gov.co/sites/default/files/Estructura_Web/5_Consulte/Recursos/Publicacionees/FundamentosPreservacionLargoPlazo.pdf

Archivo General de la Nación de Colombia. (s.f.). *Proyecto ADN Archivo Digital Nacional*. https://www.archivogeneral.gov.co/sites/default/files/Estructura_Web/magazine/ADN/ADN_AGN.pdf

Archivo Universitario Rafael Obregón Loría (AUROL) y Centro de Informática (CI). (s.f.). *Presentación Lanzamiento SiGeDI*. https://archivo.ucr.ac.cr/docum/sigedi_lanzamiento.pdf

Archivo Universitario Rafael Obregón Loría (AUROL). (s.f.). *Contactos de las unidades que utilizan SIGEDI*. https://archivo.ucr.ac.cr/sigedi_unidades.htm

Archivo Universitario Rafael Obregón Loría (AUROL). (2009). *Carta de servicios*. https://archivo.ucr.ac.cr/cservicios.html

Archivo Universitario Rafael Obregón Loría (AUROL). (2017-a). *Procedimientos*. https://archivo.ucr.ac.cr/CUSED/informes.html

Archivo Universitario Rafael Obregón Loría (AUROL). (2017-b). *Tablas de Plazos de Conservación*. https://archivo.ucr.ac.cr/CUSED/informes.html

Archivo Universitario Rafael Obregón Loría (AUROL). (2017-c). *Personal encargado de los Archivos de la Administración*. https://archivo.ucr.ac.cr/b-archi.html

Archivoz. (2020). *Los repositorios digitales en Archivos*. https://www.archivozmagazine.org/es/repositorios-digitales-de-archivos/

Arribas-del Pozo, M. (2019). *Gestión de Archivos MF0978_2*. Ediciones Paraninfo S.A.

Artefactual Systems Inc. (2022-a). *Archivematica.* https://www.archivematica.org/es/

Artefactual Systems Inc. (2022-b). *Archivematica documentation.* https://www.archivematica.org/en/docs/archivematica-1.13/

Asamblea Legislativa de la República de Costa Rica. (1940). *Ley N° 362 Ley Orgánica de la Universidad de Costa Rica*. https://www.cu.ucr.ac.cr/normativ/ley_de_creacion_ucr.pdf

Asamblea Legislativa de la República de Costa Rica. (2005). *Ley de Certificados, Firmas Digitales y Documentos Electrónicos Nº 8454*. http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=55666

Asamblea Nacional Constituyente. (1949). *Constitución Política de la República de Costa Rica*. https://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=871

Asociación Española de Normalización y Certificación (AENOR). (2008). *UNE-ISO/TR 18492:2008 IN Conservación a largo plazo de la información basada en documentos*. Madrid: AENOR.

Asociación Española de Normalización y Certificación (AENOR). (2015-a). *UNE-ISO 14641-1: 2015 Archivo electrónico Parte 1: Especificaciones para el diseño y funcionamiento de un sistema de información para la preservación de información digital*. Madrid: AENOR.

Asociación Española de Normalización y Certificación (AENOR). (2015-b). *UNE-ISO 14721:2015 Sistemas de transferencia de datos e información espaciales. Sistema abierto de información de archivo (OAIS). Modelo de referencia.* Madrid: AENOR.

Asociación Española de Normalización y Certificación (AENOR). (2016). *UNE-ISO 15489-1:2016 Información y documentación. Gestión de documentos. Parte 1: Conceptos y Principios*. Madrid: AENOR.

Asociación Española de Normalización y Certificación (AENOR). (2017) *UNE-ISO 16363:2017 Sistemas de transferencia de información y datos espaciales. Auditoría y certificación de repositorios digitales de confianza*. Madrid: AENOR.

Asociación Española de Normalización y Certificación (AENOR). (2020). *UNE-ISO 17068:2020 Información y documentación. Repositorio de tercero de confianza para documentos electrónicos*. Madrid: AENOR.

Barnard-Amozorrutia, A. (2020). La preservación de archivos digitales en México. Los casos de estudio en el marco de InterPARES. en A. Barnard (Ed.), *El proyecto InterPARES en América Latina y el Caribe* (1 ed, pp.82-108). Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. https://inai.janium.net/janium/Documentos/3801%20InterPARES.pdf

Bernal-Torres, C. (2010). *Metodología de la investigación*. Pearson Educación de Colombia Ltda. https://abacoenred.com/wp-content/uploads/2019/02/El-proyecto-de-investigaci%C3%B3n-F.G.-Arias-2012-pdf.pdf

Biblioteca Nacional de España. (s.f.). *Diccionario de Datos de Metadatos de Preservación: PREMIS Versión 2.0*. http://www.loc.gov/standards/premis/PREMIS_es.pdf

Business Integrators Systems Limitada. (2022). *Arca. Repositorio de preservación para objetos digitales*. http://www.bis.co.cr/Products/Arca

Bustelo-Ruesta, C. (2011). *Serie 30300: Sistema de Gestión para los Documentos*. España: SEDIC.

Bustos-González, A y Fernández-Porcel, A. (2008). *Directrices para la creación de repositorios institucionales en universidades y organizaciones de educación superior.* https://repository.urosario.edu.co/bitstream/handle/10336/223/Directrices.pdf?sequence=1&isAllowed=y

Calvo-López, D. y Otárola-Sáenz, M. (2020). *Propuesta de un plan para la gestión de fotografías digitales con valor científico cultural. Estudio de Caso: Dirección General del*

Archivo Nacional de Costa Rica. [Tesis de Licenciatura no publicada]. Universidad de Costa Rica.

Cantillano-Mora,N., Rojas-Mora, L.C., Otárola-Saénz, M., Valerín-Alvarado, E. e Irola-Rojas, S. (22, 23 y 24 de julio de 2019). *El Archivo Digital Nacional (ADN)*. Memoria del XXXI Congreso Archivístico Nacional, San José, Costa Rica. https://www.archivonacional.go.cr/web/educativo/memoria_congreso_2019.pdf

Caplan, P. (2009). *Entender PREMIS*. http://loc.gov/standards/premis/UnderstandingPREMIS_espanol.pdf

Castillo-Solano, G. y Umaña-Alpízar, R. (2018). *Modelo de Preservación de Documentos Digitales en la Administración Universitaria. Estudio De Caso: Universidad Nacional* [Tesis de maestría no publicada]. Universidad de Costa Rica.

Castillo-Solano, G. y Umaña-Alpízar, R. (2019). Modelo para la preservación de documentos digitales. *Revista del Archivo Nacional*, 83(1-12), 129-182. http://www.dgan.go.cr/ran/index.php/RAN/article/view/453/371

Castro-Mattei, A. (2020). *Informe General de Labores Período de Transición 2020*. https://ci.ucr.ac.cr/sites/default/files/2022-03/Informe%20Transicion%20de%20Gestion%202020.pdf

Castro-Obando, V. (2022). Capítulo 1: Políticas públicas y base institucional para el desarrollo tecnológico. En Programa Sociedad de la Información y el Conocimiento (PROSIC) (Ed.), *Hacia la Sociedad de la Información y el Conocimiento: Informe 2022*. (pp.17-101). Universidad de Costa Rica. http://www.prosic.ucr.ac.cr/sites/default/files/recursos/informe_2022_completo.pdf

Cedeño-Molina, R.A; Granados-Peraza, N.M; Guevara-Acón, G y Montero-Paniagua, C.E. (2014). *Propuesta de un Modelo de Requisitos Archivísticos para un Sistema de Gestión de Documentos Electrónicos de Archivo (SGDEA) en Costa Rica*. [Seminario de Graduación de Licenciatura Universidad de Costa Rica]. http://repositorio.sibdi.ucr.ac.cr:8080/jspui/handle/123456789/2373

Centro de Informática de la Universidad de Costa Rica. (2016-a). *Manual de la Organización del Centro de Informática Universidad de Costa Rica*. https://ci.ucr.ac.cr/sites/default/files/2022-03/CI-UCM-D03%20Manual%20de%20la%20organizacion%20CI%20V2.5.pdf

Centro de Informática de la Universidad de Costa Rica. (2016-b). *Lineamientos técnicos para cuentas de acceso*. https://ci.ucr.ac.cr/sites/default/files/2022-03/CI-URS-L01-2016%20Lineamientos%20tecnico%20para%20cuentas%20de%20acceso%20V1.0.pdf

Centro de Informática de la Universidad de Costa Rica. (2019). *Metodología de continuidad de tecnologías de la Información y la Comunicación (TIC)*. https://dev.ci.ucr.ac.cr/sites/default/files/2022-03/CI-URS-D01%20Metodologia%20de%20continuidad%20de%20TIC%20V2.0%20y%20anexos.pdf

Centro de Informática de la Universidad de Costa Rica. (2020-a). *Lineamiento General para la Gestión de Seguridad de la Información en los Sistema de Información*. https://ci.ucr.ac.cr/sites/default/files/2022-03/CI-ADS-L01%20Lineamiento%20general%20para%20la%20gestion%20de%20la%20seguridad%20de%20la%20informacion%20en%20los%20sistemas%20de%20informacion%20V1.0.pdf

Centro de Informática de la Universidad de Costa Rica. (2020-b). *Lineamientos técnicos para el uso de software institucional*. https://ci.ucr.ac.cr/sites/default/files/2022-03/CI-AGU-L02%20Lineamientos%20Tecnicos%20para%20el%20uso%20de%20Software%20Institucional%20V1.0.pdf

Centro de Informática de la Universidad de Costa Rica. (2021-a). *Marco de Gobierno y Gestión de TI de la Universidad de Costa Rica*. https://ci.ucr.ac.cr/sites/default/files/2022-03/Marco%20de%20Gobierno%20y%20gestion%20TI%20UCR%20V1.0.pdf

Centro de Informática de la Universidad de Costa Rica. (2021-b). *CI-AGS-P11 Procedimiento para la realización y custodia de respaldos*. [Procedimiento no publicado]. Universidad de Costa Rica

Centro de Informática de la Universidad de Costa Rica. (2022-a). *Resguardo y protección de la información*. https://ci.ucr.ac.cr/es/resguardo-y-proteccion-de-la-informacion

Centro de Informática de la Universidad de Costa Rica. (2022-b). *Administración de la Continuidad de Operaciones*. https://ci.ucr.ac.cr/sites/default/files/2022-04/administracio%CC%81n%20de%20la%20continuidad%20de%20operaciones.pdf

Centro de Informática de la Universidad de Costa Rica. (2022-c). *Estándares para compra de equipo tecnológico*. https://ci.ucr.ac.cr/es/estandares-para-compra-de-equipo-tecnologico

Centro de Informática de la Universidad de Costa Rica. (s.f.-a). *CI-AGS-P01 Procedimiento para la realización de respaldos y pruebas de recuperación de datos.* [Procedimiento no publicado]. Universidad de Costa Rica

Centro de Informática de la Universidad de Costa Rica. (s.f.-b). *Panfleto resguardo y protección de la información*. https://ci.ucr.ac.cr/sites/default/files/2022-04/resguardo%20y%20proteccio%CC%81n%20de%20la%20informacio%CC%81n.pdf

Centro de Informática de la Universidad de Costa Rica. (s.f.-c). *Comisión institucional de equipamientos*. https://ci.ucr.ac.cr/es/comision-institucional-de-equipamientos#

Centro de Informática de la Universidad de Costa Rica. (s.f.-d). *Campaña de Ciberseguridad*. https://ci.ucr.ac.cr/campana-de-ciberseguridad

Chávez-Abad, R. (2015). *Introducción a la Metodología de la Investigación*. UTMACH. http://repositorio.utmachala.edu.ec/handle/48000/6785

Comisión de las Naciones Europeas. (2003). *El papel de la administración electrónica en el futuro de Europa (Texto pertinente a efectos del EEE). Bruselas: Comisión de las Naciones Europeas*. ttps://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0567:FIN:ES:PDF

Comisión Económica para América Latina y el Caribe [CEPAL]. (2020a). *Gestión del Conocimiento (GDC)*. https://biblioguias.cepal.org/c.php?g=738015&p=5789030

Comisión Económica para América Latina y el Caribe [CEPAL]. (2020b). *Gestión de datos de investigación*. https://biblioguias.cepal.org/gestion-de-datos-de-investigacion/metadatos

Comisión Institucional de Archivo Digital. (2022). *Acta de la Sesión 2-2022*. [No publicado]. Universidad de Costa Rica.

Comisión Institucional de Equipamiento de la Universidad de Costa Rica. (2022). *Acta de la Comisión Institucional de Equipamiento CIEQ-22-2022*. https://ci.ucr.ac.cr/sites/default/files/2022-06/Acta%20de%20la%20Comisio%CC%81n%20Institucional%20de%20Equipamiento%20CIEQ-22-2022.pdf

Comisión Universitaria de Selección y Eliminación de Documentos (CUSED). (2015). *Informe de Valoración Nº 16-2015 Comisión Universitaria de Selección y Eliminación de Documentos.* http://archivo.ucr.ac.cr/CUSED/informes/16-2015CUSED.pdf

Comisión Universitaria de Selección y Eliminación de Documentos (CUSED). (2018-a). *Procedimiento para elaborar la Identificación archivística en la Universidad de Costa Rica*. https://archivo.ucr.ac.cr/CUSED/procedimientos/CUSED_PIA_2020.pdf

Comisión Universitaria de Selección y Eliminación de Documentos (CUSED). (2018-b). *Procedimiento para la valoración de documentos en la Universidad de Costa Rica*. https://archivo.ucr.ac.cr/CUSED/procedimientos/CUSED-PVD-2018.pdf

Comisión Universitaria de Selección y Eliminación de Documentos (CUSED). (2018-c). *Procedimiento para la eliminación de documentos en la Universidad de Costa Rica*. https://archivo.ucr.ac.cr/CUSED/procedimientos/CUSED_PED-2018.pdf

Comisión Universitaria de Selección y Eliminación de Documentos (CUSED). (2021-1). *Oficio CUSED-13-2021*. [No publicado]. Universidad de Costa Rica.

Comisión Universitaria de Selección y Eliminación de Documentos (CUSED). (2021-2). *Tabla de Plazos de Conservación Y Eliminación de Documentos Series Comunes en la Universidad de Costa Rica*. https://archivo.ucr.ac.cr/CUSED/informes/CUSED_TPC_2018_V1.3.pdf

Comité Gerencial de Informática de la Universidad de Costa Rica. (2016). *Plan Estratégico Institucional en Tecnologías de Información 2016-2020*. https://transparencia.ucr.ac.cr/medios/documentos/2016/PEITI_2016.pdf

Comité Técnico del Sistema de Archivos de la Universidad de Costa Rica (SAU-CT). (2016). *Normas de trabajo del Comité Técnico*. https://archivo.ucr.ac.cr/CT/docs/Normas.pdf

Comité Técnico del Sistema de Archivos Universitarios (SAU-CT). (2021). *Oficio SAU-CT-23-2021*. [No publicado]. Universidad de Costa Rica.

Concha, G. y Naser, A. (2012). Panorama de Gobierno Electrónico en la región: resultados e impactos. Por A. Naser y G.Concha (Ed.). *El desafío hacia el gobierno abierto en la hora de la igualdad*. http://repositorio.cepal.org/bitstream/handle/11362/3969/1/S2012004_es.pdf

Consejo Internacional de Archivos (ICA). (2000). *Norma Internacional de Descripción Archivística ISAD (G)*. ICA.

Consejo Internacional de Archivos (ICA). (2004). *Norma Internacional sobre los Registros de Autoridad de Archivos relativos a Instituciones, Personas y Familias ISAAR-CPF.* https://www.ica.org/sites/default/files/ISAAR2ES.pdf

Consejo Nacional de Rectores (CONARE). (2012). *Compendio Leyes, Decretos y Convenios de la Educación Superior Universitaria Estatal*. https://repositorio.conare.ac.cr/bitstream/handle/20.500.12337/2131/OPES-02-2013.pdf?sequence=1&isAllowed=y

Consejo Universitario de la Universidad de Costa Rica. (1974). *Estatuto Orgánico de la Universidad de Costa Rica.* https://www.cu.ucr.ac.cr/normativ/estatuto_organico.pdf

Consejo Universitario de la Universidad de Costa Rica. (2004). *Lineamientos para la emisión de la normativa institucional*. https://www.cu.ucr.ac.cr/normativ/emision_normativa.pdf

Consejo Universitario de la Universidad de Costa Rica. (2008). *Políticas de la Universidad de Costa Rica para los años 2010–2014*. https://www.cu.ucr.ac.cr/uploads/tx_ucruniversitycouncildatabases/normative/politicas_institucionales_2010-2014.pdf

Consejo Universitario de la Universidad de Costa Rica. (2008). *Reglamento del Sistema de Archivos de la Universidad de Costa Rica.* https://www.cu.ucr.ac.cr/normativ/sistema_archivos.pdf

Consejo Universitario de la Universidad de Costa Rica. (2009). *Normas generales y específicas para la formulación, ejecución y evaluación del presupuesto de la Universidad de Costa Rica*. https://www.cu.ucr.ac.cr/normativ/normas_presupuesto.pdf

Consejo Universitario de la Universidad de Costa Rica. (2020). *Plan Estratégico Institucional 2021-2025*. https://transparencia.ucr.ac.cr/medios/documentos/2021/plan_estrategico_institucional_2021-2025.pdf

Consejo Universitario de la Universidad de Costa Rica. (2020). *Políticas Institucionales 2021-2025*. https://www.cu.ucr.ac.cr/uploads/tx_ucruniversitycouncildatabases/normative/politicas_institucionales_2021-2025.pdf

Consejo Universitario de la Universidad de Costa Rica.(s.f.-1). *Normativa*. https://www.cu.ucr.ac.cr/normativa/orden-alfabetico.html

Consejo Universitario de la Universidad de Costa Rica. (s.f.-2). *Políticas*. https://www.cu.ucr.ac.cr/politicas.html

Cruz-Mundet, J.R. (2011). Principios, términos y conceptos fundamentales. Por J.R. Cruz-Mundet. *Administración de documentos y archivos. Textos fundamentales*. Madrid: Guillomía Comunicación Gráfica C.B.

Cruz-Mundet, J.R. (2012). *Archivística: Gestión de documentos y administración de archivos*. Madrid: Alianza Editorial, S.A.

Cruz-Romero, R. (2018). Gobernanza digital: Un análisis de propuestas para Costa Rica. *e-Ciencias de la Información, 8* (1). https://revistas.ucr.ac.cr/index.php/eciencias/article/view/29808/32547

Díaz Majada, G. (Junio 2020). AtoM. La irrupción del software libre de descripción normalizada y difusión archivística. *Hilo_s Documentales*, 2 (3). 7-21. https://revistas.unlp.edu.ar/HilosDocumentales/issue/view/698/Hilos%20junio%202020

Digital Library Federation. (2010). *<METS> Metadata Encoding and Standard: Primer and Reference Manual*. https://www.loc.gov/standards/mets/METSPrimer.pdf#page=109&zoom=100,92,369

DSpace. (2022). *Introduction*. https://wiki.lyrasis.org/display/DSDOC7x/Introduction

DuraCloud. (2022). *Features*. *https://duraspace.org/duracloud/about/features/*

Federal Agencies Digital Guidelines Initiative [FADGI]. (2017). *About*. http://www.digitizationguidelines.gov/about/

Federal Agencies Digital Guidelines Initiative [FADGI]. (2021). *FADGI Impacts and Benefits*. http://www.digitizationguidelines.gov/about/FADGI-Impacts.html

Fedora. (2022). *Technical Specifications*. https://duraspace.org/fedora/resources/technical-specifications/

Flores, D. (05 de abril de 2020-a). *La Cadena de Custodia Digital Archivística - CCDA combinada con Preservación Digital Sistémica - PDS para Archivos*. https://www.dpconline.org/blog/wdpd/blog-daniel-flores-wdpd

Flores, D. (02 de abril de 2020-b). *Modelo de Preservación Digital Sistémica: Cadena de Custodia Digital Archivística - CCDA, Sevilla, ES* [Video]. Youtube. https://www.youtube.com/watch?v=VgcglqOe1Mo

Flores, D. (26 de octubre de 2022). *Objetos digitales contemporáneos como documentos de archivo de cara a la Transformación digital*. https://www.archivonacional.go.cr/web/congreso2022/2022ponencia_objetosdigitales.pdf

Foix, L. (2003). *La gestión de fondos fotográficos en entidades no comerciales*. https://arxiu-web.upf.edu/hipertextnet/numero-1/fotografia.html

Fonseca-Chacón, N. (2022-03-16). Notaria pública C.23138. *Protocolo notarial, tomo segundo*. Escritura número ciento veintisiete, visible de folio ciento catorce frente-línea diecisiete, a folio ciento diesciseis-línea veintisiete.

Gamboa-Suárez, J.L. (2020). *Importancia de la seguridad informática y ciberseguridad en el mundo actual*. http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/8668/IMPORTANCIA%20DE%20LA%20SEGURIDAD%20INFORM%c3%81TICA%20Y%20CIBERSEGURIDAD%20EN%20EL%20MUNDO%20ACTUAL.pdf?sequence=1&isAllowed=y

García-Morales, E. (2013). *Gestión de documentos en la e-administración*. Barcelona: Editorial UOC.

Giménez-Chornet, V. (2014). Criterios ISO para la preservación digital de los documentos de archivo. *Códices*, 10 (2), 135-150 https://ciencia.lasalle.edu.co/cgi/viewcontent.cgi?article=1169&context=co

Gobierno de Reino Unido. (s.f.). *Guidance. The role of the senior responsible owner. https://www.gov.uk/government/publications/the-role-of-the-senior-responsible-owner/the-role-of-the-senior-responsible-owner*

Grace, S. (2009). *Investigating the Significant Properties of Electronic Content over Time*. https://significantproperties.kdl.kcl.ac.uk/inspect-finalreport.pdf

Guerra-Rosado, F.J. (2017). *La comunicación en interpretación del patrimonio*. https://www.miteco.gob.es/es/ceneam/articulos-de-opinion/2017-05-francisco-guerra-nutri_tcm30-380035.pdf

Hernández-Olivera, L, Martín-González, Y, Ríos-Hilario, A, y Travieso-Rodríguez, C. (2011). *La construcción de la archivística. Una aproximación a la investigación científica a través de las tesis doctorales*. II Reunião Brasileira de Ensino e Pesquisa em Arquivologia REPARQ 2011. https://gredos.usal.es/bitstream/handle/10366/124133/Reparq%202%20La%20construccion%20de%20la%20archivistica.pdf?sequence=1&isAllowed=y

Hernández-Sampieri, R. (2014). *Metodología de la investigación sexta edición*. McGraw-Hill / Interamericana Editores, S.A. de C.V. http://www.digitalrepositorio.com/files/original/97a5883a1d6106e6ac908afd7ea838d1.pdf

Hermann-Acosta, A. (2020). *Storytelling y comunicación multidireccional: una estrategia formativa para la era digital*. https://revistas.uasb.edu.ec/index.php/uru/article/download/1482/1322?inline=1

International Council on Archives [ICA]. (2016). *¿Qué es un documento de archivo?*. https://www.ica.org/es/que-es-un-documento-de-archivo

International Organization for Standardization (ISO). (s.f.). *ISO/IEC 27000 family Information security management*. https://www.iso.org/standard/iso-iec-27000-family

InterPARES 1 Project. (s.f.). *Project summary*. http://www.interpares.org/ip1/ip1_index.cfm

InterPARES 2 Project. (s.f.-a). *Methodological principles*. http://www.interpares.org/ip2/ip2_methodological_principles.cfm

InterPARES 2 Project. (s.f.-b). *Project summary 2002-2007*. http://www.interpares.org/ip2/ip2_index.cfm

InterPARES 3 Project. (2012). *"Glosario InterPARES de Preservación Digital : Parte correspondiente a InterPARES 3" en español versión 3.0*. http://www.interpares.org/display_file.cfm?doc=ip3_mexico_glosario_interpares3_v3-0.pdf

InterPARES 3 Project. (s.f.). *Project summary*. http://www.interpares.org/ip3/ip3_index.cfm

InterPARES Project. (s.f.-a). *Director's message*. http://www.interpares.org/ip_director_welcome.cfm

InterPARES Project. (s.f.-b). *Project overview*. http://www.interpares.org/

InterPARES Trust. (2018). *InterPARES Trust*. https://interparestrust.org/

InterPARES. (2013). *Los Caminos de los Documentos de Archivo Digitales: Tópicos de Preservación Digital. Módulo 4: Un Resumen de Metadatos.* http://interpares.org/ip3/display_file.cfm?doc=ip3_canada_gs12_module_4_sp.pdf

InterPARES. (2018-a). *Dictionary.* http://www.interpares.org/ip2/display_file.cfm?doc=ip2_dictionary.pdf&CFID=26983280&CFTOKEN=10476782

InterPARES. (2018-b). *Glossary*. http://www.interpares.org/ip2/display_file.cfm?doc=ip2_glossary.pdf&CFID=26983280&CFTOKEN=10476782

Lacombe-Rocha, C. (2020). Estudos de caso realizados no âmbito do TEAM Brasil en A. Barnard (Ed.), *El proyecto InterPARES en América Latina y el Caribe* (1 ed, pp.55-81). Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. https://inai.janium.net/janium/Documentos/3801%20InterPARES.pdf

Leija-Román, D. (2017). *Preservación digital distribuida y la colaboración interinstitucional: Modelo de preservación digital para documentos con fines de investigación en universidades de México.* [Tesis de doctorado, Universitat de Barcelona]. http://diposit.ub.edu/dspace/bitstream/2445/117368/1/DALR_TESIS.pdf

Libnova. (2010-2016-a). *Libsafe, software de preservación digital: sencillo, flexible, potente.* http://www.preservaciondigital.es/soluciones-para-preservacion-digital/libsafe-product-tour/

Libnova. (2010-2016-b). *Plataforma Libsafe para preservación digital.* *http://www.preservaciondigital.es/soluciones-para-preservacion-digital/*

Library of Congress. (2016). *METS: introducción y tutorial*. https://www.loc.gov/standards/mets/METSOverview_spa.html#MHead

Library of Congress. (2017). *Guidelines for using PREMIS with METS for exchange*. https://www.loc.gov/standards/premis/guidelines2017-premismets.pdf

Library of Congress. (2023). *Sustainability of Digital Formats: Planning for Library of Congress Collections*. https://www.loc.gov/preservation/digital/formats/fdd/fdd000146.shtml

Library of Congress. (s.f.-a). *Digital Preservation*. https://www.digitalpreservation.gov/

Library of Congress. (s.f.-b). *Digital Preservation at the Library of Congress*. https://www.loc.gov/preservation/digital/

Library of Congress. (s.f.-c). *Encoded Archival Description Tag Library, Version 2002*. https://www.loc.gov/ead/tglib/appendix_a.html#a1

Lynch, Clifford. (2003). Institutional Repositories: Essential Infrastructure For Scholarship In The Digital Age. *ARL* (226), 1-7. https://www.cni.org/wp-content/uploads/2003/02/arl-br-226-Lynch-IRs-2003.pdf

Marini, F. (2006). Trusted digital repositories: overview and key issues. *ARCHIVI & COMPUTER, 16*(1), 76-94. http://www.interpares.org/display_file.cfm?doc=ip1-2_dissemination_jar_marini_archivi-computer_16_2006.pdf

Martin-Flatin, J. (1998). *Push vs. Pull in Web-Based Network Management*. https://arxiv.org/ftp/cs/papers/9811/9811027.pdf

Ministerio de Ciencia Tecnología y Telecomunicaciones (MICITT). (2013). *Política de Formatos Oficiales de los Documentos Electrónicos Firmados Digitalmente Dirección de Certificadores de Firma Digital Ministerio de Ciencia, Tecnología y Telecomunicaciones*. http://www.archivonacional.go.cr/pdf%5Cmarco_juridico_2016%5Cdirectrices%5Cdirectriz_politica_documentos_firmados_digitalmente.docx8

Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT). (2023). *Estrategia Nacional de Ciberseguridad Costa Rica 2023-2027*.

https://www.micitt.go.cr/wp-content/uploads/2023/04/Estrategia-Nacional-de-Ciberseguridad-MICITT-2023-2027.pdf

Ministerio de Cultura y Deporte - Gobierno de España. (s.f.). *Normalización archivística internacional*. http://censoarchivos.mcu.es/CensoGuia/proyecto.htm

Ministerio de Trabajo y Seguridad Social de Costa Rica (MTSS). (2019). *Guía para la Elaboración de Políticas Institucionales*. https://www.mtss.go.cr/perfiles/lineamientos_circulares_directrices_politicas_internas/lineamientos-circulares-directrices-politicas%20internas/guia_politicas_institucionales_MTSS.pdf

Mohd Zuhan Bin Mohd Zain y Ab Razak Bin Che Hussin. (2019). *Development of Instrument for Assessing Information Systems Continuance Use. Proceedings of the 2nd International Conference on Software Engineering and Information Management.* (p.213-217). ISBN: 978-1-4503-6642-7. Consultado en base de datos de texto completo UCR

National Archives and Records Administration [NARA]. (s.f.-a). *About the National Archives of the United States*. https://www.archives.gov/publications/general-info-leaflets/1-about-archives.html

National Archives and Records Administration [NARA]. (s.f.-b). *About the ERA 2.0 Project*. https://www.archives.gov/era/about

National Archives and Records Administration [NARA]. (s.f.-c). *Digital Preservation - Home*. https://www.archives.gov/preservation/electronic-records

National Archives and Records Administration [NARA]. (s.f.-d). *Digital Preservation Strategy*. https://www.archives.gov/preservation/electronic-records/digital-preservation-strategy

National Archives and Records Administration [NARA]. (s.f.-e). *What is the National Archives and RecordsAdministration?*. https://www.archives.gov/about

National Archives of Australia. (s.f.). *Digital Preservation Policy*. https://www.naa.gov.au/about-us/our-organisation/accountability-and-reporting/archival-policy-and-planning/digital-preservation-policy#standards

National Information Standards Organization [NISO]. (2017). *Data Dictionary – Technical Metadata for Digital Still Images.* https://groups.niso.org/higherlogic/ws/public/download/17937/ANSI-NISO%20Z39.87-2006%20%28R2017%29%2C%20Data%20Dictionary%20-%20Technical%20Metadata%20for%20Digital%20Still%20Images.pdf

Ochoa-Gutiérrez, J.; Sáenz-Giraldo, A. y Tirado-Tamayo, T. (2021). Experiencias de gestión de los procesos de preservación digital a partir del modelo OAIS en repositorios institucionales. *Anales de Documentación*, 2021, vol. 24, nº 1. http://dx.doi.org/10.6018/analesdoc.428141

Poder Ejecutivo de la República de Costa Rica. (2017). *Alcance N° 217: Decreto Ejecutivo N°40554-C Reglamento ejecutivo a la Ley del Sistema Nacional de Archivos*. https://www.imprentanacional.go.cr/pub/2017/09/07/ALCA217_07_09_2017.pdf

Portal Administración Electrónica. (s.f.-a). *Archivo Electrónico*. https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/Archivo_electronico.html

Portal Administración Electrónica. (s.f.-b). *Implantación de la Ley 39/2015 y Ley 40/2015*. https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Leyes-39-y-40-2015.html

Portal Administración Electrónica. (s.f.-c). *Política de gestión de documentos electrónicos*. https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/Archivo_electronico/pae_Politica-de-gestion-de-documentos-electronicos.html

Portal de Archivos Españoles. (s.f.). *Preguntas frecuentes*. https://pares.culturaydeporte.gob.es/preguntas-frecuentes.html#cla-0-01

PREMIS Editorial Committee. (2015). *PREMIS Data Dictionary for Preservation Metadata version 3.0.* https://www.loc.gov/standards/premis/v3/premis-3-0-final.pdf

Preservica. (2022-a). *Todo lo que necesita para salvaguardar, preparar para el futuro y acceder a su valioso contenido digital durante décadas*. https://preservica.com/digital-archive-software-1

Preservica. (2022-b). *Key features*. https://preservica.com/digital-archive-software-1/living-data-archive

Preservica. (2022-c). *Next generation archiving and active digital preservation.* https://cdn2.assets-servd.host/preservica-core/production/resources/Preservica-Brochure.pdf

Princeton University Library. (2021). *Acerca del Archivo Digital de Efímera de América Latina y el Caribe*. https://lae.princeton.edu/about?locale=es

Rectoría de la Universidad de Costa Rica. (2013). *Reglamento del Comité Gerencial de Informática*. http://ocu.ucr.ac.cr/images/ArchivosOCU/CapacitacionRIDS/NormativaRids/Resolucion-R-242-2013ComiteInformaticaUCR.pdf

Rectoría de la Universidad de Costa Rica. (2014). *Resolución R-289-2014*. https://www.ucr.ac.cr/medios/documentos/2014/resolucion_r-289-2014-11546ce13771240.pdf

Rectoría de la Universidad de Costa Rica. (2015). *Resolución R-102-2015*. https://www.cu.ucr.ac.cr/uploads/tx_ucruniversitycouncildatabases/officialgazette/2015/a07-2015.pdf

Rectoría de la Universidad de Costa Rica. (2018). *Reglamento del Centro de Informática*. https://www.cu.ucr.ac.cr/uploads/tx_ucruniversitycouncildatabases/officialgazette/2018/a12-2018.pdf

Rectoría de la Universidad de Costa Rica. (2020). *Resolución R-174-2020*. https://www.cea.ucr.ac.cr/images/cargas/Resolucion_R-174-2020.pdf

Rectoría de la Universidad de Costa Rica. (2022). *Resolución de Rectoría R-77-2022.* [No publicado]. Universidad de Costa Rica.

Red de Transparencia y Acceso a la Información [RTA]. (2014). *Guía de Implementación Gerencial – Administración electrónica*. http://mgd.redrta.org/guia-de-implementacion-gerencial-administracion-electronica/mgd/2015-01-22/100319.html

Rivas-Fernández, J.B. (2012). La problemática del patrimonio digital: El caso de Costa Rica. *Biblios* (47), 52-71. https://biblios.pitt.edu/ojs/index.php/biblios/article/view/31/108

RODA. (2022-a). *Welcome to RODA!*. https://www.roda-community.org/#welcome

RODA. (2022-b). *Overview.* *https://www.roda-community.org/?locale=es_CL#theme/Overview.md*

Rodríguez, J.R. y Lamarca, I. (2012). *Gestión de la información y el conocimiento.* http://openaccess.uoc.edu/webapps/o2/bitstream/10609/78267/7/Direcci%C3%B3n%20de%20sistemas%20de%20informaci%C3%B3n%20%28Executive%29_M%C3%B3dulo%204_Gesti%C3%B3n%20de%20la%20informaci%C3%B3n%20y%20el%20conocimiento.pdf

Rodríguez-Achútegui, M. (2023). *Guía de recursos para el desarrollo de proyectos y experiencias turísticas en torno al Patrimonio Cultural Inmaterial*. https://atlanticculturescape.eu/content/uploads/2023/01/GUIA-DE-RECURSOS-PROYECTOS-TURISTICOS-PCI.pdf

Rosetta. (2022). *Rosetta. Preserve sus activos digitales para el futuro*. https://exlibrisgroup.com/products/rosetta-digital-asset-management-and-preservation/

Russo-Gallo, P. (2009). *Gestión documental en las organizaciones*. Barcelona: Editorial UOC.

Sánchez-Tamez, M. (2016). *Los acervos históricos en las redes sociales*. https://www.amabpac.org.mx/wp/los-acervos-historicos-en-las-redes-sociales-por-mariana-e-sanchez-tamez/

Sandí-Delgado, J. y Cruz-Alvarado, M. (2017). Repositorios institucionales digitales: Análisis comparativo entre SEDICI (Argentina) y Kérwá (Costa Rica). *e-Ciencias de la Información* 7(1), 1-32. DOI: http://dx.doi.org/10.15517/eci.v7i1.25264

Serra-Serra, J. (2013-a). *Proyecto para la definición del archivo digital de la Universidad de Costa Rica* [No publicado]. Universidad de Costa Rica.

Serra-Serra, J. (2013-b). *Informe de evaluación de riesgos y de contexto*. [No publicado]. Universidad de Costa Rica.

Serra-Serra, J. (2013-c). *Modelo funcional y técnico del archivo digital*. [No publicado]. Universidad de Costa Rica.

Serra-Serra, J. (2013-d). *Política de preservación digital*. [No publicado]. Universidad de Costa Rica.

Serra-Serra, J. (2013-e). *Estrategia de preservación digital*. [No publicado]. Universidad de Costa Rica.

Serra-Serra, J. (2013-f). *Modelo de Protocolo de Transferencia*. [No publicado]. Universidad de Costa Rica.

Society of American Archivists (2019). *Encoded Archival Description Tag Library Version EAD3 1.1.1*. https://www.loc.gov/ead/EAD3taglib/EAD3-TL-eng.html

Society of American Archivists (SAA) (2022). *Encoded Archival Context - Corporate Bodies, Persons, and Families (EAC-CPF) Tag Library Version EAC-CPF 2.0*. https://eac.staatsbibliothek-berlin.de/schema/v2/eac.html#elem-descriptiveNote

Society of American Archivists (SAA) (s.f.). *Crosswalks ISAAR(CPF) to EAC-CPF* https://www.loc.gov/ead/EAD3taglib/EAD3-TL-eng.html

Térmens Graells, M. (19-20 de noviembre de 2009). *Los archivos y las bibliotecas ante la preservación digital: ¿un sólo enfoque?*. Actas XI Jornadas de Gestión de la Información. Madrid, España. http://eprints.rclis.org/13883/1/XIJGI-Termens.pdf

The National Archives. (2011). *Risk Assessment Handbook.* https://cdn.nationalarchives.gov.uk/documents/information-management/Risk-Assessment-Handbook.pdf

The National Archives. (2017-a). *Digital Strategy*. https://cdn.nationalarchives.gov.uk/documents/the-national-archives-digital-strategy-2017-19.pdf

The National Archives. (2017-b). *File profiling tool (DROID)*. https://www.nationalarchives.gov.uk/information-management/manage-information/policy-process/digital-continuity/file-profiling-tool-droid/

The National Archives. (s.f.-a). *Frequently asked questions*. http://nationalarchives.gov.uk/help/pronom/faq.htm

The National Archives. (s.f.-b). *Our digital strategy*. https://www.nationalarchives.gov.uk/about/our-role/plans-policies-performance-and-projects/our-plans/digital-strategy/

The National Archives. (s.f.-c). *Our history*. https://www.nationalarchives.gov.uk/about/our-role/what-we-do/our-history/

The National Archives. (s.f.-d). *Our role*. https://www.nationalarchives.gov.uk/about/our-role/

The National Archives. (s.f.-e). *Self-assessment tool.* http://www.nationalarchives.gov.uk/documents/information-management/self-assessment-tool.xls

UNESCO. (s.f). *Noción de preservación digital*. https://es.unesco.org/themes/information-preservation/digital-heritage/concept-digital-preservation

Universidad de Costa Rica. (2016). *Organigrama Institucional*. https://www.ucr.ac.cr/acerca-u/marco-estrategico/organigrama-institucional.html

Universidad de Costa Rica. (2020). *La UCR en cifras*. https://www.ucr.ac.cr/acerca-u/ucr-en-cifras.html

Universidad de Costa Rica. (2021). *Plan Estratégico Institucional 2021-2025*. https://transparencia.ucr.ac.cr/medios/documentos/2021/plan_estrategico_institucional_2021-2025.pdf

Universidad de la Plata. (2019). *Qué son los repositorios institucionales y cómo utilizarlos*. https://unlp.edu.ar/recursos/como-funcionan-los-repositorios-institucionales-14545

Universidad de Navarra. (10 de marzo de 2023). *Fotografía y patrimonio cultural*. https://www.unav.edu/noticias/-/contents/10/03/2023/fotografia-y-patrimonio-cultural/content/lovPblW1fC70/44305727

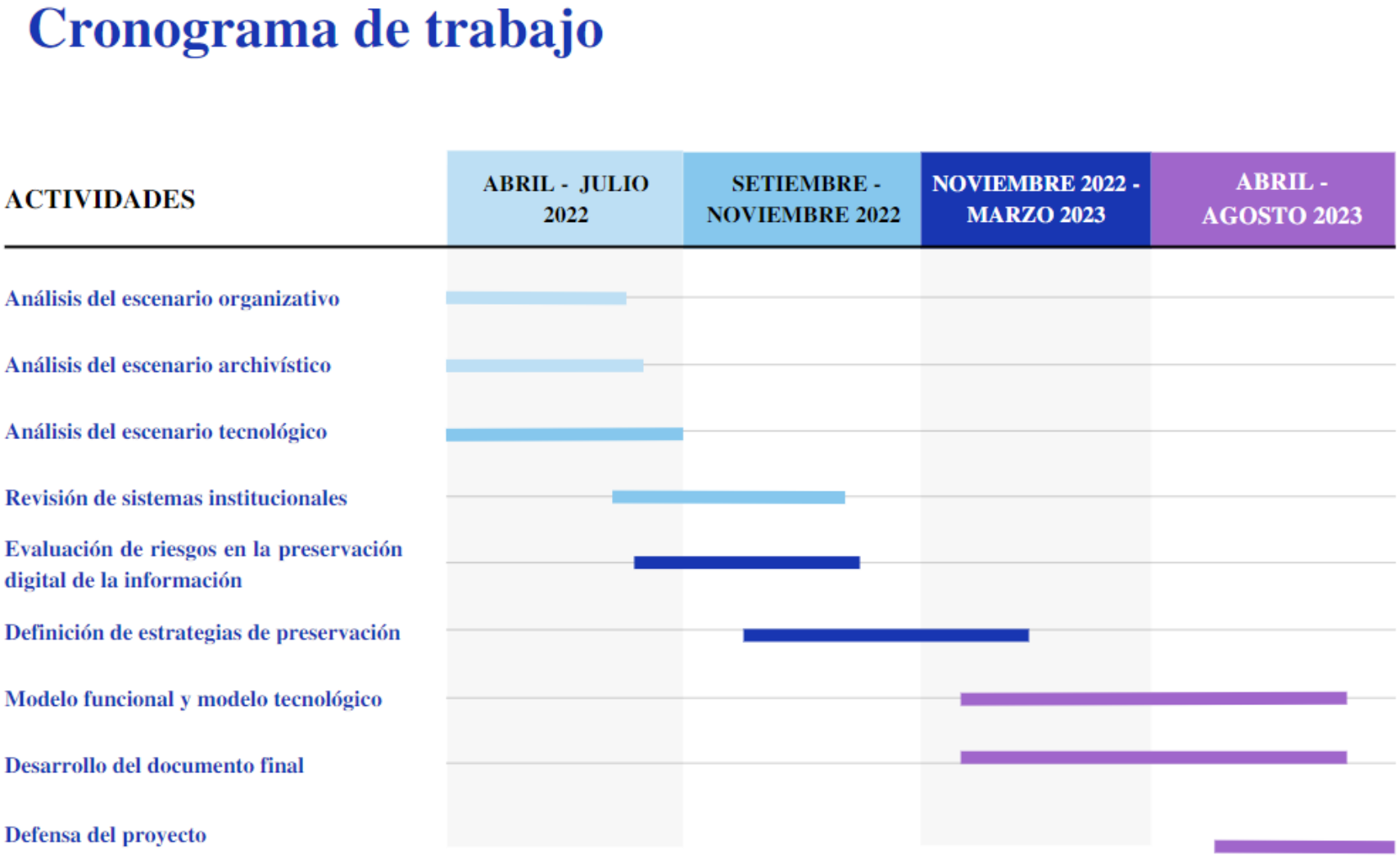
Universidad de Palermo. (s.f.). *El storytelling, el arte de contar historias con efectividad*. https://www.palermo.edu/negocios/que-es-el-storytelling.html

Universitat Oberta de Catalunya. (s.f.). *Redes sociales*. http://multimedia.uoc.edu/blogs/dim/es/dcu/xarxes-socials/

Voutssas, J. y Barnard-Amozorrutia, A. (2014). *Glosario de preservación archivística digital versión 4.0. Universidad Nacional Autónoma de México*. https://iibi.unam.mx/archivistica/glosario_preservacion_archivistica_digital_v4.0.pdf

Woodley, M. (2005). *Using Dublin Core. DCMI Glossary*. https://www.dublincore.org/specifications/dublin-core/usageguide/glossary/#schema

6. Cronograma



7. Anexos

Anexo 1. *Herramienta de autoevaluación Digital continuity self-assessment tool: Evaluación de Continuidad Digital y Gestión del Riesgo.*

Evaluación de la Continuidad Digital y Gestión del Riesgo de la Información
Como parte del Trabajo Final de Graduación titulado "Modelo de Preservación Digital Sistémica para el Desarrollo de un Archivo Digital en la Universidad de Costa Rica", desarrollado por los estudiantes Jorge Luis Mora Cerdas y Jéssica Barahona Chavarría, a continuación se presenta la herramienta de autoevaluación de preservación digital de la información. El cuestionario está basado en la *Digital Continuity Self-Assessment Tool*, desarrollado por los Archivos Nacionales del Reino Unido y tiene como objetivo llevar a cabo la evaluación de los riesgos, para la aplicación de acciones correctivas que aseguren la preservación y el uso de la información institucional.
Uso de la herramienta de autoevaluación
"Se recomienda que la herramienta sea completada por funcionarios relacionados con la gestión de la información dentro de la Unidad: archivista, profesional en Informática y jefe (a) administrativo. La herramienta de autoevaluación de continuidad digital divide la evaluación del riesgo en tres secciones: A - Roles y responsabilidades para la comprensión de la continuidad digital B - Requerimientos de información y las dependencias técnicas C - Gestión del riesgo en cuanto a la preservación digital En cada sección encontrará una serie de preguntas, con dos tipos de respuesta: - Botones circulares: donde debe seleccionar la respuesta que más se parezca a su situación - Casillas de verificación: donde puede seleccionar tantas opciones como sean aplicables. Todas las preguntas deberán ser completadas para finalizar el cuestionario. Los datos recopilados en esta herramienta serán utilizados de forma confidencial, únicamente con fines de investigación y serán accedidos exclusivamente por miembros de la CIADi y los estudiantes Jorge Luis Mora Cerdas y Jéssica Barahona Chavarría, para el análisis correspondiente."
Glosario
“Continuidad Digital La continuidad digital es la capacidad de utilizar la información digital de la manera que necesita, durante el tiempo que se necesite. Si no trabaja activamente para garantizar la continuidad digital, su información puede volverse inutilizable fácilmente. La continuidad digital se trata de asegurar que su información esté completa, disponible y, por lo tanto, utilizable para sus necesidades. La información puede considerarse utilizable si usted puede: encontrarla cuando la necesita, abrirla como lo necesite, trabajar con ella de la manera que se necesita, entender qué es y de qué se trata y confiar en que es lo que dice que es."

"DROID
Es el acrónimo para Identificación de Objeto de Registro Digital. Es una herramienta de software libre desarrollada por The National Archive de Reino Unido y permite perfilar automáticamente un amplio rango de formatos de archivos. Por ejemplo, le indica las versiones que se tienen, la edad y el tamaño del archivo y cuando fueron cambiados por última vez. También provee datos que ayudan a encontrar duplicados.

"Information Asset
El Activo de Información es un conjunto de información definido y gestionado como una sola unidad, que puede ser entendido, compartido, protegido y utilizado de forma efectiva. Los activos de información tienen valores, riesgos, contenidos y ciclos de vida reconocibles y gestionables. http://www.nationalarchives.gov.uk/documents/identify-information-assets.pdf"

"Information Asset Owner (AIO)
El Propietario de Activos de Información es un rol asignado a un miembro sénior del personal por parte del SIRO para asegurar que activos de información específicos sean gestionados apropiadamente. Esto significa que los activos de información son apropiadamente protegidos contra riesgos y que su valor para la organización es completamente reconocido."

"Information Asset Register (IAR)
El Registro de Activos de Información es un mecanismo para registrar los activos de información, el cual debería ser utilizado para documentar lo que se sabe acerca de los activos de información, las necesidades del negocio y el entorno tecnológico. Consiste en un número separado de registros que documentan aspectos particulares de la información digital y su ambiente."

"Configuration management
La gestión de la configuración es el proceso que asegura que el rendimiento y la funcionalidad de los servicios de las TI (Tecnologías de la Información) sean consistentes con los requerimientos y el diseño de los sistemas durante toda su vida útil. Mantiene la información sobre los objetos de configuración requeridos para brindar un servicio de TI, incluyendo las relaciones entre ellos."

"Senior Information Risk Owner (SIRO)
El SIRO es el responsable ejecutivo de los riesgos de la información y dirige la respuesta del Departamento. El SIRO se debe asegurar de que el riesgo para la continuidad digital está siendo gestionado de forma eficiente y efectiva, y que haya un enfoque multidisciplinario para la gestión de riesgos de información en una organización.

"Senior Responsible Owner (SRO)
El Propietario Principal Responsable (SRO) es la persona con la responsabilidad general de asegurar la continuidad digital en una organización.

A Comprensión digital continuidad y funciones y responsabilidades

1 Entendiendo la continuidad Digital

1,1	1.1. ¿La gestión de la continuidad digital es reconocida como un objetivo estratégico de su Unidad?	○ No hay reconocimiento o comprensión de la continuidad digital en ninguna parte de la Unidad. ○ Hay cierta comprensión de la continuidad digital, pero no en los niveles superiores de la Unidad ◉ Hay un reconocimiento en los niveles superiores de la Unidad sobre la importancia de la gestión de continuidad del digital, pero no es un objetivo formal ○ La gestión de la continuidad digital está documentado como un objetivo clave de la Unidad
1,2	¿Hay responsabilidades claras en cuanto a la gestión de los riegos para la continuidad digital?	○ No hay reconocimiento organizativo o propiedad de la gestión de los riegos para la continuidad digital. ◉ Alguien por debajo del nivel de Dirección en la Unidad es responsable de la gestión de riesgos para la continuidad digital. ○ El SIRO (o equivalente) es responsable gestión de los riegos para la continuidad digital, como un todo. ○ 4. El SIRO es responsable de la gestión de los riegos para la continuidad digital de la Unidad en conjunto. El SIRO es apoyado también por IAOs que son responsables de la continuidad digital de activos de información
1,3	¿Está alguien asumiendo la responsabilidad para la gestión de continuidad digital?	○ No. ○ Individuos están tomando responsabilidad de forma aislada para gestionar continuidad digital, pero no es centralizada ◉ Un individuo o equipo está tomando la iniciativa en la gestión de continuidad digital a través de la Unidad ○ El SIRO ha nombrado un SRO de continuidad digital, a un nivel adecuado y con autoridad para actuar.
1,4	¿Su Unidad definió el alcance y el proceso para la gestión de continuidad digital?	○ No. ◉ Hay no hay estrategia definida, pero se tomarán acciones para este fin en específico

		◯ Se ha definido un plan de acción con plazos claros para la gestión de continuidad digital
		◯ El alcance y el proceso de gestión de continuidad digital ha sido definido e incluye la integración de la gestión de continuidad digital con los procesos habituales.

2 Roles y responsabilidades

2,1	¿Personas de distintas disciplinas trabajan en conjunto a través de su Unidad para administrar la continuidad digital?	◯ No se hace nada. ◯ Individuos y unidades de negocio trabajan de forma aislada ◉ Individuos y unidades de negocios están colaborando en una base para este fin. ◯ Se ha establecido un enfoque multidisciplinario para coordinar las acciones
2,2	Funciones y responsabilidades: gestión de la información (IM)	◯ Especialistas en IM no entienden sobre continuidad digital o su rol para gestionarla ◯ Especialistas en IM entienden sobre continuidad digital pero no su rol para gestionarla. ◉ Especialistas IM están actuando para gestionar continuidad digital, pero están trabajando de forma aislada de las profesiones relacionadas dentro de la Unidad ◯ Especialistas IM tienen roles claros y responsabilidades y están gestionando la continuidad digital dentro de un enfoque multidisciplinario.
2,3	Funciones y responsabilidades: tecnologías de la información (TI)	◯ Especialistas de TI no entienden sobre continuidad digital o su rol para gestionarla. ◯ Especialistas en TI entienden sobre continuidad digital pero no su rol para gestionarla. ◉ Especialistas de TI están actuando para gestionar continuidad digital, pero están trabajando de forma aislada de las profesiones relacionadas dentro de la Unidad. ◯ Especialistas de TI tienen roles claros y responsabilidades y están gestionando la continuidad digital dentro de un enfoque multidisciplinario
2,4	Funciones y responsabilidades: aseguramiento de la información (IA)	◯ Especialistas en IA no entienden sobre continuidad digital o su rol para gestionarla

		○ Especialistas en IA comprenden sobre continuidad digital pero no su rol para gestionarla. ◉ Especialistas de IA están actuando para gestionar continuidad digital, pero están trabajando de forma aislada de las profesiones relacionadas dentro de la Unidad. ○ Especialistas en IA tienen roles claros y responsabilidades y están gestionando la continuidad digital dentro de un enfoque multidisciplinario
2,5	Funciones y responsabilidades: gerentes de proyecto y gerentes de cambio	○ Los jefes de proyecto o gerente cambio no entienden sobre continuidad digital o su rol para gestionarla ○ Los jefes de proyecto o cambio comprenden continuidad digital pero no su rol para gestionarla. ◉ Los jefes de proyecto o el cambio están actuando para gestionar continuidad digital, pero están trabajando de forma aislada de las profesiones relacionadas dentro de la Unidad. ○ Los jefes de proyecto o cambio tienen roles claros y responsabilidades y están gestionando la continuidad digital dentro de un enfoque multidisciplinario.
2,6	¿Los Propietarios de activos de información de la Unidad (IAOs) entienden su rol y toman medidas?	○ La Unidad no ha designado IAOs. ○ No entienden de continuidad digital ni su rol para gestionarla ◉ Asumen la responsabilidad de su rol en la gestión de continuidad digital, pero están trabajando de forma aislada ○ Tienen roles claros y responsabilidades y están gestionando la continuidad digital como parte de un enfoque multidisciplinario.

	Comprensión digital continuidad y funciones y responsabilidades				
	La Pregunta	El riesgo	Su Respuesta	Puntaje	Sus Acciones
1	**Entendiendo la continuidad Digital**				
1,1	**1.1. ¿La gestión de la continuidad digital es reconocida como un objetivo estratégico de su Unidad?**	Gestión de continuidad digital debe ser reconocido como un objetivo estratégico. Sin este reconocimiento es poco probable que la cuestión se dará los recursos y el apoyo que requiere.	Hay un reconocimiento en los niveles superiores de la Unidad sobre la importancia de la gestión de continuidad del digital, pero no es un objetivo formal	3	Mantener la continuidad digital debe ser documentada como un objetivo en las políticas pertinentes, por ejemplo, las políticas de administración IM, IA y el cambio.
1,2	**¿Hay responsabilidades claras en cuanto a la gestión de los riegos para la continuidad digital?**	Continuidad digital propiedad de alto nivel de la organización mayor información riesgo propietario (SIRO), o equivalente nivel de junta directiva e integrado en las estructuras de gobernanza de información existentes . Sin gobierno senior, es poco probable que la organización constantemente o efectivamente gestionar continuidad	Alguien por debajo del nivel de Dirección en la Unidad es responsable de la gestión de riesgos para la continuidad digital.	2	Riesgos de la información son riesgos para la capacidad de la organización para llevar a cabo su negocio de manera eficaz y responsable. Propiedad de riesgo información importante debe estar en nivel de placa o equivalente.
1,3	**¿Está alguien asumiendo la responsabilidad para la gestión de continuidad digital?**	Un propietario responsable Senior (SRO) deben ser nombrados por el SIRO para llevar la gestión de la continuidad digital a través de la organización. Sin un liderazgo claro, será difícil asegurar un enfoque eficiente, consistente y completa.	Un individuo o equipo está tomando la iniciativa en la gestión de continuidad digital a través de la Unidad	3	El individuo o equipo debe participar el SIRO y asegurarse de que sus acciones están alineadas con y son apoyadas por información gobernanza y riesgo gestión las estructuras existentes.
1,4	**¿Su Unidad definió el alcance y el proceso para la gestión de continuidad digital?**	Un ámbito de aplicación y proceso deben definirse para la gestión de continuidad digital a nivel organizativo, como incrustar dentro de procesos de 'negocios como siempre'. Sin esto será difícil asegurar que acciones ofrecen los resultados deseados y son sostenibles.	Hay no hay estrategia definida, pero se tomarán acciones para este fin en específico	2	La organización debe definir el alcance y el proceso de gestión de continuidad del digital, para poder determinar prioridades, asignar recursos y asegurar que las acciones son apropiadas. Acciones ad hoc pueden llevar a desperdiciadas recursos debido a la falta de coordinación o problemas importantes que quedan sin resolver debido a la falta de priorización.
2	**Roles y responsibilidades**				
2,1	**¿Personas de distintas disciplinas trabajan en conjunto a través de su Unidad para administrar la continuidad digitall?**	Exitosa gestión de la continuidad digital requiere de conocimientos de un número de diferentes áreas. Personal procede de funciones claves a través de la organización (gestión de la información, ti, IA, proyecto, gestión de cambios) para permitir un enfoque multidisciplinario para la gestión de continuidad digital. Sin esto, es probable que acción descoordinada y riesgos para la continuidad digital trataron sólo parcialmente.	Individuos y unidades de negocios están colaborando en una base para este fin.	3	Reunir estas personas en una manera más estructurada para manejar continuidad digital y coordinar la planificación y acciones, garantizando que actividad ajusta a las prioridades de la organización.
2,2	**Funciones y responsabilidades: gestión de la información (IM)**	Information management practitioners are responsible for understanding the information the organisation holds and the business activities it supports. They must define and implement policies and processes that will deliver the required usability over time and through change. Without this, the business may lose the ability to use its information as it needs, when it needs.	Especialistas IM están actuando para gestionar continuidad digital, pero están trabajando de forma aislada de las profesiones relacionadas dentro de la Unidad	3	Los profesionales de gestión de información deben entender cómo su trabajo en la gestión de continuidad digital puede apoyar los objetivos de otros equipos. Esto puede utilizarse para establecer relaciones entre los diferentes equipos que eventualmente pueden trabajar como parte de un equipo coordinado, multidisciplinario para asegurarse que continuidad digital de su información está protegida.

2,3	**Funciones y responsabilidades: tecnologías de la información (TI)**	Tecnólogos de información (IT) son responsables por el ambiente técnico que soporta la información de la organización. Debe asegurar que el ambiente permite que la información que se utilizará como es requerido por el negocio, con el tiempo y todo cambio. Sin esto, la empresa puede perder la capacidad para utilizar su información ya que necesita cuando lo necesita.	Especialistas de TI están actuando para gestionar continuidad digital, pero están trabajando de forma aislada de las profesiones relacionadas dentro de la Unidad.	3	Tecnólogos de información deben comprender cómo su trabajo en la gestión de continuidad digital puede apoyar los objetivos de otros equipos. Esto puede utilizarse para establecer relaciones entre los diferentes equipos que eventualmente pueden trabajar como parte de un equipo coordinado, multidisciplinario para asegurarse que continuidad digital de su información está protegida.	
2,4	**Funciones y responsabilidades: aseguramiento de la información (IA)**	Especialistas en aseguramiento de la información son responsables de la confidencialidad, integridad y disponibilidad de la información y los sistemas que lo admitan. Se centran en garantizar que la información está protegida y disponible para la explotación de negocios y generalmente tendrá un papel clave en la gestión de riesgos de la información, incluyendo los riesgos para la continuidad digital. Sin su participación en la gestión de continuidad del digital, el negocio puede no ser abordar eficazmente estos riesgos.	Especialistas de IA están actuando para gestionar continuidad digital, pero están trabajando de forma aislada de las profesiones relacionadas dentro de la Unidad.	3	Los profesionales de aseguramiento de la información deben comprender cómo su trabajo en la gestión de continuidad digital puede apoyar los objetivos de otros equipos. Esto puede utilizarse para establecer relaciones entre los diferentes equipos que eventualmente pueden trabajar como parte de un equipo coordinado, multidisciplinario para asegurarse que continuidad digital de su información está protegida.	
2,5	**Funciones y responsabilidades: gerentes de proyecto y gerentes de cambio**	Continuidad digital es el cambio más riesgo durante los períodos de cambio, ya sea negocio o cambio de tecnología. Sin gestión activa de la continuidad digital, los riesgos de la organización perdiendo la habilidad de usar su información según sea necesario.	Los jefes de proyecto o el cambio están actuando para gestionar continuidad digital, pero están trabajando de forma aislada de las profesiones relacionadas dentro de la Unidad.	3	Gerentes de proyecto y el cambio deben asegurarse que los requisitos y criterios de éxito se desarrollan como parte de un equipo coordinado y multidisciplinar que contiene IA, IM y otras funciones de negocios para asegurarse de que está protegida la continuidad digital de	
2,6	**¿Los Propietarios de activos de información de la Unidad (IAOs) entienden su rol y toman medidas?**	Los IAOs deben asegurarse de que la organización entiende que lo que necesita para utilizar sus activos de información. Esto es especialmente importante durante periodos de cambio. Gestión de la continuidad digital eficaz requiere estrecha colaboración entre IM y IA con IAOs asegurándose que se entienden los requerimientos del negocio para el uso de información. Sin esto, no será posible administrar la información adecuadamente, para asegurar que puede ser utilizado como sea necesario, con el tiempo y a través del cambio.	Asumen la responsabilidad de su rol en la gestión de continuidad digital, pero están trabajando de forma aislada	3	Un enfoque multidisciplinario para la gestión de continuidad digital debe reunir a personal clave a través de la organización para coordinar sus acciones.	

B Requerimientos de información y dependencias técnicas

1 Entendiendo los activos de Información

1,1	¿La organización entiende qué información tiene?	○ No. ○ Alguna información es rastreada por unidades de negocio, pero no hay ninguna visión corporativa completa ◉ La información crítica para el negocio o datos personales es entendida y documentada, pero no incluye toda la información de valor para la Unidad. ○ Toda la información de valor para la Unidad es incluida dentro de los activos de información y listada en un IAR completa.
1,2	¿La Unidad está documentando y dando seguimiento a las siguientes características en un Registro de Activos de Información o similar?	☑ Donde se encuentra la información (por ejemplo, sistemas, equipos, presentación de lugares) ☐ Sus características técnicas (p. ej. información de formato de archivo) ☐ Plazos de Retención (tablas de plazo) ☐ Valor de Negocio ☐ Riesgo para el Negocio ☐ Requerimientos de usabilidad ☐ Propiedad ☑ Restricciones de acceso y seguridad ☑ Sensibilidad de la información ☐ Riesgos del activo
1,3	La Unidad tiene...	☐ ... información que no está cubierta por un activo de información

		☑ ... información que no tiene un objetivo claro de uso
		☐ ... información que se sujeta o es propiedad de terceros
1,4	¿La Unidad entiende el valor de su información, el valor financiero y el uso que entrega a la empresa?	○ No, la Unidad no entiende el valor de su información. ○ La Unidad ha reconocido el valor de activos particular pero no todos. ◉ La Unidad comprende el valor de toda su información, pero esto no se utiliza sistemáticamente como una herramienta para apoyar la gestión de su información. ○ La Unidad comprende el valor de toda su información y utiliza esto para informar cómo administra su información.
1,5	La Unidad necesita conservar su información por...	☐ ... un corto plazo solo para uso del negocio, es decir, por menos de 5 años ☐ ... un mediano plazo para apoyo a las operaciones del negocio, es decir, de 5 a 10 años ☐ ... un largo plazo, de 10-30 años ☑ ... más de 30 años
1,6	La Unidad tiene la información digital que...	☐ ... no sabe la edad ☐ ... tiene más de cinco años ☐ .. tiene más de diez años ☐ ... tiene más de veinte años
1,7	¿La Unidad entiende cómo necesita utilizar (buscar, abrir, trabajar con, entender y confiar en) sus activos de información, tanto ahora como en el futuro?	○ No, la Unidad no conoce cómo debe utilizar todos sus activos de información. ◉ La Unidad comprende algunos aspectos de sus requisitos de usabilidad, pero no completamente.

- ○ La Unidad entiende y ha documentado todos sus requisitos de usabilidad actual pero no ha considerado cómo pueden cambiar.
- ○ La Unidad entiende y ha documentado todos los requisitos de usabilidad y ha considerado cómo pueden cambiar

1,8 La Unidad tiene la información que...	☑ ... está conforme con la petición de libertad de información
	☑ ... requiera de consulta pública o investigaciones
	☑ ... está cubierta por la ley de protección de datos
	☑ ... puede requerir de evidencia legal o forense
	☑ ... está sujeta a los actos de registros públicos
	☑ ... contiene datos sensibles o restringidos
	☑ ... debe ser compartida con otras unidades
	☑ ... debe ser publicado como información pública y apoya la transparencia
	☑ ... ayuda a los servicios del negocio
	☐ ... debe proporcionarse según un SLA
	☑ ... es necesario para ser reutilizada, reanalizada o reasignada
	☐ ... depende de otros activos de información para ser entendida?
	☑ ... tiene una historia de cambio que se debe conservar
	☐ ... la Unidad debe demostrar que no ha cambiado

2 Entendiendo las dependencias técnicas

2,1	¿La Unidad entiende su entorno técnico?	○ No, la Unidad no tiene una comprensión global de su entorno técnico. ○ La Unidad tiene una comprensión de los sistemas claves, pero no es completa ni documentada. ◉ La Unidad tiene una comprensión de todos sus sistemas y cómo son interdependientes, pero no hay ninguna coordinación de documentación o de gestión ○ La Unidad entiende y ha documentado su entorno técnico y las interdependencias, y utiliza esto para manejar su tecnología.
2,2	¿La Unidad entiende en qué formatos se almacena su información y las aplicaciones necesitan para usarlos?	○ No, la Unidad no entiende qué formatos de archivo posee o las aplicaciones que necesita para usarlos ○ La Unidad sólo entiende las aplicaciones más comunes que utiliza, pero no los formatos específicos y versiones que posee o las aplicaciones de las cuales dependen para usarlos ◉ La Unidad entiende que todas las aplicaciones que utiliza, pero no los formatos específicos y versiones que posee o las aplicaciones de las cuales dependen para usarlos. ○ La Unidad comprende todos los formatos específicos y versiones que posee y las aplicaciones de las cuales dependen para usarlos.
2,3	¿La Unidad está documentando y rastreando las siguientes opciones en una CMDB (Base de datos de gestión de la configuración) o equivalente?	☑ Sistemas ☐ Aplicaciones ☑ Bases de Datos ☑ Equipo físico ☐ Contratos de Soporte del Proveedor/Garantías ☐ Contraseñas y llaves de cifrado ☐ Gestión de Incidentes ☐ Dispositivos Externos o Removibles ☐ Se lleva a cabo Gestión de Formatos de Archivos

		☐ Acuerdos de Nivel de Servicio ☐ Licencias ☐ Acceso y Autorización ☐ Seguridad y Actualización ☐ Ajustes de configuración
2,4	¿La Unidad entiende cómo el entorno técnico apoya sus requisitos de usabilidad de la información?	○ No, la Unidad no entiende qué requisitos de usabilidad información necesitan ser apoyados por su entorno tecnológico ○ La Unidad tiene una comprensión limitada de cómo el entorno técnico está apoyando a las necesidades clave, pero la comprensión no es completa y no está asignadas a los activos de información individuales. ◉ La Unidad entiende el entorno técnico y la usabilidad que proporciona, pero no está asignado al soporte de activos de información individuales. ○ La Unidad está mapeando las relaciones entre el entorno tecnológico y los activos de información asegurar que se cumple con los requisitos de usabilidad.
2,5	¿La Unidad depende de tecnología obsoleta para cumplir con los requisitos de usabilidad de la información?	○ La Unidad posee tecnología obsoleta no administrada, hay limitada o ninguna comprensión de la tecnología o qué información apoya y cómo ○ La Unidad depende de tecnología obsoleta para entregar a los activos de información, pero la tecnología está siendo gestionada sin planes de migrar a otras tecnologías ◉ La Unidad se basa en tecnología obsoleta administrada para entregar a los activos de información y hay una estrategia para migrar a otras tecnologías cuando sea posible ○ La Unidad no depende de tecnología obsoleta.
2,6	¿La Unidad depende de tecnología hecha a la medida para ofrecer información de requisitos de usabilidad?	○ La Unidad no ha apoyado tecnología hecha a la medida, hay limitada o ninguna comprensión de la tecnología o qué información apoya y cómo. ○ La Unidad depende de tecnología hecha a la medida para entregar los activos de información, pero el soporte no está disponible durante toda la vida útil de los activos de información.

	◉ La Unidad depende de tecnología hecha a la medida para entregar a los activos de información, pero la tecnología está siendo apoyada durante la vida útil de los activos de información. ◯ La Unidad no depende de tecnología hecha a la medida.

2,7 La Unidad tiene información...	☑ almacenada en medios externos o extraíbles (por ejemplo, tarjetas, USB llaves, cintas o discos duros externos) ☑ almacenada en discos locales de los usuarios individuales (por ejemplo, computadoras portátiles) ☑ almacenada en servidores de correo electrónico (incluyendo archivos adjuntos) ☑ almacenada en sistemas de gestión de documentos (Sharepoint, SGDEA) ☑ almacenada en almacenamiento archivístico en línea (por ejemplo, archivos de correo electrónico) ☑ almacenada en almacenamiento de archivo sin conexión ☑ guardada en entornos protegidos por contraseña o cifrado

	Requerimientos de información y dependencias técnicas				
	La Pregunta	El Riesgo	Su Respuesta	Puntaje	Sus Acciones
1,1	¿La organización entiende qué información tiene?	La organización requiere una buena comprensión de toda la información, agrupan en activos manejables y asignado a propietarios específicos. Estos deberían documentarse en una completa Información activo registro (IAR). Sin esto, la organización será capaz de gestionar eficazmente los riesgos para su información, o de entender el impacto en el negocio de los cambios en los activos de	La información crítica para el negocio o datos personales es entendida y documentada, pero no incluye toda la información de valor para la Unidad.	3	La Organización debería llevar a cabo una auditoría de información para entender toda la información que tiene, no sólo centrándose en personales, sensibles o información crítica del negocio. Luego debe compilar un IAR comprensiva que detalla sus conclusiones y agrupar la información en activos manejables.
1,2	¿La Unidad está documentando y dando seguimiento a las siguientes características en un Registro de Activos de Información o similar?	Es vital que la organización entiende que la información que tiene, qué uso se requiere de él y cómo los procesos de gestión de tecnología e información deben apoyarlo. Sin esta comprensión continuidad digital puede perderse.	Donde se encuentra la información (por ejemplo, sistemas, equipos, presentación de lugares)	Yes	Los IAOs deberían revisar las secciones de la información activo registro regularmente, para que esté al día.
			Sus características técnicas (p. ej. información de formato de archivo)	No	Sin esta información la organización será incapaz de evaluar todos los riesgos derivados del cambio de tecnología u obsolescencia del formato. Herramientas como puede droide ayudan a comprender la gama de formatos de archivo celebradas.
			Plazos de Retención (tablas de plazo)	No	A menos que la organización entiende cuánto necesita para mantener la información, no puede asegurar que es almacenar y gestionar sólo la información que requiere. Esto no puede representar el uso más eficiente de los recursos limitados y puede hacer más difícil encontrar la información necesaria, administrar con eficacia y revisar información para la migración, la eliminación o la transferencia por ejemplo.
			Valor de Negocio	No	Si la organización no entiende el valor de negocio de la información, no puede asegurar es gestionarlo correctamente, apoyar adecuadamente o explotar eficientemente. También es más difícil priorizar la actividad de gestión del riesgo adecuada y
			Riesgo para el Negocio	No	A menos que los riesgos de registros de organización para el negocio, no se puede asegurar que son ser administrados adecuadamente y hay un aumento de la probabilidad que la organización va a experimentar pérdida de la continuidad digital.
			Requerimientos de usabilidad	No	Si la organización no graba los requisitos de usabilidad de la información, no puede asegurar que mantiene el correcto nivel de funcionalidad de su entorno de tI. Esto puede significar que la organización no es capaz de trabajar con la información requerida, o que el dinero se desperdicia proporciona funcionalidad que no es
			Propiedad	No	Cada activo de información debe tener un propietario que es responsable de él - esto incluye la rendición de cuentas para la adecuada gestión de la continuidad
			Restricciones de acceso y seguridad	Yes	Los IAOs deberían revisar las secciones de la IAR regularmente, para que esté al día.
			Sensibilidad de la información	Yes	Los IAOs deberían revisar sus secciones de la IAR regularmente, para que sea hasta la fecha, sobre todo teniendo en cuenta que la sensibilidad puede variar con el tiempo.
			Riesgos del activo	No	Si la organización no registra los riesgos del activo, no puede ser cierto que los riesgos son ser administrados adecuadamente en el tiempo y cambio y mitigación apropiadas y planes de contingencia puesto en marcha.
1,3	La Unidad tiene...	información digital puede ser difícil de manejar porque hay un elemento de incertidumbre que lo rodea. Esto puede ser información que no pertenece a un activo de información, cuyo uso propiedad o negocio no está claramente definido. Es importante que la información digital ha definido propiedad y propósito; Si no lo hace, puede ser retenido innecesariamente o no puede manejar de información vital sobre el cambio.	... información que no está cubierta por un activo de información	No	Mantener bajo revisión, particularmente como cambio de actividad o información es transferida a la organización.

			... Información que no tiene un objetivo claro de uso	Yes	Si la información no tiene un negocio claro uso, ya no puede ser necesario y chould ser desechados apropiadamente. La organización debe gestionar la información lleva a cabo y cumplir con todas las leyes (por ejemplo FOIA y DPA). Eliminación de información redundante en línea con programas de retención acordado puede proporcionar eficiencias.
			... Información que se sujeta o es propiedad de terceros	No	Mantener bajo revisión, particularmente como cambio de actividad o información es transferida a la organización.
1,4	**¿La Unidad entiende el valor de su información, el valor financiero y el uso que entrega a la empresa?**	Comprender el valor de la información que la organización lleva a cabo le permitirá gestionar la información y priorizar la gestión de continuidad digital en consecuencia, centrándose en la información de mayor valor. Sin organización el valor de la información, gestión de riesgos para la continuidad del digital no puede ser adecuadamente o rentable priorizado e información de alto valor puede permanecer en situación de riesgo.	La Unidad comprende el valor de toda su información, pero esto no se utiliza sistemáticamente como una herramienta para apoyar la gestión de su información.	3	La organización debe usar su entendimiento del valor de su información al evaluar el riesgo, la determinación de prioridades y toma de decisiones sobre gestión de la información.
1,5	**La Unidad necesita conservar su información por...**	Diferentes riesgos se aplican a diferentes edades de la información. Generalmente la información ya debe conservarse, mayor el riesgo de perder continuidad digital.	... un corto plazo solo para uso del negocio, es decir, por menos de 5 años	No	La Organización debería comprobar que no hay ningún requisito para almacenar su información.
			... un mediano plazo para apoyo a las operaciones del	No	
			... un largo plazo, de 10-30 años	No	
			... más de 30 años	Yes	La organización necesita una estrategia de preservación
1,6	**La Unidad tiene la información digital que...**	Si la organización no ha sido proteger su información contra la pérdida de continuidad digital, puede que ya haya perdido la capacidad de encontrar, abrir, trabajar con, entender o confiar en su información. Debe actuar inmediatamente para identificar pérdidas y restablecer la continuidad siempre que sea posible.	... no sabe la edad	No	Comprender la edad de la información digital es un aspecto de poder gestionar la continuidad de esa información. Esta continuación es posible alinear con los requerimientos del negocio para tecnología apoyo apropiada en lugar de como necesaria.
			... tiene más de cinco años	No	La organización es realmente probable que contienen la información que tiene más de 5 años. Por ejemplo, registros financieros. Para obtener información que es entre cinco y diez años de edad, el riesgo principal para la continuidad del digital es que la información ha sido mal manejada y no es entendido. Esto es particularmente un riesgo si se ha transferido la propiedad de la información. Esta información puede no ser bien entendido o fáciles de encontrar. La organización debe probar y riesgo evaluar la información, tomar medidas para mitigar el riesgo y restaurar la continuidad siempre que sea posible.
			.. tiene más de diez años	No	Organizaciones del sector público son capaces de mantener la información que tiene más de 10 años. Por ejemplo, los registros seleccionados para conservación permanente (en los archivos del nacional o local de registro), aunque dependiendo de procesos de gestión de información en el tiempo, estos pueden ser documentos de papel en lugar de digital. La organización debe revisar su información y comprobar también sus obligaciones.
			... tiene más de veinte años	No	La organización es probable que contenga información que tiene más de 20 años. Por ejemplo, salud y seguridad, gestión de fincas o registros de pensiones. Función de procesos de gestión de información en el tiempo, estos pueden ser registros de papel en lugar de digital. La organización debe revisar su información y comprobar también sus obligaciones.

1,7	**¿La Unidad entiende cómo necesita utilizar (buscar, abrir, trabajar con, entender y confiar en) sus activos de información, tanto ahora como en el futuro?**	Gestión de continuidad digital es garantizar que la organización puede utilizar su información en la forma que necesita, durante el tiempo que necesita. La organización debe definir sus requisitos de usabilidad para todos sus activos de información teniendo en cuenta cómo necesita encontrar, abrir, trabajar con, entender y confiar en la información, ahora y en el futuro. Sin esta comprensión, no será capaz de gestionar con eficacia continuidad digital y aumentan los riesgos de perder accidentalmente la posibilidad de utilizar la información.	La Unidad comprende algunos aspectos de sus requisitos de usabilidad, pero no completamente.	2	Los requisitos de uso para todos los activos deben ser identificados. Si se identifica la información sin un uso claro, hay una oportunidad para deshacerse de él.	
1,8	**La Unidad tiene la información que...**	Gestión de continuidad digital es garantizar que la organización puede utilizar su información en la forma que necesita, durante el tiempo que necesita. Estos tipos de información tienen requisitos de usabilidad muy específicas y puede haber graves consecuencias financieras y reputacionales para la organización si esta usabilidad se pierde.	... está conforme con la petición de libertad de información	Yes	Si la organización contiene información que es objeto de una solicitud de libertad de información, esto incluye cualquier información que ya no es utilizable debido a la gestión de la información pobre. La organización puede ser responsable de la recuperación de la información. Código de prácticas del Lord Canciller sobre la gestión de registros bajo el artículo 46 de la libertad de información ley 2000 asesora mejor práctica sobre gestión de la información, diciendo 'Las autoridades deben saber qué registros tienen y donde están y deben asegurarse de que sean utilizables para como sean necesarios'.	
			... requiera de consulta pública o investigaciones	Yes	Obligación de la organización a disposición de información digital para investigaciones y preguntas del público se solicita mientras mantiene la información. Una investigación podría tomar lugar años después se creó la información, y si no se encauza adecuadamente esta información podrían sufrir pérdida de continuidad digital. Podría haber consecuencias legales, financieras o de reputación si la organización no es capaz de proporcionar la información solicitada. Recuperación es a menudo costoso y no siempre es posible.	
			... está cubierta por la ley de protección de datos	Yes	Si la organización logra continuidad digital, tendrá confianza en que puede encontrarse la información necesaria para mantener la confianza pública en la organización y proteger su reputación, que es completa y en contexto y es digno de confianza. La organización debe manejar información digital adecuada y a un estándar auditable, en consonancia con los requisitos legales y directrices sobre prácticas idóneas. La responsabilidad de cuidar la información incluye información sobre los empleados y miembros del público en general, que está cubierto por la ley de protección de datos. La organización debe tomar especial cuidado para asegurarse de que mantenga la continuidad de la información cubierta por la ley de protección de datos si se va a seguir siendo obediente.	
			... puede requerir de evidencia legal o forense	Yes	Una vez que la organización ha identificado qué evidencia se requiere para producir, debe tener en cuenta cómo va a recuperar y hacer uso de esa información cuando sea necesario. Principios 9 y 10 de la guía de buenas prácticas de CESG en preparación forense se relacionan fuertemente con continuidad digital. Si la organización ha perdido la continuidad digital de su evidencia no se puede recuperar con eficacia y eficiencia o incluso potencialmente utilizar para fines probatorio.	
			... está sujeta a los actos de registros públicos	Yes	La organización debe asegurar que logra la continuidad de esta información hasta que es trasladado a un lugar permanente del depósito, como los archivos del nacional. Ya que es probable que para 20-30 años desde el punto de creación de información, esta información es probable que necesita gestión de continuidad digital particularmente cuidadoso.	

1,7	**¿La Unidad entiende cómo necesita utilizar (buscar, abrir, trabajar con, entender y confiar en) sus activos de información, tanto ahora como en el futuro?**	Gestión de continuidad digital es garantizar que la organización puede utilizar su información en la forma que necesita, durante el tiempo que necesita. La organización debe definir sus requisitos de usabilidad para todos sus activos de información teniendo en cuenta cómo necesita encontrar, abrir, trabajar con, entender y confiar en la información, ahora y en el futuro. Sin esta comprensión, no será capaz de gestionar con eficacia continuidad digital y aumentan los riesgos de perder accidentalmente la posibilidad de utilizar la información.	La Unidad comprende algunos aspectos de sus requisitos de usabilidad, pero no completamente.	2	Los requisitos de uso para todos los activos deben ser identificados. Si se identifica la información sin un uso claro, hay una oportunidad para deshacerse de él.	
1,8	**La Unidad tiene la información que...**	Gestión de continuidad digital es garantizar que la organización puede utilizar su información en la forma que necesita, durante el tiempo que necesita. Estos tipos de información tienen requisitos de usabilidad muy específicas y puede haber graves consecuencias financieras y reputacionales para la organización si esta usabilidad se pierde.	... está conforme con la petición de libertad de información	Yes	Si la organización contiene información que es objeto de una solicitud de libertad de información, esto incluye cualquier información que ya no es utilizable debido a la gestión de la información pobre. La organización puede ser responsable de la recuperación de la información. Código de prácticas del Lord Canciller sobre la gestión de registros bajo el artículo 46 de la libertad de información ley 2000 asesora mejor práctica sobre gestión de la información, diciendo 'Las autoridades deben saber qué registros tienen y donde están y deben asegurarse de que sean utilizables para como sean necesarios'.	
			... requiera de consulta pública o investigaciones	Yes	Obligación de la organización a disposición de información digital para investigaciones y preguntas del público se solicita mientras mantiene la información. Una investigación podría tomar lugar años después se creó la información, y si no se encauza adecuadamente esta información podrían sufrir pérdida de continuidad digital. Podría haber consecuencias legales, financieras o de reputación si la organización no es capaz de proporcionar la información solicitada. Recuperación es a menudo costoso y no siempre es posible.	
			... está cubierta por la ley de protección de datos	Yes	Si la organización logra continuidad digital, tendrá confianza en que puede encontrarse la información necesaria para mantener la confianza pública en la organización y proteger su reputación, que es completa y en contexto y es digno de confianza. La organización debe manejar información digital adecuada y a un estándar auditable, en consonancia con los requisitos legales y directrices sobre prácticas idóneas. La responsabilidad de cuidar la información incluye información sobre los empleados y miembros del público en general, que está cubierto por la ley de protección de datos. La organización debe tomar especial cuidado para asegurarse de que mantenga la continuidad de la información cubierta por la ley de protección de datos si se va a seguir siendo obediente.	
			... puede requerir de evidencia legal o forense	Yes	Una vez que la organización ha identificado qué evidencia se requiere para producir, debe tener en cuenta cómo va a recuperar y hacer uso de esa información cuando sea necesario. Principios 9 y 10 de la guía de buenas prácticas de CESG en preparación forense se relacionan fuertemente con continuidad digital. Si la organización ha perdido la continuidad digital de su evidencia no se puede recuperar con eficacia y eficiencia o incluso potencialmente utilizar para fines probatorio.	
			... está sujeta a los actos de registros públicos	Yes	La organización debe asegurar que logra la continuidad de esta información hasta que es trasladado a un lugar permanente del depósito, como los archivos del nacional. Ya que es probable que para 20-30 años desde el punto de creación de información, esta información es probable que necesita gestión de continuidad digital particularmente cuidadoso.	

2,1	**¿La Unidad entiende su entorno técnico?**	La organización debe entender su entorno técnico – la tecnología apoya y cómo ayuda a entregar los servicios que la organización requiere de él. Esto debe documentarse en una base de datos de gestión de configuración (CMDB) o equivalente y esta debe utilizarse para tomar decisiones y gestionar el cambio. Si no se entiende el entorno técnico, existe un mayor riesgo de que no sea capaz de proporcionar los requerimientos de usabilidad el negocio necesita de la información. También hay mayor riesgo que los cambios en el entorno técnico no será bien administrado, y continuidad digital perdió como resultado.	La Unidad tiene una comprensión de todos sus sistemas y cómo son interdependientes, pero no hay ninguna coordinación de documentación o de gestión	3	La organización debe documentar su comprensión del entorno técnico y utilizar esto para informar de su gestión e identificar áreas de riesgo o potenciales ahorros y eficiencias. Debe utilizarse también para comprender las dependencias técnicas de la organización activos de información.
2,2	**¿La Unidad entiende en qué formatos se almacena su información y las aplicaciones necesitan para usarlos?**	Es importante identificar no sólo aplicaciones, pero también tipos y versiones de formatos de archivo, ya que existen relaciones complejas entre ellos. Aplicaciones de la organización no pueden abrir los formatos de archivo que se sostiene, sobre todo si el formato es antiguo o no estándar. Si la organización no es asegurar que todos los formatos tiene puede ser utilizado por las aplicaciones disponibles, es un mayor riesgo de perder continuidad digital.	La Unidad entiende que todas las aplicaciones que utiliza, pero no los formatos específicos y versiones que posee o las aplicaciones de las cuales dependen para usarlos.	3	La organización necesita realizar una auditoría completa de sus formatos de archivo y determinar qué aplicaciones deben utilizan estos formatos. Esto permitirá identificar dependencias en tecnologías heredadas y a medida y donde la organización puede estar en riesgo de perder continuidad digital.
2,3	**¿La Unidad está documentando y rastreando las siguientes opciones en una CMDB (Base de datos de gestión de la configuración) o equivalente?**	Todas estas áreas deben ser documentados y referencias cruzadas de una manera que permite a la organización un seguimiento de dependencias y relaciones entre todos los elementos que componen el entorno de la tecnología. Este proceso también debe incluir referencia cruzada a la IAR para ver qué activos de las diferentes tecnologías de apoyo. Sin esta comprensión y asignación de la organización se pondrá mal para reaccionar para cambiar, no se puede ver rápidamente el impacto más amplio de cambios o fallos en elementos específicos.	You ticked 0 out of 14	0	La organización debe crear o ampliar su documentación para cubrir todas estas áreas de su entorno y asegurar que se mantiene hasta la fecha. La información debe utilizarse para apoyar la toma de decisiones y gestión del cambio.
2,4	**¿La Unidad entiende cómo el entorno técnico apoya sus requisitos de usabilidad de la información?**	Los requisitos de usabilidad de la información deben ser entendidos por todas las partes de la organización que están involucradas en su entrega. La organización debe asignar y rastrear las relaciones entre el entorno técnico y cómo apoya la utilidad de cada uno de sus activos de información. Esto permitirá a la organización evaluar rápidamente y con eficacia el impacto del cambio en la capacidad para utilizar información e identificar tecnologías redundantes. Si no tiene este conocimiento, hay riesgo que se introducirán cambios que afecta negativamente la capacidad de utilizar la información.	La Unidad entiende el entorno técnico y la usabilidad que proporciona, pero no está asignado al soporte de activos de información individuales.	3	La organización debe asignar y rastrear las relaciones entre el entorno técnico y cómo apoya la utilidad de cada uno de sus activos de información.
2,5	**¿La Unidad depende de tecnología obsoleta para cumplir con los requisitos de usabilidad de la información?**	Tecnología obsoleta aumenta riesgo de continuidad digital porque reduce la capacidad de responder a los cambios, y será cada vez más difícil y costoso de mantener y resolver problemas que se presentan. También tiende a ser más difíciles de extraer información de tecnología obsoleta, llevó a cabo a menudo en estructuras o formatos no estándar. La tecnología más obsoleta es izquierda no administrada, mayor será el riesgo y más difícil será para moverse lejos de.	La Unidad se basa en tecnología obsoleta administrada para entregar a los activos de información y hay una estrategia para migrar a otras tecnologías cuando sea posible	3	La Organización debería comprobar regularmente la continuidad y tratar de implementar sus estrategias para alejarse lo más pronto posible.
2,6	**¿La Unidad depende de tecnología hecha a la medida para ofrecer información de requisitos de usabilidad?**	Tecnología a medida aumenta el riesgo para la continuidad digital porque la organización es encerrada en una tecnología particular, proveedor o mantenimiento internos habilidades y conocimientos, crear dependencia en su continuo apoyo. Esto reduce la capacidad de responder a los cambios, y puede ser cada vez más difícil y costoso mantener el apoyo en el tiempo. Puede ser más difícil extraer información de la tecnología a medida, llevó a cabo a menudo en estructuras o formatos no estándar.	La Unidad depende de tecnología hecha a la medida para entregar a los activos de información, pero la tecnología está siendo apoyada durante la vida útil de los activos de información.	3	La organización debe considerar una estrategia para pasar a abrir o soluciones estándar.

2,7	**La Unidad tiene información...**	Estos tipos de opciones de almacenamiento de información cada tienen riesgos específicos asociados a ellos que podrían conducir a pérdidas de continuidad digital.	almacenada en medios externos o extraíbles (por ejemplo, tarjetas, USB llaves, cintas o discos duros externos)	Yes	Medios extraíbles son un riesgo para la continuidad digital porque los medios de comunicación pueden degradar horas extras lleva a corrupción o una completa incapacidad para acceder a la información. El hardware utilizado para leer los medios de comunicación también puede quedar obsoleto. Información almacenada en estos dispositivos también es difícil de encontrar si no es indexado y seguimiento.
			almacenada en discos locales de los usuarios individuales (por ejemplo, computadoras portátiles)	Yes	Información almacenada en discos locales de los usuarios individuales no será cubierta por la información y procesos de gestión de tecnología: se oculta de búsqueda corporativa herramientas, no puede ser respaldada y no será parte de los procesos de auditoría. Esta información estará en mayor riesgo de perder continuidad digital si no está sujeta a estrategias de gestión empresarial.
			almacenada en servidores de correo electrónico (incluyendo archivos adjuntos)	Yes	Almacenamiento de información en mensajes de correo electrónico aumenta el riesgo de que la información va a ser difícil encontrar y entender en el contexto en el cual se utiliza.
			almacenada en sistemas de gestión de documentos (Sharepoint, SGDEA)	Yes	Mientras que los sistemas de gestión de documentos pueden mejorar la encontrabilidad y manejar el contexto de la información (por ejemplo, metadatos), esto puede ser perdida cuando se transfiere información del sistema. Beneficios de estos sistemas pueden ser perdidos si no utilizados o configurados correctamente y los usuarios deben ser entrenados para no perder continuidad digital.
			almacenada en almacenamiento archivístico en línea (por ejemplo, archivos de correo electrónico)	Yes	Estos sistemas utilizan la gestión de las relaciones complejas para garantizar el acceso a la información, que debe ser gestionado y mantenido en el tiempo. Contenido y el contexto de la información debe gestionarse con cuidado cuando transfiere dentro y fuera de estos sistemas para no perder continuidad digital.
			almacenada en almacenamiento de archivo sin conexión	Yes	Almacenar información por largos períodos de almacenamiento de archiving sin uso regular aumenta el riesgo de que la continuidad digital se pierdan sin darse cuenta de la organización. La organización debe probar regularmente la capacidad para abrir y utilizar la información según sea necesario. La organización debe asegurar que la información está disponible en plazos aceptables para satisfacer las necesidades del negocio.
			guardada en entornos protegidos por contraseña o cifrado	Yes	Contraseñas y claves de cifrado deben ser cuidadosamente manejadas para asegurar que el acceso a la información no se pierda durante los cambios de personal. Los usuarios pueden introducir contraseña sin supervisión y políticas deben ser desarrolladas para esto.

C Administración

1 Gestión de Riesgo

1,1 ¿La Unidad considera los riesgos que corre su información como un riesgo empresarial significativo?

- ○ No.
- ○ Esto es reconocido como un riesgo, pero no hay estructuras definidas para la gobernanza de la información y la gestión de riesgos de la información.
- ◉ Los riesgos para la información personal y sensible están reconocidos y manejados; hay estructuras definidas para la gobernanza de la información y la gestión de riesgos de la información únicamente para este tipo de información.
- ○ Sí, este aspecto se reconoce como un riesgo significativo para la capacidad de funcionamiento de la Unidad.

1,2 ¿La pérdida de continuidad digital es reconocida y manejada como un riesgo clave de información corporativa?

- ○ No está reconocido.
- ○ Los riesgos para la continuidad digital son reconocidos, pero no formalmente reconocidos o gestionados como un riesgo significativo de la información.
- ◉ Los riesgos para la continuidad digital son reconocidos e incluidos en un registro de riesgos de información corporativa, pero no es activamente gestionado.
- ○ La pérdida de la continuidad digital está incluida en un registro de riesgos corporativos, gestión de incidencias e informes de procesos, y se toman las acciones apropiadas.

1,3 ¿Cómo gestiona la Unidad los incidentes de información?

- ○ La Unidad no administra incidentes de información ni tiene algún procedimiento para hacerlo.
- ◉ Los incidentes se manejan localmente cuando ocurren, pero la Unidad no ha establecido procesos corporativos de gestión de incidencias.
- ○ La Unidad ha establecido procesos de gestión de incidencias, pero sólo se utilizan para incidentes de pérdida de datos con datos personales y sensibles.
- ○ Sí, todos los tipos de incidentes de información son grabados y gestionados a través de procesos de gestión de incidentes establecidos y son escalados al nivel apropiado.

1,4 ¿La Unidad valora los riesgos de continuidad para activos de información individuales?

- ○ No se han evaluado los riesgos para los activos de información individuales.
- ◉ Podrían haber sido evaluados los riesgos de toda o parte de la información custodiada por unidades de negocio individuales
- ○ Ha sido evaluado el riesgo de todos los activos de información custodiados internamente, pero esto excluye activos administrados o custodiados entes externos.
- ○ Sí, todos los activos de información han sido riesgo evaluada continuidad digital.

1,5 ¿La Unidad realiza pruebas regularmente para comprobar la continuidad de sus activos de información?

- ○ Nunca.

- (●) La continuidad digital solo es probada después de cambios significativos que pueden haberla afectado.
- ( ) Se realizan inspecciones al azar de la continuidad digital de activos de información.
- ( ) Las pruebas de continuidad son parte del programa regular de la Unidad para el mantenimiento de la información y la tecnología

2 Gestión del Cambio

2,1 ¿La Unidad tiene un proceso de gestión de cambio definido?

- ( ) No.
- (●) Los procesos de gestión de cambio específico se establecen sobre una base caso por caso.
- ( ) Sí, para cambio técnico.
- ( ) Sí, para la gestión de todos los tipos de cambio a través de la Unidad.

2,2 ¿Las evaluaciones y pruebas de impacto de continuidad digital son componentes standard de la gestión del cambio?

- ( ) No.
- (●) El impacto en la continuidad digital no es parte del proceso estándar.
- ( ) Sólo se evalúa el impacto en la continuidad digital para cambios en la información de forma clave y a gran escala donde es obvio que habrá un impacto.
- ( ) Sí, las evaluaciones de impacto de continuidad digital y las pruebas se llevan a cabo como parte estándar del proceso de gestión de cambio.

2,3 ¿La Unidad espera experimentar algunos de los siguientes tipos de cambio en un futuro cercano?

- [ ] Cambios significativos o adiciones a la función del negocio (por ejemplo, reestructuración organizativa a gran escala o cierre).
- [ ] Importación o exportación de grandes volúmenes de información.
- [x] Introducción de nuevos registros o tecnología gestión de la información (SGDEA, Sharepoint).
- [ ] Cambio significativo de personal o nivel de recursos.
- [ ] Cambios significativos en el entorno tecnologico (por ejemplo, actualizar sistemas).
- [ ] Outsourcing de las Tecnologías de la Información, gestión de la información u otras funciones importantes para el negocio (por ejemplo, contratos o servicios compartidos).
- [ ] Expiración de importantes contratos o acuerdos de soporte.
- [ ] Reestructuración de la arquitectura de la información o sistemas importantes para el negocio (por ejemplo, combinar conjuntos de datos, o archivo plan reestructuración).
- [ ] Cambios en la legislación organizacional o en los requisitos reglamentarios (por ejemplo, cambios a la ley de archivos).

3 Gestión de Tecnología

3,1	¿La Unidad está administrando activamente el ciclo de vida de su tecnología, incluyendo el mantenimiento de contratos de soporte y planificación de las transiciones de final de la vida?	○ No hay comprensión del ciclo de vida de la tecnología y la Unidad no es eficaz en la administración de sostenibilidad del servicio ○ El ciclo de vida de algunos sistemas es claramente entendido y gestionado, pero esto no se aplica a todos los sistemas. ◉ La Unidad tiene una idea clara del ciclo de vida de la tecnología, pero no tiene un plan claro de las acciones que se tomarán al final de la vida para cada componente ○ La Unidad está gestionando el ciclo de vida de todos sus sistemas y tiene una hoja de ruta de la tecnología para todos los servicios, con un plan para brindar sostenibilidad del servicio.
3,2	La estrategia de Tecnologías de la Información incluyen:	☐ racionalización/reducción del número de sistemas y formatos ☑ normalización del entorno de TI – minimizar sistemas a medida, etc. ☑ uso de estándares abiertos, formatos y estructuras de datos ☑ requisitos de interoperabilidad a través de sistemas ☐ reducción de volúmenes de datos ☐ metodología de gestión de servicios para la entrega de TI
3,3	Está el requisito para la continuidad digital incorporado en la Unidad en ...	☐ Contratos informáticos y adquisición de nueva tecnología ☑ Desarrollo o modificación de los sistemas TIC ☐ Arquitecturas empresariales y técnicas ☑ Estrategias de almacenamiento ☐ Procesos de proyectos de TI y gestión del cambio
3,4	La Unidad gestiona las interdependencias de los distintos elementos dentro de su entorno técnico	○ No hay comprensión de cómo interactúan los diferentes elementos. ◉ Hay cierto entendimiento de las interacciones entre los sistemas clave del negocio, pero esto no es completo. ○ La Unidad utiliza una CMDB (Base de Datos) para realizar un seguimiento de las dependencias e interacciones de sus componentes de tecnología. ○ La Unidad utiliza una CMDB (Base de Datos) que incluye los activos de información y los elementos de configuración. Las utiliza para gestionar el cambio de la tecnología y la información.

3 Gestión de la Información

4,1	¿Existe una política vigente que le indique al personal donde guardar la información y cómo organizarla?	○ No, no hay ninguna política o procedimiento definido.

	○ No existe política, pero hay buena práctica esporádica a través de la Unidad. ◉ Hay una política vigente, pero no se entiende bien y su aplicación es adoptada inconstantemente. ○ Hay una política bien entendida y bien adoptada en toda la Unidad.
4,2 ¿Existe una política vigente para definir el nombre y descripción (metadatos) de los documentos?	○ No. ◉ No existe política, pero hay buena práctica esporádica a través de la Unidad. ○ Hay una política vigente, pero no se entiende bien y su aplicación es adoptada inconstantemente. ○ Hay una política bien entendida y bien adoptada en toda la Unidad.
4,3 ¿La Unidad tiene plazos de retención?	○ No, la Unidad no entiende cuánto tiempo necesita resguardar su información. ○ La Unidad no tiene tablas de plazos de retención, pero las unidades de negocio pueden administrar la retención y la eliminación de su información. ◉ Existen tablas de plazos de retención, pero no son aplicados o actualizados de forma sistemática. ○ Existen tablas de plazos de retención, se aplican y la información es gestionada y eliminada en forma acorde.
4,4 Los sistemas de gestión de la información le permiten a la Unidad…	☑ asegurar la información, aplicar controles de acceso ☐ aplicar control de versiones ☑ administrar el acceso al correo electrónico ☑ eliminar información ☑ declarar la información como expediente corporativo (institucional) ☑ aplicar los metadatos necesarios para encontrar y entender la información ☐ captura e Informe sobre logs de auditoría ☑ gestionar las relaciones entre o dentro de elementos de información (por ejemplo archivos adjuntos de correo electrónico) ☑ administrar la información general de datos, por ejemplo, formatos utilizados, espacio utilizado

	Administración				
	La Pregunta	**El Riesgo**	**Su Respuesta**	**Puntaje**	**Sus Acciones**
1,1	**¿La Unidad considera los riesgos que corre su información como un riesgo empresarial significativo?**	Información es un activo empresarial valioso. Sin este reconocimiento es poco probable que la organización va a tomar las medidas adecuadas para proteger su información mediante el establecimiento de control robusto de la información y las estructuras de gestión de	Los riesgos para la información personal y sensible están reconocidos y manejados; hay estructuras definidas para la gobernanza de la información y la gestión de riesgos de la información únicamente para este tipo de información.	3	La organización debe extenderse su gobernanza y estructuras de gestión de riesgo para cubrir todos sus activos de información. Es necesario identificar toda la información de valor para el negocio y establecer procesos de gestión de riesgos a este.
1,2	**¿La pérdida de continuidad digital es reconocida y manejada como un riesgo clave de información corporativa?**	Los riesgos para la continuidad digital son riesgos de la información como cualquier otro y representan una amenaza para la capacidad de la organización para utilizar su información digital. Estos riesgos deben reconocidos, documentados, tratados, revisados y escalados apropiadamente; Si no existe no es probable que el compromiso amplio de organización que es necesario garantizar que la información se gestiona	Los riesgos para la continuidad digital son reconocidos e incluidos en un registro de riesgos de información corporativa, pero no es activamente gestionado.	3	Riesgos de continuidad digital deben ser identificados, deben tomarse medidas supervisado y adecuado para su gestión. Incidentes de pérdida de la continuidad digital deben administrados y realiza un seguimiento según los procedimientos de gestión de incidentes de la organización.
1,3	**¿Cómo gestiona la Unidad los incidentes de información?**	La organización debe tener un proceso de gestión de incidencias que se utiliza para todos los incidentes que involucran información, incluso cuando hay una falla de continuidad digital. Si no se manejan incidentes de información, cuestiones no serán resueltas correctamente y pueden reaparecer.	Los incidentes se manejan localmente cuando ocurren, pero la Unidad no ha establecido procesos corporativos de gestión de incidencias.	2	Establecer un proceso de gestión de incidencias para la captura y seguimiento de todos los incidentes que involucran información, para que asuntos son administrados a través de resolución, lecciones para prevenir futuros problemas y mitigar el riesgo y las estadísticas están disponibles según sea necesario.
1,4	**¿La Unidad valora los riesgos de continuidad para activos de información individuales?**	Propietarios de activos de información (IAOs) son responsables de la gestión de los riesgos de sus activos de información, los que están en manos de terceros incluidos. Si activos individuales no son riesgo evaluado, los riesgos específicos no se entiende ni gestionados y pérdida de la continuidad digital es más probable.	Podrían haber sido evaluados los riesgos de toda o parte de la información custodiada por unidades de negocio individuales	2	Cada IAO formalmente debe evaluar los riesgos para sus activos de información. Esto debe también revisarse centralmente para coordinar acciones y gestión.
1,5	**¿La Unidad realiza pruebas regularmente para comprobar la continuidad de sus activos de información?**	Es extremadamente difícil restaurar la continuidad una vez que se ha perdido, y la dificultad aumenta con el tiempo. Es mucho más rentable para identificar pérdidas temprano, pruebas periódicas permitirán esto.	La continuidad digital solo es probada después de cambios significativos que pueden haberla afectado.	2	La organización debe comprobar regularmente la continuidad, esta incrustación dentro de cualquier procesos y horarios para la información y el mantenimiento de la tecnología existente. IAOs deberían probar regularmente para la continuidad de sus activos.
	Gestión del Cambio				
2,1	**¿La Unidad tiene un proceso de gestión de cambio definido?**	Sin procesos de gestión de cambio de una organización no es capaz de entender y mitigar los riesgos, a la continuidad digital. Un proceso bien definido e implementado permitirá a la organización evaluar y gestionar el impacto del cambio en la continuidad digital de la información.	Los procesos de gestión de cambio específico se establecen sobre una base caso por caso.	2	Ampliar procesos ad hoc en un acercamiento organizativo establecido para cambiar la gestión que se puede aplicar como un marco sobre una base caso-por-caso asegurar un enfoque coherente. Asegurar que las evaluaciones de impacto en la continuidad de los activos de información se llevan a cabo como una parte fundamental del proceso.
2,2	**¿Las evaluaciones y pruebas de impacto de continuidad digital son componentes standard de la gestión del cambio?**	Continuidad digital está más en peligro durante el cambio, es fundamental considerar el impacto en la información de todos los tipos y escalas de cambio. Esta evaluación de impacto debe ser una parte estándar del proceso de gestión de cambio de la organización.	El impacto en la continuidad digital no es parte del proceso estándar.	2	Las evaluaciones de impacto de continuidad digital deben realizarse para todos los cambios a través de la organización, y debe elaborarse un proceso estándar. Asegúrese de que está probado continuidad digital después de cambio.
2,3	**¿La Unidad espera experimentar algunos de los siguientes tipos de cambio en un futuro cercano?**	Cualquiera de estos cambios puede tener un impacto significativo en los requerimientos de usabilidad y requieren acciones específicas para asegurarse de que se mantenga la continuidad digital.	Cambios significativos o adiciones a la función del negocio (por ejemplo, reestructuración organizativa a gran escala o cierre).	No	
			Importación o exportación de grandes volúmenes de información.	No	
			Introducción de nuevos registros o tecnología gestión de la información (SGDEA, Sharepoint).	Yes	La organización debe asegurarse de que la nueva tecnología es capturar los metadatos requeridos, usando estándares abiertos donde sea posible. Asegurar que la información (con metadatos asociados) puede ser exportado desde el sistema cuando sea necesario para volver a utilizar o archivar.
			Cambio significativo de personal o nivel de recursos.	No	

			Cambios significativos en el entorno tecnológico (por ejemplo, actualizar sistemas).	No	
			Outsourcing de las Tecnologías de la Información, gestión de la información u otras funciones importantes para el negocio (por ejemplo, contratos o servicios compartidos).	No	
			Expiración de importantes contratos o acuerdos de soporte.	No	
			Reestructuración de la arquitectura de la información o sistemas importantes para el negocio (por ejemplo, combinar conjuntos de datos, o archivo plan reestructuración).	No	
			Cambios en la legislación organizacional o en los requisitos reglamentarios (por ejemplo, cambios a la ley de archivos).	No	
	Gestión de Tecnología				
3,1	**¿La Unidad está administrando activamente el ciclo de vida de su tecnología, incluyendo el mantenimiento de contratos de soporte y planificación de las transiciones de final de la vida?**	Entender que el ciclo de vida de tecnología asegurará que la organización puede apoyar requerimientos de usabilidad de la información y plan de cambio tecnológico más eficazmente. Si la organización no tiene planes para los ciclos de vida de la tecnología, corre el riesgo de que información atrapada en sistemas no gestionados de la herencia o.	La Unidad tiene una idea clara del ciclo de vida de la tecnología, pero no tiene un plan claro de las acciones que se tomarán al final de la vida para cada componente	3	La organización debe desarrollar un plan de tecnología para permitir planificación largo plazo, para que haya sostenibilidad de la prestación de servicios y decisiones están alineadas con las estrategias de negocio más amplias.
3,2	**La estrategia de Tecnologías de la Información incluyen:**	These are principles which, if included in the organisation's IT strategy, will over time ensure that the organisation is well placed to manage its digital continuity.	racionalización/reducción del número de sistemas y formatos	No	Reducir la complejidad del entorno de TI al minimizar el número de sistemas y formatos en uso será reducir los gastos generales, hacer cambio más fácil de administrar y mejorar la interoperabilidad.
			normalización del entorno de TI – minimizar sistemas a medida, etc.	Yes	Se debe reducir la dependencia de la organización en los sistemas a medida, tanto a través de optimizar los sistemas actuales y consideración durante la adquisición y desarrollo.
			uso de estándares abiertos, formatos y estructuras de datos	Yes	Estándares abiertos permitirá transición de información entre los sistemas más fácilmente y ampliar la elección de la tecnología disponible, evitando el bloqueo de privativo formatos y software.
			requisitos de interoperabilidad a través de sistemas	Yes	La organización debe estar comprometida con interoperabilidad a través de su entorno de ti, incluyendo tecnología suministrados por terceros, para asegurar que puede transferirse información entre sistemas para apoyar uso de negocio y continuidad digital.
			reducción de volúmenes de datos	No	Gestión eficaz de los datos para eliminar información innecesaria reducirá el volumen general. Esto hará más fácil para la organización encontrar y gestionar la información que necesita y reducir los costes y la complejidad asociados con el mantenimiento de la continuidad digital durante largos periodos.
			metodología de gestión de servicios para la entrega de TI	No	Es vital que el entorno de ti apoya uso de negocio de la información y que este requisito debe reflejarse en la aplicación de la metodología de gestión de servicio a través de todos los servicios de ti. Por ejemplo, clara comprensión de los requerimientos de continuidad digital, reflejada en el catálogo de servicios y administra a través de SLAs apropiados.
3,3	**Está el requisito para la continuidad digital incorporado en la Unidad en ...**	If digital continuity is not embedded at the highest levels of IT operations, it is unlikely to be given the consideration that is necessary. Without early visibility of digital continuity risks and requirements, it may be necessary to make expensive and difficult changes to systems in order to restore continuity at a later date.	Contratos informáticos y adquisición de nueva tecnología	No	Si la organización no garantiza requerimientos de continuidad digital se incluyen en los contratos y especificaciones iniciales al adquisición de nuevos sistemas, existe el riesgo que introducirá tecnología que no es compatible con lo que se necesita utilizar la información y no es flexible lo suficiente como para adaptarse a los cambios. El contrato debe incluir una comprensión de los activos de información implicados y un requisito para evaluar el impacto del cambio sobre
			Desarrollo o modificación de los sistemas TIC	Yes	

Anexo 2. *Gestión de Objetos Digitales en las Unidades de la Universidad de Costa Rica.*

A continuación se presenta un cuestionario que tiene como finalidad recopilar información general sobre la gestión de objetos digitales en distintas Unidades de la UCR.

Los datos recopilados en esta herramienta serán utilizados de forma confidencial, únicamente con fines de investigación y serán accedidos exclusivamente por miembros de la CIADi y los estudiantes Jorge Luis Mora Cerdas y Jéssica Barahona Chavarría, para el análisis correspondiente.

Nombre de la Unidad: _____

Pregunta	Respuesta
1. Aproximadamente, ¿Cuál es el volumen anual (en GB) de información que genera la Unidad? (puede tomar como referencia la información producida en el año 2021)	
2 ¿Cuál es el volumen aproximado (la cantidad) anual de objetos digitales (documentos textuales, audios, videos, fotografías, etc.) que producen?	
3. ¿Cuántos usuarios utilizan anualmente sus servicios de información? (funcionarios, profesores, investigadores, estudiantes, etc.)	
4 ¿Qué tipos de datos/ documentos/ información producen en su Unidad? (puede marcar varias opciones)	☐ Tipo de pregunta ☐ Textual ☐ Audio ☐ Video ☐ Fotografía ☐ Otra
5. Producción de objetos digitales en su Unidad:	1. Textual ☐ Menor producción ☐ Mediana producción ☐ Mayor producción ☐ No se producen 2. Audio ☐ Menor producción ☐ Mediana producción ☐ Mayor producción

Pregunta	Respuesta
	☐ No se producen 3. Video ☐ Menor producción ☐ Mediana producción ☐ Mayor producción ☐ No se producen 4. Fotografías ☐ Menor producción ☐ Mediana producción ☐ Mayor producción ☐ No se producen 5. Otros ☐ Menor producción ☐ Mediana producción ☐ Mayor producción ☐ No se producen
6. Seleccione el nivel de confidencialidad de la información que se produce en su Unidad (puede marcar varias opciones)	☐ Acceso Público ☐ Acceso Restringido ☐ Datos personales de acceso irrestricto (los contenidos en bases de datos públicas de acceso general, según dispongan leyes especiales y de conformidad con la finalidad para la cual estos datos fueron recabados) ☐ Datos personales de acceso restringido (los que, aun formando parte de registros de acceso al público, no son de acceso irrestricto por ser de interés solo para su titular o para la Administración Pública) ☐ Datos sensibles (información relativa al fuero íntimo de la persona, como por ejemplo los que revelen origen racial, opiniones políticas, convicciones religiosas o espirituales, condición socioeconómica, información biomédica o genética, vida y orientación sexual, entre otros) ☐ Otra
7. ¿Utilizan esquemas de metadatos descriptivos para los documentos producidos en su Unidad? ¿Cuál(es)?	
8. Los sistemas informáticos que utilizan en su Unidad ¿tienen interoperabilidad con otros sistemas? ¿Cuáles?	

Pregunta	Respuesta
9. ¿Qué estrategia(s) utilizan en su Unidad para el almacenamiento de la información digital?	☐ Propia de la Unidad (servidores propios, dispositivos de almacenamiento portátiles, etc.) ☐ Propia de la Institución (ej. Servidores Centro de Informática UCR) ☐ Externa contratada ☐ Otra
10. ¿Cuáles medios utilizan en su Unidad para almacenar los objetos digitales? (puede marcar varias opciones)	☐ Servidores institucionales ☐ Discos duros externos ☐ Computadoras personales ☐ Nube ☐ Otros dispositivos (llave maya, CD, DVD, etc.) ☐ Otra
11. ¿Qué tipo de software utilizan los sistemas con los que trabajan en su Unidad?	☐ Libre (puede ser usado, copiado, estudiado, mejorado y redistribuido sin limitaciones) ☐ Propietario (uso de licencias) ☐ Otra
12. ¿Qué tipo de seguridad se está implementando para el acceso a la información? (niveles de seguridad en distintas capas, etc.)	
13. ¿Tienen definidas tablas de acceso a la información? (conjunto de reglas que identifiquen derechos de acceso y el régimen de permisos y restricciones aplicables)	☐ Sí ☐ No ☐ Otra

Anexo 3. *Herramienta para la evaluación de aplicaciones tecnológicas desarrolladas para preservación y archivo digital.*

Sección	Pregunta	Tipo de respuesta
I. Información general	1.1. Nombre del Sistema	
	1.2. Nombre extendido	
	1.3. Institución / Empresa a cargo del Sistema	
	1.4. Tipo de software	☐ Libre ☐ Propietario ☐ No Indica
	1.5. ¿Es código abierto?	☐ Sí ☐ No ☐ No Indica
	1.6. Sitio web / contacto	
	1.7. ¿Cuenta con soporte y mantenimiento?	☐ Sí ☐ No ☐ No Indica
	1.8. Lenguaje de programación	
	1.9. ¿El sistema se basa en estándares internacionales?	
	1.10. Estándares en los que se basa	
	1.11. Versión actual	
	1.12. Versiones anteriores	
II. Funciones del Sistema	2.1. Funciones principales del Sistema	
	2.2. Módulos con los que cuenta	
	2.3. Interoperabilidad con otros sistemas	☐ Sí ☐ No ☐ No Indica
	2.4. Sistemas con los que interopera	
	2.5. ¿Permite la firma digital certificada?	☐ Sí ☐ No ☐ No Indica

Sección	Pregunta	Tipo de respuesta
III. Ingreso de información	3.1. ¿Permite recibir y recoger SIP desde otros sistemas?	☐ Sí ☐ No ☐ No Indica
	3.2. ¿Genera los metadatos necesarios para los paquetes de información (SIP, AIP y DIP)?	☐ Sí ☐ No ☐ No Indica
	3.3. ¿Permite almacenar los AIP de forma segura?	☐ Sí ☐ No ☐ No Indica
	3.4. ¿Permite extraer información descriptiva de los AIP para consulta?	☐ Sí ☐ No ☐ No Indica
	3.5. ¿Genera notificaciones y bitácoras?	☐ Sí ☐ No ☐ No Indica
	3.6. ¿Permite el uso de formatos accesibles? (código abierto, no dependencia de terceros)	☐ Sí ☐ No ☐ No Indica
	3.7. ¿Permite la estabilidad y compatibilidad? (funcionalidad e integridad del formato con versiones posteriores)	☐ Sí ☐ No ☐ No Indica
	3.8. ¿Permite la estandarización y uso de formatos normalizados?	☐ Sí ☐ No ☐ No Indica
IV. Acceso dentro del Sistema	4.1. ¿Permite el acceso a diferentes niveles? (documento, expediente)	☐ Sí ☐ No ☐ No Indica
	4.2. ¿Se pueden realizar búsquedas por contenido y metadatos del documento y el AIP?	☐ Sí ☐ No ☐ No Indica
	4.3. ¿Permite visualizar copias de los documentos sin software especializado?	☐ Sí ☐ No ☐ No Indica

Sección	Pregunta	Tipo de respuesta
	4.4. ¿Genera registros de eventos y notificaciones?	☐ Sí ☐ No ☐ No Indica
	4.5. ¿Se pueden generar DIP a partir del procesamiento del contenido y metadatos de los AIP?	☐ Sí ☐ No ☐ No Indica
V. Seguridad	5.1. Almacenamiento (Base de datos. Unidades lógicas en uno o más servidores)	
	5.2. Medios de almacenamiento	☐ Servidores del cliente ☐ Servicio de almacenamiento en la nube ☐ Otra
	5.3. Protocolo (XML-SOAP Web Services Integration)	☐ Sí ☐ No ☐ No Indica
	5.4. ¿Permite realizar respaldos de la información almacenada?	☐ Sí ☐ No ☐ No Indica
	5.5. ¿Permite personalizar la configuración de seguridad y trazabilidad de las acciones?	☐ Sí ☐ No ☐ No Indica
	5.6. ¿Permite definir perfiles y roles de usuarios?	☐ Sí ☐ No ☐ No Indica