

PREDECI MODELO DE PRESERVACIÓN DE EVIDENCIA DIGITAL



www.cidepro.org

Fernando Tiverio Molina Granja
Juan Carlos Santillán Lima
Washington Gilberto Luna Encalada
Raúl Marcelo Lozada Yáñez

Fernando Tiverio Molina Granja
Juan Carlos Santillán Lima
Washington Gilberto Luna Encalada
Raúl Marcelo Lozada Yáñez

PREDECI
MODELO DE PRESERVACIÓN
DE EVIDENCIA DIGITAL

PREDECI
DIGITAL EVIDENCE PRESERVATION MODEL

Fernando Tiverio Molina Granja
Juan Carlos Santillán Lima
Washington Gilberto Luna Encalada
Raúl Marcelo Lozada Yáñez

Predeci
Modelo de preservación de evidencia digital

Predeci
Digital evidence preservation model



Autores:

Fernando Tiverio Molina Granja

Facultad de Ingeniería

Universidad Nacional de Chimborazo

fmolina@unach.edu.ec

 <https://orcid.org/0000-0003-2486-894X>

Washington Gilberto Luna Encalada

Facultad de Informática y Electrónica

Escuela Superior Politécnica

de Chimborazo

wluna@esPOCH.edu.ec

 <https://orcid.org/0000-0001-8412-9554>

Juan Carlos Santillán Lima

Facultad de Informática

Facultad de Ingeniería - LEICI

Instituto de Investigaciones en

Electrónica, Control y Procesamiento
de Señales

Universidad Nacional de La Plata

Becario SENESCYT

juancarlos.santillanl@info.unlp.edu.ar

jsantillanlima@ext.ing.unlp.edu.ar

 <https://orcid.org/0000-0001-5812-7766>

Raúl Marcelo Lozada Yáñez

Facultad de Informática y Electrónica

Escuela Superior Politécnica

de Chimborazo

raul.lozada@esPOCH.edu.ec

 <https://orcid.org/0000-0001-9245-0858>

Advertencia: Está prohibido, bajo las sanciones penales vigentes que ninguna parte de este libro puede ser reproducida, grabada en sistemas de almacenamiento o transmitida en forma alguna ni por cualquier procedimiento, ya sea electrónico, mecánico, reprográfico, magnético o cualquier otro sin autorización previa y por escrito del Centro de Investigación y Desarrollo Profesional (CIDEPRO).



Primera Edición, julio 2020

Predeci

Modelo de preservación de evidencia digital

ISBN: 978-9942-823-46-5 (eBook)

ISSN: 2600-5719 (electronic)

<https://doi.org/10.29018/978-9942-823-46-5>

Editado por:

Centro de Investigación y Desarrollo Profesional

© **CIDEPRO Editorial 2020**

Babahoyo, Ecuador

Móvil - (WhatsApp): (+593) 9 8 52-92-824

www.cidepro.org

E-mail: editorial@cidepro.org

Este texto ha sido sometido a un proceso de evaluación por pares externos con base en la normativa editorial de CIDEPRO.

Diseño y diagramación:

CIDEPRO Editorial

Diseño, montaje y producción editorial:

CIDEPRO Editorial

Hecho en Ecuador

Made in Ecuador

ÍNDICE

PREFACIO	XI
----------------	----

PREFACE.....	XV
--------------	----

CAPÍTULO 1

JUSTIFICACIÓN DEL MODELO	19
--------------------------------	----

Justificación teórica.....	19
----------------------------	----

Justificación práctica	27
------------------------------	----

Marco filosófico o epistemológico.....	34
--	----

Los repositorios como nuevo paradigma	37
---	----

CAPÍTULO 2

FUNDAMENTO TEÓRICO	43
--------------------------	----

Repositorios institucionales	43
------------------------------------	----

Interoperabilidad, recolección, difusión y accesibilidad	44
--	----

Beneficios de los repositorios institucionales	44
--	----

Proyectos sobre preservación digital	45
--	----

InterPARES	45
------------------	----

Planets	46
---------------	----

OAIS	47
------------	----

El modelo de información OAIS	49
-------------------------------------	----

Las entidades funcionales de un archivo OAIS	50
--	----

Ingesta	52
---------------	----

Almacenamiento de archivo	53
---------------------------------	----

Gestión de datos	55
------------------------	----

Administración	56
----------------------	----

Planificación de la preservación	57
Acceso	58
Metadatos	59
Conceptualización y categorización	63
Premis	65
Mets	68
Taxonomía de metadatos de preservación	74
La preservación digital.....	84
Amenazas y Estrategias	88
Riesgos de preservación digital	90
Metas de preservación digital	91
Metodologías de preservación digital	92
Opciones metodológicas	93
Preservación Bit	102
Museos informáticos.....	103
Evidencia digital	104
Aspectos relativos a la evidencia	104
Principios relativos a la evaluación de la evidencia digital	105
Principios de los procedimientos relativos a la evidencia digital ...	106
Características de la evidencia.....	108
Preservación de evidencia	109
Integridad probatoria.....	110
Admisibilidad	111
Normativa legal de admisibilidad de la evidencia	115
Legislación internacional	117

CAPÍTULO 3

MODELO CONCEPTUAL DE PRESERVACIÓN DIGITAL APLICABLE A LA MEJORA DE LA PRESERVACIÓN DE EVIDENCIA DIGITAL EN INSTITUCIONES DE INVESTIGACIÓN CRIMINAL - PREDECI.....	125
Propósito y alcance	125
Aplicabilidad	129
Justificación.....	129
Ambiente predecí	131
Funciones tomadas de OAIS.....	133
Modelo funcional.....	134
Descripción detallada de las entidades funcionales	138
Función ingesta	139
Función almacenamiento	143
Función de gestión de datos.....	147
Entidad funcional administración	149
Entidad Plan de Preservación.....	152
Función acceso.....	155
Diagramas de flujo de datos.....	157
Relaciones de las entidades funcionales	159

CAPÍTULO 4

GUÍA DE IMPLEMENTACIÓN	161
Guía de implementación del modelo Predecí	161
Nivel 1: Plan de implementación.....	161
Nivel 2: Plan de desarrollo.....	161
Nivel 3: Plan de evaluación de la implementación.....	163
Proceso de aplicación de la guía de implementación del modelo Predecí.....	163
Nivel 1: Plan de implementación.....	163
Nivel 2: Plan de desarrollo.....	166
Nivel 3: Plan de evaluación de la implementación.....	182
Consideración de Capacitación.....	183
Consideración del informe final.....	184
Flujo de trabajo de la guía.....	184
Glosario de términos	185
Siglas y abreviaturas	198
ACERCA DE LOS AUTORES	200
REFERENCIAS BIBLIOGRÁFICAS.....	205

PREFACIO

Actualmente, todo dispositivo digital es parte de las actividades de una persona o institución y es capaz de generar información que puede convertirse en evidencia valiosa en caso de presentarse un incidente de seguridad; ya sea entre muchas otras en forma de una fotografía, documento, registro de geo-localización, mensaje de texto, correo electrónico o incluso un número telefónico registrado como parte de una llamada. Esta evidencia es útil para investigar casos relacionados con actividades cibercriminales o de ataques informáticos, el problema es que muchas veces la recolección, el manejo y la preservación de esta información no se realizan de manera adecuada. (Martínez, 2012)

Para que esta información se convierta en evidencia se debe aplicar los procesos de informática forense. Esta actividad permite recuperar, preservar y presentar datos que han sido procesados electrónicamente y almacenados en un sistema informático que podrán ser utilizados como evidencia en un proceso judicial.

Una vez que se ha obtenido la información de los dispositivos es muy importante mantener y preservar dicha información desde que inicia el proceso, durante la investigación y hasta que finalice el juicio o la investigación para garantizar que no exista contaminación, daño, alteración o manipulación de la evidencia y de esta forma mantener la confiabilidad en el proceso.

Dentro de los procesos de preservación de las entidades o instituciones que tienen la responsabilidad de custodiar datos a largo plazo, se encuentra la preservación digital, interviniendo para ello técnicas y destrezas del campo de las ciencias de la información y de la informática.

Uno de los beneficios de la preservación digital es lograr que el material digital de dichas entidades sea accesible informacionalmente en el tiempo, independientemente si este material digital disponible fuese creado digitalmente desde su origen o generado a partir de material analógico. Las entidades y/o personas que requieran preservar material digital pueden ser hospitales, bibliotecas, museos, fiscalías, instituciones de investigación criminal o cualquier otra entidad que tenga la responsabilidad u obligación legal de custodiar datos digitales.

La preservación digital dentro de las implicaciones históricas, tiene afección directa a la herencia cultural, pues sin información (digital o no) que se custodie, no hay herencia ni cultura, pero sin tecnología que permita la preservación o recuperación de dicha información, tampoco lo habría.

En el ámbito forense, la preservación de la evidencia digital es un aspecto de especial importancia al momento de decidir la admisibilidad en un proceso judicial vigente, o en un futuro proceso, reabierto por apelaciones, por ejemplo, o como fuente de información histórica.

Aunque el primer motivo que le habrá llevado a la recopilación de evidencias sobre el incidente sea la resolución del mismo, puede que las necesite posteriormente para iniciar un proceso judicial contra sus atacantes y en tal caso deberá documentar de forma clara cómo ha sido preservada la evidencia tras la recopilación. o, probablemente se requiera reabrir el caso en un futuro, o se requiera información para otros procesos judiciales como referencia de juzgamiento. En este proceso, es imprescindible definir métodos, procedimientos y modelos adecuados para el manejo de la evidencia. Finalmente, las implicaciones tecnológicas, tienen un impacto elevado en la preservación digital, pues afecta tanto a los diferentes procesos como al modelo de preservación de datos en una unidad de información.

En una institución que realice procesos de preservación digital, si no se dispone de la tecnología adecuada que permita dar soporte a la preservación de datos, no se podrán ejecutar dichos procesos de preservación. En cualquier caso, no hay un modelo tecnológico establecido generalmente aceptado, aunque sí se han creado estándares y criterios prácticos. (LeFurgy, 2009)

La relación entre las implicaciones sociales, históricas, económicas y tecnológicas hacen que la preservación digital obtenga un reconocimiento como un área importante de investigación, enmarcada en las ciencias de la información y de la informática, debido a las implicaciones informacionales y tecnológicas que existen.

En el caso particular de las instituciones de investigación criminal, existe un vacío que esta investigación pretende ayudar a cubrir. Este libro propone un modelo a seguir para preservar la evidencia digital, que permita garantizar de mejor manera la integridad y aumentar la admisibilidad de la evidencia, apoyado en técnicas de preservación a largo plazo, enfocado en la gestión de los archivos.

PREFACE

Today, every digital device is part of the activities of a person or institution and is capable of generating information that can become valuable evidence in the event of a security incident; whether it be in the form of a photograph, document, geo-location record, text message, email or even a phone number registered as part of a call, among many others. This evidence is useful to investigate cases related to cyber-criminal activities or computer attacks, the problem is that many times the collection, management and preservation of this information is not done properly (Martínez, 2012).

For this information to become evidence, computer forensic processes must be applied. This activity allows for the recovery, preservation and presentation of data that has been electronically processed and stored in a computer system that can be used as evidence in a judicial process.

Once the information has been obtained from the devices it is very important to maintain and preserve this information from the beginning of the process, during the investigation and until the end of the trial or investigation to ensure that there is no contamination, damage, alteration or manipulation of the evidence and thus maintain the reliability of the process.

Within the preservation processes of the entities or institutions that have the responsibility to safeguard data in the long term, there is digital preservation, involving techniques and skills from the field

of information science and computer science. One of the benefits of digital preservation is to make the digital material of such organisations accessible through information over time, regardless of whether this available digital material was created digitally from its source or generated from analogue material. Entities and/or individuals requiring digital preservation may include hospitals, libraries, museums, prosecutors' offices, criminal investigation institutions or any other entity that has a legal responsibility or obligation to safeguard digital data.

Digital preservation, within the historical implications, has a direct effect on cultural heritage, because without information (digital or not) that is guarded, there is no heritage or culture, but without technology that allows the preservation or recovery of such information, there would not be either.

In the forensic field, the preservation of digital evidence is an aspect of special importance when deciding on the admissibility in a current judicial process, or in a future process, reopened by appeals, for example, or as a source of historical information. Although the first reason you may have collected evidence about the incident is to resolve it, you may need it later to initiate legal proceedings against your attackers and in that case you should clearly document how the evidence has been preserved after collection. Or, you may need to reopen the case in the future, or you may need information for other legal proceedings as a trial reference. In this process, it is essential to

define appropriate methods, procedures and models for handling the evidence. Finally, the technological implications have a high impact on digital preservation, as they affect both the different processes and the model of data preservation in an information unit.

In an institution that carries out digital preservation processes, if the appropriate technology is not available to support the preservation of data, it will not be possible to carry out these preservation processes. In any case, there is no established generally accepted technological model, although practical standards and criteria have been developed. (LeFurgy, 2009).

The relationship between social, historical, economic and technological implications means that digital preservation is recognised as an important area of research within the information and computer sciences because of the information and technological implications involved.

In the particular case of criminal investigation institutions, there is a gap that this research aims to help fill. This book proposes a model to follow for the preservation of digital evidence, in order to better guarantee the integrity and increase the admissibility of the evidence, supported by long-term preservation techniques, focused on the management of archives.



JUSTIFICACIÓN DEL MODELO



Capítulo 1

JUSTIFICACIÓN DEL MODELO

Justificación teórica

La UNESCO, indica “El patrimonio digital no está sujeto a límites temporales, geográficos, culturales o de formato. Aunque sea específico de una cultura, cualquier persona del mundo es un usuario en potencia. Las minorías pueden dirigirse a las mayorías y los individuos a un público de dimensión mundial. Hay que preservar y poner a disposición de cualquier persona el patrimonio digital de todas las regiones, naciones y comunidades a fin de propiciar, con el tiempo, una representación de todos los pueblos, naciones, culturas e idiomas”. (UNESCO, 2004)

La Alianza Nacional de Administración Digital (NDSA), es un consorcio de instituciones que están comprometidas con la preservación de largo plazo de la información digital, en el 2014, menciona que la efectiva preservación digital es vital para mantener los registros necesarios para comprender y evaluar las acciones del gobierno, la base de evidencia científica para replicar los experimentos, basándose en el conocimiento previo y la preservación del patrimonio cultural de la nación. (National Digital Stewardship Alliance, 2014)

Es necesario un trabajo sustancial para asegurar que el contenido digital de hoy sigue siendo accesible, útil y comprensible en el futuro, independientemente de su manera de creación.

La evidencia digital plantea retos particulares a la ICC. Esta evidencia digital es, en general, la información transmitida o almacenada en un formato digital que puede usar en un procedimiento de un caso judicial. La evidencia digital puede venir en forma de fotografías, vídeos y grabaciones de audio, correos electrónicos, blogs y redes sociales. Como la evidencia digital se vuelve más frecuente, la ICC debe considerar cómo responder a su uso.

El uso cada vez mayor de la evidencia digital en los procesos ofrece nuevas oportunidades y desafíos. Un e-mail, una interceptación de las comunicaciones por satélite, o una grabación digital de eventos en vivo pueden ayudar a establecer un vínculo de evidencia entre el acusado y la comisión de un crimen internacional. Dependiendo de la autenticidad de los datos, la evidencia digital también puede proporcionar información sobre el tiempo, el lugar y la forma de un evento para complementar la evidencia viva voz o testimonio vivo.

Sin embargo, la evidencia digital también puede ser alterado o degradado. Además, la evidencia digital se separó de su fuente; por ejemplo, una fotografía captura un solo punto de vista de un lugar en un momento determinado, y del mismo modo, una dirección de correo no captura el porte o el tono de voz del autor. (Ashoore, Bower, & Warden, 2013)

En los últimos años se ha multiplicado los documentos digitales, su uso entre los diferentes sectores de la sociedad y la tipología de

documentos, así también surgieron diferentes propuestas aunque las bibliotecas internacionales no se pusieron de acuerdo en cuanto al método más adecuado, si acordaron en cuanto a la necesidad de poner en común unas normas básicas y una lista de tareas adecuadas para la puesta en marcha de un programa de digitalización de archivos, surge el modelo Open Archival Information System (OAIS) (Consultative Committee for Space Data Systems, 2002), como modelo de referencia conceptual que establece las seis funciones de un sistema integral de preservación de documentos digitales a largo plazo. (Térmens, 2009)

La importancia de la publicación de este modelo radica en su estandarización en la ISO 14721 (International Organization for Standardization, 2012), que empezaría a materializarse en proyectos concretos, aunque el objetivo principal sea la preservación a largo plazo, la comunidad científica se ha planteado también otros problemas asociados: garantizar los principios de originalidad (la unicidad del documento) e integridad (que el documento no haya sido modificado ni alterado) del objeto, y de la información misma cuando éste sea migrado, modificado o cambiado de soporte.

Hoy en día, las opciones dentro de la preservación digital más aplicadas son la preservación de la tecnología, la migración de formatos antiguos a otros más nuevos, la emulación mediante software actual de software anterior, los metadatos y, la más sencilla y de menor coste, la replicación o copiado de la información. Ninguno de ellos se impone sobre los otros, puesto que la preservación es un campo todavía en

desarrollo y no todas las entidades tienen las mismas necesidades. (Serra, 2001) y (Térmens, 2009)

Con cada uno de estos métodos surgieron también proyectos diferentes, que las distintas bibliotecas nacionales o universitarias pusieron en marcha cuando empezaba a ser evidente que el volumen de información digital seguiría creciendo y sería necesario preservarlo.

Entre ellos destacaron por ser pioneros InterPARES (The International Research on Permanent Authentic Records in Electronic Systems, 2013), PREMIS (PREMIS Data Dictionary, 2012), PADI (PANDORA, Australia's Web Archive, 2011), PLANETS (Open Planets Foundation , 2010) y LOCKSS (The LOCKSS Program, 2004). No se ha definido aún qué recursos deben ser preservados, dependerá de la institución y la regulación del país, así como el de los derechos de autor en el documento nacido digital, ya que todavía no existe una solución definitiva.

Según Torres, no se han desarrollado las herramientas necesarias para construir un sistema de preservación digital a largo plazo, aunque sí se han llevado a cabo estrategias de preservación digital que no son la solución definitiva. Añade además que los especialistas de la información no poseen las aptitudes necesarias para desarrollar estas herramientas y necesitan “aliarse de forma mucho más entusiasta con los informáticos” para que la preservación digital pueda ser un hecho. (Torres Freixinet, 2008)

La información digital tiene un importante valor económico como producto cultural y como fuente de conocimiento.

Desempeña además un papel muy significativo en el desarrollo sostenible a nivel nacional, teniendo en cuenta que habitualmente los datos personales, gubernamentales y comerciales se crean en forma digital. La desaparición de este patrimonio generará empobrecimiento económico y cultural y dificultará el avance del conocimiento. (Gladney H., 2011)

Indica, además, que no se ha avanzado nada en la puesta en práctica de métodos para la preservación digital y los científicos aun trabajan en esta teoría. “No hay una solución o conjunto de soluciones claras para confrontar los desafíos de la preservación digital. El impredecible desarrollo tecnológico (...) y el del entorno político (...) contribuyen al reto de plantear el curso que seguirán”.

James Tetteh Ami-Narh, indica que “se espera que el investigador forense sea competente en el uso de una variedad de herramientas forenses y de asegurar que todos los procesos de investigación forense se llevan a cabo dentro del marco legal aceptado del sistema judicial.

Las áreas identificadas como las más propensas a ser cuestionada en un caso legal eran la jurisdicción del caso, la búsqueda y captura, la expoliación de evidencia, la preservación de las evidencias, el examen y análisis de las evidencias. Además, las trampas más comunes y rectificaciones sugeridas para errores en el proceso podrían ser investigados”. (Ami-Narh, 2008)

Otra cuestión crítica a considerar es la falta de depósitos adecuados para el resguardo de este tipo de material probatorio, en función de los cuidados especiales y espacio físico que requieren los elementos tecnológicos, siendo habitual que las típicas oficinas de secuestros no alcancen los requisitos mínimos para garantizar la correcta preservación de las fuentes de evidencia digital (Gómez L. , 2013). Se indica, además, que una dirección para la investigación proporciona una profundidad insuficiente para una evaluación detallada.

Aquellas instituciones que actualmente realizan propuestas de preservación digital emplean sistemas grandes y costosos. La gran mayoría de ellas aplica el modelo Open Archival Information System (OAIS) (Consultative Committee for Space Data Systems, 2002), para la preservación de sus datos digitales. Un aspecto relevante de esta investigación es la de estudiar si el modelo actual de referencia OAIS (Consultative Committee for Space Data Systems, 2012) es adaptable a cualquier institución. Desde la propia comunidad científica se ha planteado esta necesidad de documentación complementaria para pequeñas instituciones bajo el nombre de OAIS-LITE. (Allinson, 2006)

Existen modelos para entornos específicos, como bibliotecas, archivos, instituciones sanitarias, todos basados en estándares y modelos generalmente aceptados, pero para su aplicabilidad en otros entornos tienen algunas limitaciones clave que se resumen a continuación:

- Tienden a centrarse en las características y la grabación de eventos de forma estática, en lugar de en el apoyo a los procesos de conservación dinámica. Por ejemplo. PREMIS, de forma deliberada, sólo se describe la información y los objetos de datos almacenados en un repositorio OAIS, en lugar de la interacción de los servicios de preservación digital y todo el ciclo de vida. (Dappart A. , 2013)
- Se centran únicamente en restricciones técnicas, en lugar de considerar el contexto global. Las actividades de preservación digital sólo pueden tener éxito si van más allá de las propiedades técnicas de los objetos digitales. Se deben tener en cuenta las propiedades que abarcan una amplia gama de factores que influyen y preservación guía los procesos, incluidos los de organización, reglamentarios, legales y financieros que se capturan como estrategia y política metas y limitaciones de la institución que los compromete. Deben tener en cuenta el marco cultural e institucional en el que se conservan los datos, documentos y registros. Por otra parte, dado que las organizaciones difieren en muchos aspectos, un enfoque de talla única para todos no puede ser apropiado. (Dappart A. , 2013)
- Se limitan a ciertos tipos de objetos digitales, por ejemplo, a los archivos en lugar de conjuntos de archivos que crean las entregas de objetos lógicos, objetos abstractos, como entidades intelectuales y colecciones, o pilas de renderizado completas.

En el caso más simple, la preservación de archivos, sin embargo, también requiere la preservación de la información de representación que es necesario para comprender los objetos de preservación en el futuro. Incluso en el caso más simple de esta información la representación es mucho más complejo que simples archivos, y requiere la capacidad de preservar objetos complejos. (Dappart A. , 2013)

- Según el estudio “Comparison of Methods & Costs of Digital Preservation” (Hendley, 1998), Se centran en determinados enfoques de solución, como la migración o emulación, exclusivamente. Un enfoque que, por ejemplo, se centra en la conservación de las propiedades técnicas de los archivos digitales se limitan las opciones de acciones de preservación y no refleja plenamente las actividades de preservación.
- En la práctica, nos encontramos con que no sólo las propiedades de los “objetos digitales”, sino también las propiedades de los entornos en los que existan, guían los procesos de preservación digital. Por lo tanto, es necesario que los objetos digitales de conservación y los entornos se consideren parte de la información a preservar. Los modelos que no tienen esta característica limita la elección de las acciones de preservación. El establecimiento de esta característica permite tratar la preservación de los objetos y su entorno o una combinación de ellos. (Dappart A. , 2013)

- Algunos modelos describen interacciones funcionales en un nivel alto. Por ejemplo, OAIS (CCSD, 2012) no admite suficientemente modelización de la interacción de preservación para capturar el intercambio de información necesario.
- Tienden a describir soluciones absolutas, en lugar de hacerlos en relación con el riesgo real y las metas de la organización, tal como se expresa en sus políticas. Las organizaciones utilizan el análisis basado en el riesgo (por ejemplo, Drambora (McHugh, Innocenti, & Ross, 2008)) para sus estrategias de preservación, las políticas y la planificación de la conservación. Combinan la información sobre los riesgos con una comprensión de las acciones que se esperan para mitigar el riesgo. Especificaciones de riesgo y acciones pueden depender de las propiedades de las acciones de preservación, así como en propiedades de los objetos de conservación o entornos que forman la entrada y salida de las acciones de preservación. Los riesgos, las acciones y las limitaciones son entidades de primer nivel en este modelo. Todos los modelos considerados parciales han dado lugar al desarrollo de soluciones prácticas que no coinciden y que ignoran aspectos importantes del dominio que deben tenerse en cuenta.

Justificación práctica

Las instituciones de investigación criminal actualmente reciben y gestionan documentos digitales de forma creciente. Las buenas prácticas de gestión de documentos requieren un modelo que permita

que se apliquen las mismas reglas y principios a todos los documentos independientemente del soporte o el formato.

Sin embargo, los documentos en formato digital tienen algunas características únicas que exigen que se realicen acciones concretas para asegurar que preserven su valor todo el tiempo que sean necesarios.

Es común que, durante los secuestros de material informático, no se tenga en cuenta la fragilidad de los medios de almacenamiento de datos y la volatilidad de la información. Sobre este aspecto, cabe destacar que existe una gran falencia en lo que se conoce como la cadena de custodia, cuyo objetivo consiste en mantener un registro de todas las operaciones que se realizan sobre la evidencia digital en cada uno de los pasos de investigación detallados. Ha sucedido que muchas veces, la evidencia digital ha sido previamente “analizada” por personal no idóneo y estos hechos no están informados formalmente.

Posteriormente, al realizar un análisis de datos se detecta que la información original ha sido alterada, y la evidencia pierde su valor probatorio. Se debe observar lo inherente al transporte de la evidencia digital. Es común que los elementos informáticos a periciar lleguen sin los más mínimos resguardos.

Usualmente, el secuestro de material informático tiene un tratamiento muy similar al de otros elementos –armas, papeles contables, etc.- y no se le da el cuidado que realmente merece, pudiendo algún golpe ocasionar roturas en el equipamiento informático. También están los aspectos técnicos referidos a la autenticación de la evidencia original.

Mientras los documentos digitales crean claramente retos únicos, en la esencia de la preservación está la exigencia de que el documento se conserve independientemente de su formato.

El siguiente extracto de ISO 15489 indica el fundamento y la importancia de la función de preservación (International Organization for Standardization, 2001). Así, una entidad o institución conserva una colección de objetos digitales por varias razones de tipo legal, histórico, e incluso documentos digitales personales (John, 2009); de tipo investigación o memoria histórica además de aquellas que recuperan sitios web (Llueca, 2006). El objetivo final es que la información no se corrompa y sea accesible a lo largo del tiempo.

En muchos casos resulta impracticable realizar copias de la evidencia original por impedimentos técnicos u otras razones de tiempo y lugar. En estos casos se deberán extremar las precauciones durante la investigación, de tal manera que siempre se debe aplicar técnicas de análisis de datos no-invasivas y utilizar todas las herramientas forenses que estén al alcance, a fin de no alterar la evidencia.

Algunos autores, hacen referencia también, a que no hay un procedimiento establecido para la conservación o preservación de la evidencia electrónica y que la presentación de la misma, ante los tribunales, se hará en cada país como resulte de la interpretación analógica de los preceptos establecidos para la evidencia tradicional, esto es, como evidencia documental y como evidencia testifical en

la mayoría de los casos. (Fredesvinda, Lázaro Herrero, & García González, 2008)

Una de las principales observaciones de ellos es un cambio lento en responder las preguntas que ayudan a solucionar problemas en preservación de la información digital con el tiempo para asegurar que el problema no aparecerá en toda su complejidad. Más allá de eso, sin embargo, en el 2011, se indica que es necesaria una investigación más fundamental con el fin de garantizar que la información de forma y sistemas de procesamiento de información se producen en el futuro plantean menos de un desafío en términos de preservación. (Strodl, Petrov, & Rauber, 2011)

Los mismos autores, mencionan que los primeros proyectos de investigación en el campo de la preservación digital se iniciaron con la definición, el diseño y discusión de los conceptos básicos, sistemas y métodos. Los temas dominantes incluían, entre otros, la selección y la evaluación, las definiciones de metadatos, identificadores únicos, herramientas de caracterización. (Strodl, Petrov, & Rauber, 2011)

La preservación digital es necesaria para la admisibilidad legal de registros e-government o cualquier forma de información digital almacenada en medios de almacenamiento o evidencia del caso en la corte como datos móviles, para establecer su procedencia, integridad, autenticidad y confiabilidad. Los mismos parámetros también son importantes para la preservación digital en adición al parámetro de

“usabilidad a largo plazo” de la información digital, como se indica en la ISO 14721:2012 y modelo de referencia OAIS. (International Organization for Standardization, 2012)

Las firmas digitales, que normalmente se utilizan para establecer la autenticidad de la información digital, tienen una limitada validez. Por lo tanto, las evidencias digitales complementarias, que sean útiles en el establecimiento de la autenticidad cuando esta es capturada y preservada, corrobora que puede ayudar a inferir o establecer la procedencia, integridad, autenticidad y fiabilidad de la información digital y por lo tanto puede llegar a ser legalmente admisible también.

Amanda Wilson hace hincapié en que “La razón por la preservación de todos los materiales de depósito legal es para ser capaz de acceder a estos documentos en el futuro. Las preocupaciones en torno a la preservación y el acceso son que a medida que cambia la tecnología, el software y el hardware se vuelven obsoletos y se sustituyen. (Wilson, 2004)

Harvey afirma que hay una necesidad de almacenar las publicaciones digitales, los flujos de bits, los medios para el tratamiento de esos, los dispositivos que nos permiten acceder a ellos, así como la información contextual para asegurar la integridad y autenticidad. Sin embargo, hay una falta de hardware estándar y el software, el rápido ritmo de obsolescencia tecnológica y muchos puntos en una vida de documentos electrónicos donde su integridad puede ser comprometida. (Harvey, 2005)

Hedges, sugiere que hay que reelaborar las reglas para definir mejor cuando la obligación de preservar los documentos electrónicos comienza y termina, y hacer frente a los tipos de sanciones que sean apropiados para las faltas por la obligación de preservación. (Hedges, 2013)

Los aspectos claves para este estudio son entre otros, entender los aspectos concretos de la preservación de los documentos digitales, guiar el desarrollo de un plan de preservación, contribuir a salvaguardar los documentos digitales a lo largo del tiempo de forma fiable, y proporcionar referencias a lo que ocurre en otros lugares.

En un reporte del Departamento de Justicia en Washington, se indica el siguiente principio: “La evidencia digital, por su propia naturaleza, es frágil y puede ser alterado, dañado o destruido por manejo inadecuado o un examen”. Por estas razones deben tomarse precauciones especiales para preservar a este tipo de evidencias. No hacerlo puede hacerla inservible o conducen a una conclusión inexacta. (U.S. Department of Justice, 2004)

Individuos y organizaciones comúnmente destruyen documentos durante el curso normal de las actividades empresariales. (Walker & McCurdy, 2002) Sin embargo, la obligación de preservar los documentos y datos electrónicos requiere buena fe y los esfuerzos razonables para retener información que puede ser relevante en una controversia o litigio. Donde, si la información pertinente es destruida,

el tribunal puede imponer sanciones de penalidades económicas a juicio de defecto. (Rothstein, Hedges, & Wiggins, 2007)

Es esencial que cada organización desarrolle su propio sistema de preservación y la definición e implementación de medidas de preservación adecuado, que cubre todo el ciclo de vida de la información (diseño, producción, almacenamiento, mantenimiento, evaluación/selección y acceso a los recursos digitales) y se concretarán en planes y modelos para garantizar la autenticidad, integridad, fiabilidad, facilidad de uso y la inteligibilidad de la información durante el tiempo que la organización lo requiera.

La definición y la evaluación de la autenticidad son tareas complejas que implican ciertas actividades/técnicas, teóricas y operativas, que son la elaboración de recomendaciones y políticas para la construcción de depósitos de identificación fiable y precisa de cada componente de la función de custodia.

En consecuencia, es necesario definir cómo y en qué se basa la autenticidad y como debe ser gestionado para asegurar la fiabilidad de la información digital, teniendo en cuenta que no es posible preservar los objetos digitales en su forma y estructura original y por lo tanto es necesario modificar con cierta periodicidad.

En Ecuador, en el documento “Retos a superar en la administración de justicia ante los delitos informáticos en el Ecuador”, de Laura Alexandra Ureta Arreaga, indica que “Podemos observar que las

sanciones establecidas se orientas específicamente a preservar aspectos que se delinean con la seguridad de la información en la que se trata de salvaguardar la confidencialidad, integridad y disponibilidad de los datos y los sistemas informáticos”. (Echeverría & Ureta, 2009)

Marco filosófico o epistemológico

La filosofía de la información es un campo de estudio relativamente nuevo, el cual no plantea desarrollar una teoría unificada de la información, sino más bien una familia integrada de teorías que analicen, evalúen y expliquen los diversos principios y conceptos de información, su dinámica y utilización principalmente en entornos digitales, con especial atención a las cuestiones sistémicas que provienen de diferentes contextos de aplicación y con vínculos con otros conceptos clave de la filosofía, como el ser, el conocimiento, la verdad, la vida y el significado. (Morán, 2015)

En consecuencia, la filosofía de la información se ha convertido en un campo de vital importancia, pues se define como el estudio filosófico que investiga de forma crítica la naturaleza conceptual y los principios básicos de información, incluyendo su dinámica, utilización y las ciencias que la estudian, además de la elaboración y la aplicación de la teoría de la información y las metodologías de cálculo a los problemas filosóficos. También legisla sobre lo que puede acontecer con el fenómeno informativo, y cómo la información debe ser debidamente procesada, administrada y usada. Además, la filosofía de la información, cuyo principales representantes son Luciano Floridi

(Floridi L. , 2013) y Anthony Beavers (Beavers, 2013), revitaliza viejas cuestiones filosóficas, plantea nuevos problemas y contribuye a la re conceptualización de nuestras visiones del mundo.

La tecnología ha producido un cambio informacional que va de lo semántico a lo óntico, situación que da lugar a una re-ontologización del mundo o, en otras palabras, una transformación de la naturaleza.

En el 2004, Floridi publicó un escrito sobre los problemas que aún se encontraban abiertos para el quehacer de la filosofía de la información; estos eran una serie de ideas y postulados que quedaban inconclusos, pendientes por desarrollar o, bien, que era necesario refutar para avanzar en la conformación de un terreno apropiado para el estudio de la información y la tecnología en la época contemporánea. Estos problemas son esquematizados de acuerdo a su respectivo enfoque, a saber:

Analíticos

- a. Definir una postura sobre el enfoque de ver a la tecnología como un elemento de expansión de la mente humana. (Perspectiva de Herbert Simon)
- b. Introducirse en la perspectiva de David Hilbert y analizar su idea de si los problemas matemáticos son la raíz de las circunstancias históricas. (Por ejemplo, el flujo de información como un problema algorítmico)
- c. El esclarecimiento de lo que invoca la palabra «información».

- d.** La respuesta a la pregunta ¿Cuál es la dinámica de la información? (problema input/output).
- e.** La posibilidad del desarrollo de una «gran» teoría unificada de la información.
- f.** Semánticos
- g.** El problema del agrupamiento de los datos ¿Cómo es que los datos obtienen su significado?
- h.** El problema de la verificación ¿Cómo es que los datos adquieren su carácter de verdaderos?
- i.** Desarrollo de la resolución de Kirkham ¿Puede la información explicar la verdad?

Cognoscitivos

- a.** Definir los diversos planteamientos sobre las formas de cognición y los niveles de abstracción (Problema de Descartes).
- b.** Estructurar las formulaciones sobre la inteligencia natural y los niveles de abstracción (Problema de la ingeniería inversa y la reingeniería).
- c.** Retomar las formulaciones sobre la inteligencia artificial y los niveles de abstracción. (Problema de Turing) La dialéctica del ciclo de información.
- d.** Esclarecer la posibilidad de cimentar a la epistemología en una teoría de la información, por ejemplo con la hipótesis del continuum datos-información-conocimiento.

- e. ¿La ciencia puede ser reducible a un modelado informativo?

Naturalistas

- a. Estatus ontológico de la información.
- b. La información como fenómeno natural y la semantización de los datos.
- c. Concebir a la naturaleza como un mundo de la información y a sus fenómenos como objetos de información.

Valorativos

- a. Investigar sobre la cuestión de si la ética computacional tiene como sustento principal algún fundamento filosófico. (Floridi L. , 2004)

Los repositorios como nuevo paradigma

Hasta el momento y desde una visión global se ha ubicado el surgimiento de las bibliotecas digitales, como un modelo basado en el paradigma de las bibliotecas tradicionales. Como toda analogía llega un momento en que sus límites eran evidentes produciéndose entonces una crisis o, como en el caso de teorías científicas, una revolución científica que ha dado origen a un nuevo paradigma, las bibliotecas digitales (Capurro, 2007). Para identificar su rol como un nuevo tipo de biblioteca autónoma es necesario ubicarla a un nivel más abstracto y para ello se requiere llegar a una reflexión epistemológica que nos muestre sus campos de aplicación y uso, donde se vea la diferencia como la biblioteca digital administra y procesa sus recursos y las formas como se relaciona con los usuarios, así como su desempeño en

contextos, como el cultural, educativo y político. Son estos contextos los que la presente investigación cubre, explícitamente para las bibliotecas digitales su campo de acción, sus usos, las características y las formas de participación de sus usuarios, sus colecciones, sus procesos, normas, servicios y lo que ellas significan en los niveles educativo, cultural, social y en lo político. (Arias, 2008)

Rafael Capurro, en el análisis que hace de la epistemología y la ciencia de la información, en donde, aporta los siguientes argumentos:

“...La ciencia de la información tiene dos raíces: una es la bibliotecología clásica o, en términos más generales, el estudio de los problemas relacionados con la transmisión de mensajes, siendo la otra la computación digital.

La primera raíz nos lleva a los orígenes mismos de la sociedad humana entendida como un entretejido o una red de relaciones, basadas en el lenguaje, es decir en un ámbito hermenéutico abierto, donde los entrecruces metafóricos y metonímicos permiten no sólo mantener fluido el mundo de las convenciones y las fijaciones que hacen posible una sociedad humana relativamente estable, sino también que nos permiten generar la capacidad de preguntar por lo que no sabemos a partir de lo que creemos que sabemos. Es claro que esta raíz de la ciencia de la información o, como también podríamos llamarla, de la ciencia de los mensajes, está ligada a todos los aspectos sociales y culturales propios del mundo humano. (Capurro, 2007)

La otra raíz es de carácter tecnológico y se refiere al impacto de la computación en el proceso de producción, recolección, organización, interpretación, almacenamiento, preservación, recuperación, diseminación transformación y uso de la información y en especial de la información científica fijada en documentos impresos...”

La segunda raíz de la ciencia de la información revela como la tecnología impacta los procesos y es allí donde surgen características propias, cuando se trata de bibliotecas digitales, u otros entornos como las instituciones de investigación criminal, tales como:

- Los documentos físicos a preservar son “objetos digitales” (contenidos de texto completo), que incluyen todo tipo de material y soportes, como pueden ser: libros, folletos, revistas, fotografías, material sonoro, vídeos, pinturas, software, etc.
- Las políticas para la conformación de las colecciones son muy propias para este tipo de bibliotecas de contenidos, dado a que están muy ligadas, entre otras, al contenido y la relevancia del documento, al valor patrimonial e histórico e integridad del mismo.
- Se dispone de normas y herramientas propias para el análisis descriptivo y temático de los objetos digitales, tales como, metadatos, indexación, ontologías que posibilitan la organización, almacenamiento preservación y posterior identificación y recuperación de los objetos digitales.

- El concepto de usuario se ha transformado y enriquecido, ya no es sólo el cliente que acude a la biblioteca, es un usuario, en el caso de esta investigación, autorizado, registrado, el cual puede ser un lector que hace uso de un documento y su contenido o que recupera un documento para usarlo y preservarlo.
- La difusión y uso del conocimiento contenido en ella es mundial, es un servicio sin ningún tipo de restricciones que nos acerca al ideal, de tener un acceso democrático al conocimiento universal.
- La “diseminación selectiva de información” (SDI) o perfiles informacionales individuales o de grupo, son modalidades propias de las bibliotecas digitales que le permiten al usuario reconocer la redundancia y ver también lo nuevo y potencialmente relevante, es decir, la información.

Estos nuevos conocimientos y saberes en los procesos de gestión de la información, han surgido como consecuencia de los cambios paradigmáticos de la bibliotecología y la ciencia de la información en el siglo pasado, los cuales nos ayudan a entender la evolución de las bibliotecas y repositorios como sistemas de información y a comprender el porqué es necesario aceptar que hay una nueva biblioteca, la biblioteca digital, y que además, debe ser preservada adecuadamente.

Capurro (2007), el identifica tres paradigmas epistemológicos predominantes en la ciencia de la información, el físico, el cognitivo y el social. Como él lo afirma, los tres paradigmas han tenido

consecuencias relevantes para el diseño y uso de los sistemas de información (Capurro, 2007). Por ello, basándose en estos presupuestos epistemológicos implícitos o explícitos de la ciencia de la información, se conceptualiza cómo éstos se comportan en el marco de las instituciones de investigación criminal y sus procesos de preservación de evidencia. En el funcionamiento de las bibliotecas digitales como medio de preservación se ve claramente cómo se agotan los límites del paradigma físico de las bibliotecas tradicionales, dado que, en el transporte físico entre el emisor y receptor, el canal y el mensaje en las bibliotecas digitales ha sido re-conceptualizado, por efectos del avance tecnológico y por las nuevas necesidades de interacción entre el receptor y emisor. En la biblioteca digital se suceden en tiempo real procesos como los de: producción, recolección, organización, almacenamiento, diseminación, recuperación, transformación y uso de la información, en donde el sujeto cognoscente o usuario, tiene un rol activo que supera el límite que originalmente se le había asignado en las bibliotecas tradicionales. Las bibliotecas digitales tienen plena identificación con el paradigma cognitivo, para ellas la conservación y la preservación del conocimiento contenido en los documentos les es fundamental, o sea, que una de sus mayores preocupaciones es el contenido intelectual que en ellas, se transforma en “objetos digitales”, sin importar el formato o soporte físico que lo contiene.



FUNDAMENTO TEÓRICO

Capítulo 2



FUNDAMENTO TEÓRICO

Repositorios institucionales

Un repositorio institucional (RI) es un conjunto de servicios para almacenar y hacer accesibles materiales de investigación en formato digital creados por una institución y su comunidad, una colección digital del producto de la investigación llevada a cabo por esa comunidad. Los repositorios institucionales se están convirtiendo en herramientas esenciales para la comunicación académica en la era digital. Ellos pueden formar parte de un sistema mayor, nacional, regional y global de repositorios, indizados de una manera estándar y recuperable, por medio de una interfaz de acceso.

También pueden proveer las bases para nuevos modelos de edición académica y pueden vincularse a otros servicios relacionados, como enseñanza a distancia electrónica, publicación electrónica de revistas de investigación o publicación por demanda (Lynch, 2003).

Las definiciones que se han dado de repositorio institucional han sido numerosas, de las analizadas se concluye que un repositorio institucional es un conjunto de servicios prestados por instituciones que tienen obligación de conservar información, a la comunidad, para recopilar, administrar, difundir y preservar la producción documental digital generada en la institución, cualquiera que sea su tipología, a través de la creación de una colección digital organizada, para garantizar un aumento de la visibilidad e impacto de la misma. (Sanchez & Melero, 2006), (Crow, 2002), (McDowell, 2007)

Interoperabilidad, recolección, difusión y accesibilidad

Entiéndase por interoperabilidad la capacidad de los sistemas, servicios y organizaciones para trabajar juntos de un modo transparente hacia objetivos comunes o diferentes. En el ámbito técnico se apoya, entre otros, en los estándares abiertos para la comunicación entre sistemas y para la descripción de recursos y colecciones. La interoperabilidad tiene que ver principalmente con el contexto de la búsqueda y acceso a los recursos. La Iniciativa de Archivos Abiertos (Open Archives Initiative - OAI) pretende desarrollar y promocionar normas de interoperabilidad que tienen como objetivo el facilitar la difusión eficaz de los contenidos. (Open Archives, 2002).

Beneficios de los repositorios institucionales

Una de las principales motivaciones es la de permitir el acceso abierto a los resultados de su actividad científica y académica. Pero quizás esta razón solamente sería insuficiente para justificar el esfuerzo considerable que supone la creación de repositorios.

En un primer nivel, un repositorio institucional es el reconocimiento de que la actividad intelectual de la institución estará representada cada vez más en soporte digital y que la principal responsabilidad de esta es ejercer el control sobre su producción intelectual, haciéndola accesible, fácilmente recuperable y asegurar su permanencia en el tiempo.

Proyectos sobre preservación digital

En la historia de la preservación digital han sido muchos los proyectos puestos en marcha, tanto a nivel internacional como particular de universidades y centros científicos. Estos proyectos han abarcado diversas áreas, desde la concienciación de los organismos productores y conservadores de información a herramientas desarrolladas, incluso por comités expertos.

Existen diversas iniciativas de modelos de conservación digital. Todos los modelos tienen en su horizonte la preservación digital a largo plazo. El modelo de ciclo de vida de conservación, propuesto por el Digital Curation Center (DCC), propone una conceptualización de todas las actividades necesarias en una unidad de custodia, a fin de obtener una concreción secuencial en todos los procesos de planificación y conservación digital. Los proyectos más destacables, por mencionar algunos: CAMiLEON (Holdsworth & Wheatley, 2010), CASPAR. (DCC, 2009), CEDARS (Jenkins, 1998), CLOCKSS (Elliot, 2007), IFLA (The International Federation of Library Associations and Institutions, 2012), NESTOR. (NESTOR, 2012), PADI. (PANDORA, Australia's Web Archive, 2011).

Centramos la atención en algunos proyectos que sobresalen por su preferencia y aplicabilidad:

InterPARES

Proyecto de la Universidad de British Columbia. Se pretende desarrollar el conocimiento esencial para la preservación a largo plazo de los

documentos digitales, y proveer las bases para estándares, políticas y planes de acción que aseguren la longevidad de este tipo de materiales y que los usuarios confíen en su autenticidad. Se ha desarrollado en cuatro fases (The International Research on Permanent Authentic Records in Electronic Systems, 2013).

Planets

PLANETS - Preservation and Long-term Access through Networked Services, es un proyecto iniciado en 2006 por un periodo de cuatro años y financiado por la Unión Europea dentro del VI Programa Marco con la misión de tratar los retos que tiene planteados la preservación digital. El primer objetivo para Planets es construir servicios prácticos y herramientas para ayudar a asegurar el acceso a largo plazo a nuestro patrimonio cultural y científico que existe en formato electrónico. Según su presentación, crea un marco sostenible para permitir la preservación de los contenidos digitales, con la finalidad de aumentar la capacidad europea para asegurar el acceso en perpetuidad a su información digital. (Open Planets Foundation , 2007).

Premis

Desarrollado por la Library of Congress, desde el 2007, establecen un Metadata basado en OAIS, aunque no coinciden completamente en la terminología usada. El modelo de referencia OAIS fue el adoptado por el estudio realizado en 2002 por el grupo de trabajo Preservation Metadata Framework, organizado conjuntamente por la OCLC y la RLG para definir los tipos de información que se deberían asociar a un

objeto digital a efectos de preservación y que es el origen del PREMIS Data Dictionary for Preservation Metadata. La versión 1.0 del PREMIS Data Dictionary fue publicada en 2005, y la actual 2.0 es de marzo de 2008. Este diccionario de datos es una traslación del modelo OAIS a unidades semánticas implementables, bajo la forma de un esquema de metadatos específicos para preservación, y sustentado en encuestas sobre sistemas reales de repositorios de preservación. Al igual que el modelo OAIS, el esquema de metadatos PREMIS no define ninguna estrategia o método de implementación, ni prescribe una tipología de acciones, ni el modo en el que deben recogerse, almacenarse o gestionarse los datos referidos a estas acciones. (PREMIS Data Dictionary, 2012).

OAIS

El modelo OAIS, ISO 14721:2003, creado por el Consultative Committee for Space Data Systems (CCSDS), es un modelo de referencia utilizado para la conservación y preservación de archivos digitales. (CCSD, 2012). El CCSDS engloba a las agencias espaciales de Brasil, Canadá, China, Unión Europea, Francia, Alemania, Italia, Japón, Rusia, Reino Unido y Estados Unidos (NASA). Este organismo define el OAIS de la siguiente manera: “An OAIS is an archive, consisting of an organization of people and systems that has accepted the responsibility to preserve information and make it available for a Designated Community.” (Consultative Committee for Space Data Systems, 2012).

El modelo OAIS fue diseñado inicialmente para su uso dentro de la comunidad científica del espacio, teniendo como objetivo conservar digitalmente los datos provenientes de las misiones espaciales (Consultative Committee for Space Data Systems, 2002). Sin embargo, ha sido adoptado ampliamente por las bibliotecas, especialmente las de aquellos países que han participado en su elaboración (Woodyard, 2002), como la Biblioteca del Congreso de Estados Unidos, la Biblioteca Británica, la Biblioteca Nacional Alemana o la Biblioteca Nacional de Nueva Zelanda, que fue la pionera en implantarlo (Knight, 2009). Es por esto que el modelo OAIS tiene una amplia aplicabilidad para la preservación a largo plazo en cualquier contexto.

Evidentemente, para poder implantar el modelo OAIS a una institución donde los recursos son limitados, se debe recurrir a su adaptación, para facilitar su aplicabilidad y su sostenibilidad financiera. Por ello, es imprescindible averiguar, en otras, las características del entorno, la formación de su personal o la seguridad de sus datos. El principal objetivo de este estudio es precisamente este, plantear la adaptación de un modelo OAIS que se pueda aplicar a las entidades de gestión en instituciones de investigación criminal para la preservación de las evidencias.

El modelo OAIS incorpora la vigilancia tecnológica, la conservación digital y todos aquellos procesos que requieren que los documentos digitales existentes en un centro de datos no puedan ser sometidos a alteraciones, modificaciones o pérdidas. En el modelo OAIS se definen

los actores dentro de un archivo, así como los flujos de información. Los actores que intervienen en un modelo OAIS son Productor (Producer), Gestor (Management) y Consumidor (Consumer).

Como se ha mencionado previamente, el modelo OAIS, es un modelo de conservación de objetos digitales que establece una serie de flujos de datos que determinan las obligaciones de un sistema de conservación a largo plazo para archivar y gestionar de los objetos digitales. Este modelo, hasta ahora, se ha considerado como un modelo válido de preservación digital, como queda patente en su extendida aplicación en la industria aeroespacial y en las bibliotecas digitales. (McCray & Gallagher, 2001)

No se ha planteado todavía el hecho de que el modelo OAIS tenga que ser el único modelo de preservación digital, aunque sí hay autores que han indicado la posibilidad de una reducción o simplificación del mismo debido a la complejidad de su puesta en funcionamiento. (Allinson, 2006) (Spence, 2006)

El modelo de información OAIS

El modelo OAIS se basa en la definición del modelo de información, para poder custodiarla posteriormente, con una serie de elementos funcionales que permiten conservar un archivo digitalmente, sin contemplar una tecnología concreta para su aplicación. Un archivo OAIS representa todo el conjunto de información mediante dos elementos, el objeto de los datos (Data Object) y su representación de la información (Representation Information).

El objeto de los datos es la información a conservar a largo plazo, es decir, el contenido. La representación de la información es la forma en cómo será accedido ese objeto con información, el continente. Ambos representan la base de conocimiento (Knowledge Base). Una base de conocimiento en un archivo OAIS permite que la información que se va a conservar a largo plazo se pueda entender y procesar. La base de conocimiento permite al archivo OAIS entender la información que se conserva a largo plazo.

Una vez revisados los participantes en el modelo OAIS, así como una parte de la definición del modelo de información, se hace necesario profundizar en el funcionamiento interno del modelo, analizando las entidades funcionales. Un archivo OAIS puede ser una entidad única pero también puede comunicarse con otros archivos OAIS en el caso de archivos federados.

El modelo OAIS, aporta un concepto escueto, aunque, debido a su sencillez, no se muestra excesivamente significativo: “data about other data” (datos sobre datos). En contraposición a esta propuesta, el modelo incluye una definición de metadato de preservación y detalla el alcance del mismo de modo minucioso, tal y como se presentará con posterioridad.

Las entidades funcionales de un archivo OAIS

El modelo OAIS, se desglosa en un conjunto de seis entidades funcionales, que son Ingesta (Ingest), almacenamiento de archivo (Archival Storage), gestión de datos (Data Management),

administración (Administration), Planificación de la preservación (Preservation Planning) y acceso (Access), según se muestra en la Figura 1. Estas entidades funcionales son las que permiten preservar la información de acuerdo con el modelo de información definido. Dicho modelo de información especifica cómo hay que gestionar la información y cómo se transporta desde la entidad funcional de Ingesta de datos hasta la entidad funcional Acceso correspondiente.

Además, existen un pequeño conjunto de responsabilidades obligatorias dentro de las entidades funcionales que son necesarias para disponer de la conformidad de un archivo OAIS, de acuerdo al modelo de información elegido.

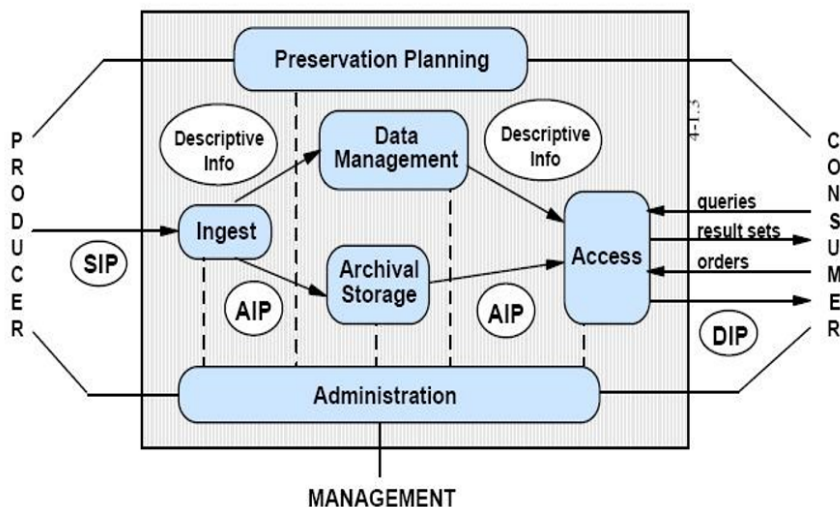


Figura 1. Entidades funcionales de OAIS.

Fuente: (Consultative Committee for Space Data Systems, 2012)

A continuación, se explican los puntos más relevantes de cada entidad funcional, aunque, su detalle se puede encontrar en la norma publicada por el CCSDS (Consultative Committee for Space Data Systems, 2012).

Ingesta

Ingesta es una entidad que acepta la información de los productores (Figura 2). El proceso de ingesta puede rechazar información del productor si esta no está definida según el modelo de información de OAIS.

En este proceso, interviene el paquete de información de envío (Submission Information Package) (SIP), con los datos que proceden del productor. El proceso ingesta genera un paquete de información de archivo (Archival Information Package) (AIP) donde la información se prepara para ser archivada.

El productor envía información al archivo en forma de paquete de información de Envío (SIP). Este es recibido por la función recepción del envío (Receive Submission), para después enviarlo al bloque de verificación de la calidad (Assurance Quality), con la misión de comprobar que coincide con el modelo de información y validar la entrada.

Una vez validado el SIP se traslada a la función generar AIP (Generate AIP) donde se generan los datos correspondientes mediante la función generar información descriptiva (Generate Descriptive Info).

Estas dos últimas funciones son coordinadas por la función coordinar las actualizaciones (Coordinate Updates), que facilita que la información que haya sido enviada sea archivable y que el paquete de información se almacene en almacenamiento de archivo (Archival Storage).

A su vez actualiza la base de datos de información mediante la función gestión de datos (Data Management).

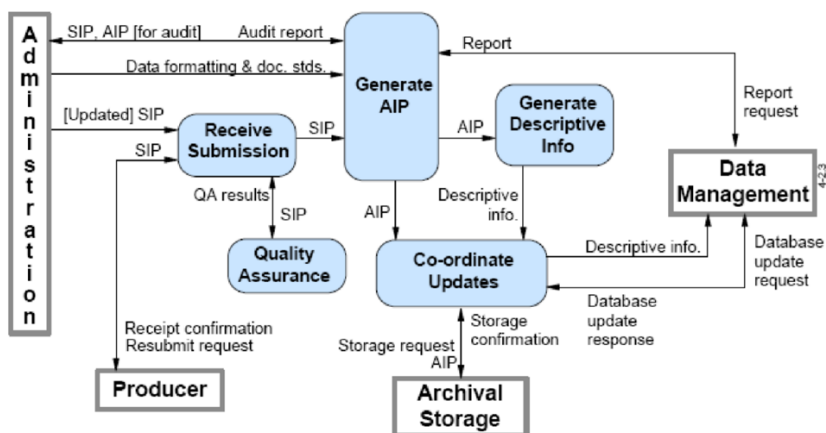


Figura 2. Función Ingesta

Fuente: (Consultative Committee for Space Data Systems, 2012)

Almacenamiento de archivo

El almacenamiento de archivo es la entidad que recibe el paquete de información de archivo (Archival Information Package) (AIP) y lo almacena en la base de datos del archivo OAIS. La función almacenamiento de archivo, como puede apreciarse en la figura 3, se encarga de recibir el AIP en la función recibir datos (Receive Data) y enviar una señal de confirmación de almacenamiento (Storage Confirmation) al bloque ingesta.

A su vez, desde la entidad funcional administración (Administration), se gestionan las políticas de acceso a través de las funciones gestión de la jerarquía de almacenamiento (Manage Storage Hierarchy) y sustitución de medios (Replace Media), que sirve para cambiar el soporte donde está la información y que esta no se pierda. Las funciones comprobación de error (Error Checking) y recuperación frente a desastres (Disaster Recovery) realizan actividades de notificación de errores y recuperación de copias del archivo, en caso de haber corrupción en los datos o en el soporte donde estos se alojan.

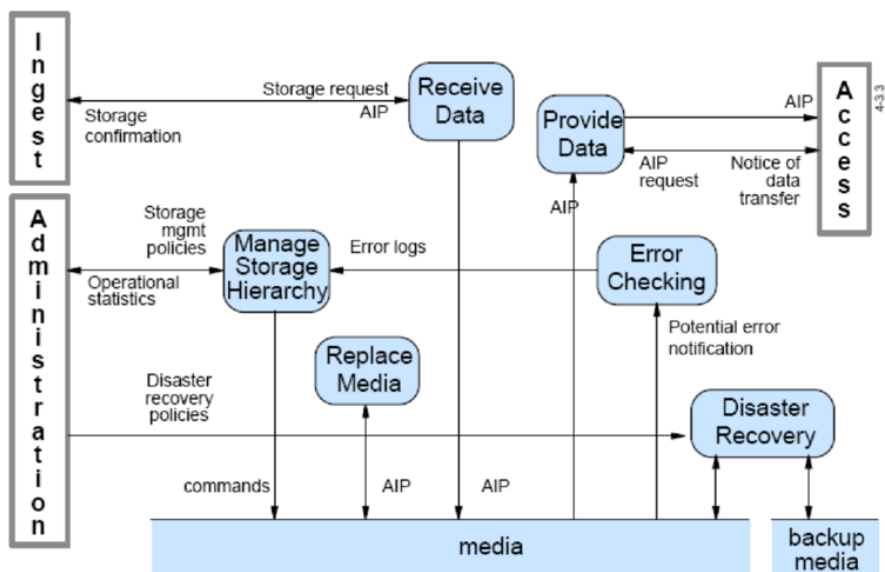


Figura 3: Función de almacenamiento de archivo
Fuente: (Consultative Committee for Space Data Systems, 2012)

Gestión de datos

La entidad funcional gestión de datos se encarga de actualizar la base de datos (Database) del archivo OAIS, así como de mejorar el acceso a la información descriptiva (Descriptive Information). La función más relevante es administrador de la base de datos (Database Administrator), responsable de mantener la integridad de los datos, crear tablas o esquemas que soporten las funciones de gestión de datos (Data Management). También tiene un bloque denominado recepción de la actualización de la base de datos (Receive Database Updates), implicado en la notificación de la actualización de la base de datos a las entidades funcionales ingesta y administración.

Dispone también de la función realización de peticiones (Perform Queries), que ofrece resultados de recuperación de información a la entidad funcional access. La función genera informe (Generate Report) es la encargada de realizar todo tipo de informes sobre los datos o estadísticas a las entidades funcionales ingesta, administración y acceso como se puede ver en la figura siguiente.

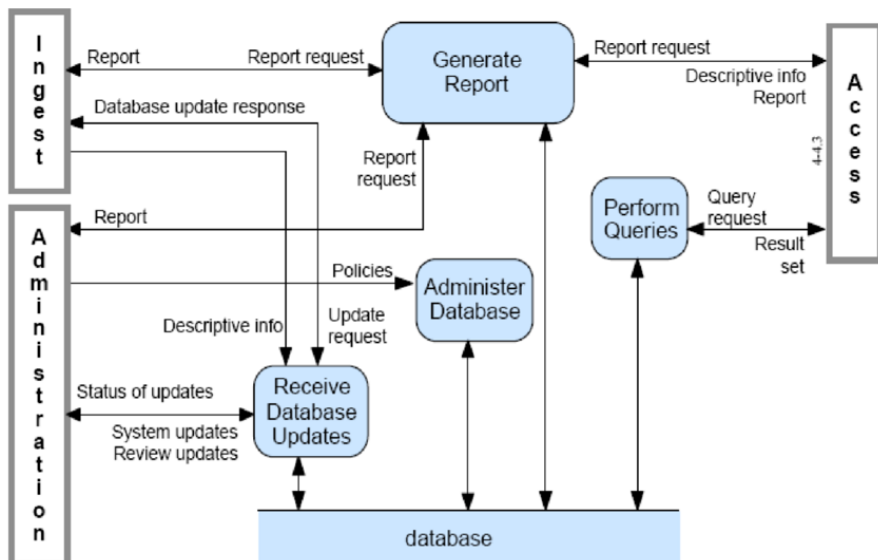


Figura 4. Función Gestión de Datos

Fuente: (Consultative Committee for Space Data Systems, 2012)

Administración

Administración es una entidad que se encarga de realizar todo el mantenimiento del archivo OAIS. Esto es, la ejecución de las operaciones de archivo o la migración/actualización de los datos archivados. Este proceso se ilustra en la figura 5.

En esta entidad funcional están involucrados todos los actores del modelo OAIS ya que administración se encarga de la gestión de todos los flujos de políticas de los datos que se van a archivar. Así, es responsable de mantener la integridad y la trazabilidad de la configuración durante las fases del ciclo de vida de los documentos.

También permite gestionar tanto los procesos de auditoría, para verificar la calidad de los archivos, como las políticas de archivos y verificación de estándares.

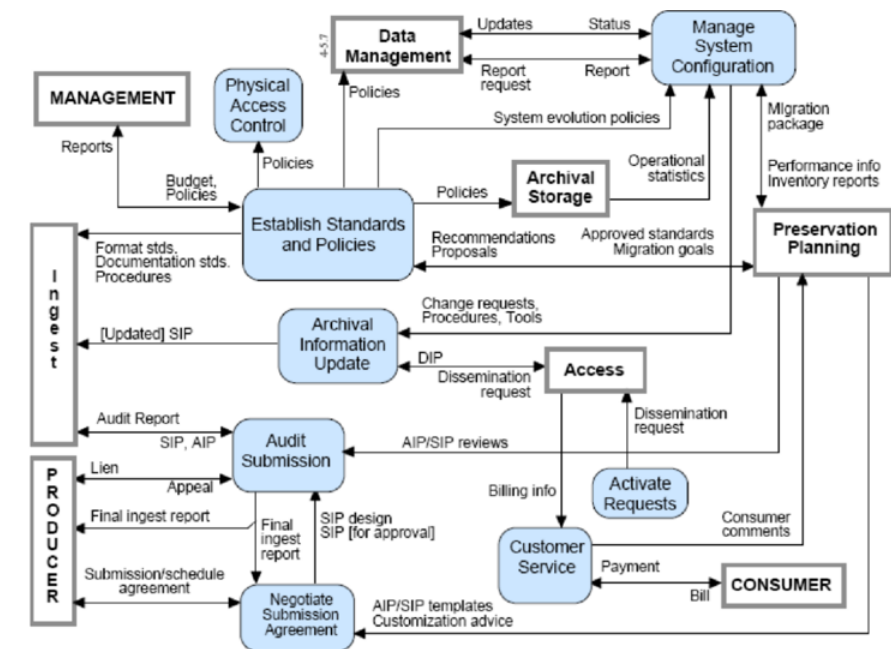


Figura 5. Función de Administración

Fuente: (Consultative Committee for Space Data Systems, 2012)

Planificación de la preservación

La planificación de la preservación (Preservation Planning) es la entidad que monitoriza los servicios del archivo OAIS como asegurar que la información sea accesible, a largo plazo para la comunidad designada.

También se encarga de realizar recomendaciones de mejora del archivo y permite la monitorización de los nuevos avances en la tecnología, para

poder aplicar después nuevas políticas de preservación y estándares. Todo este proceso se ilustra en la figura 6.

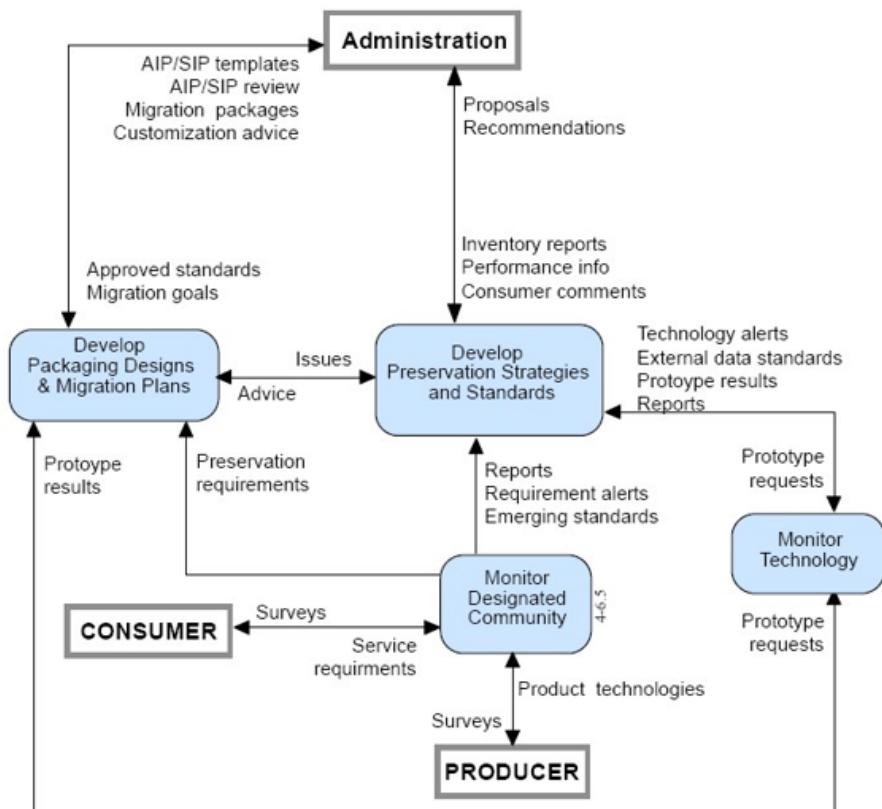


Figura 6. Función de Preservation Planning
Fuente: (Consultative Committee for Space Data Systems, 2012)

Acceso

Acceso (Access) es la entidad funcional que facilita servicios a los consumidores para que puedan recibir y entender la información que solicitan.

Esta última función coordina las actividades de acceso de información, recuperación y generación de paquetes de información, el paquete de información de diseminación (Disseminated Information Package-DIP), para que el consumidor pueda disponer de la información que requiere, tal y como se ilustra en la figura 7.

Los datos que recibirá el consumidor serán una copia exacta de la información introducida en el archivo OAIS, pero es posible que esta información pueda estar representada en un formato diferente al original.

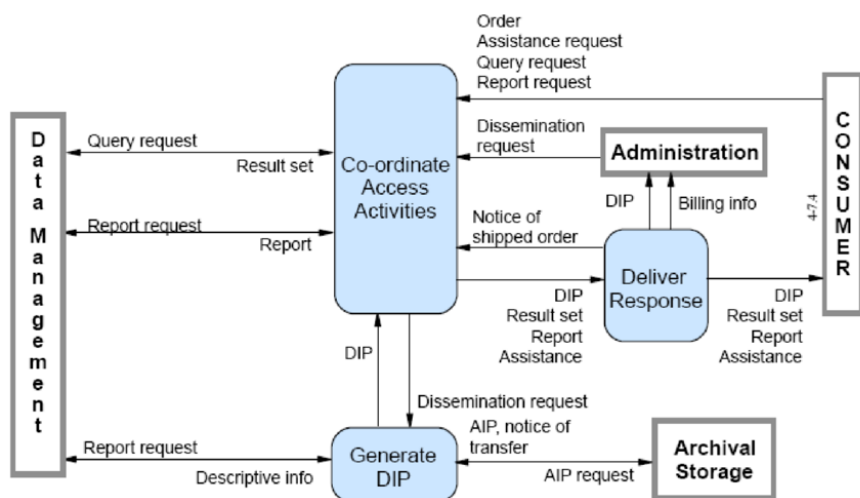


Figura 7: Función de Acceso

Fuente: (Consultative Committee for Space Data Systems, 2012)

Metadatos

En cuanto a la utilización de metadatos en repositorios institucionales, una de las primeras medidas de un sistema de preservación digital es la asignación de metadatos a los objetos digitales. Los metadatos son

necesarios para permitir el acceso a los documentos depositados y su gestión y preservación a largo plazo.

La clasificación más comúnmente aceptada de metadatos es la siguiente:

- *Metadatos descriptivos*: representan los datos sobre el contenido intelectual, que ayudan a identificar y localizar un recurso. El estándar más utilizado es Dublin Core.
- *Metadatos administrativos*: datos necesarios para la gestión de un recurso: mantenimiento, almacenamiento, entrega; incluyen los aspectos técnicos y los relacionados con los derechos. Se trata pues de todos aquellos esquemas que describen la procedencia de un objeto digital, los procesos realizados para su creación o generación, sus características técnicas, sus condiciones de acceso y derechos de propiedad intelectual, y las acciones ya realizadas o previstas relacionadas la preservación del objeto mismo.
- *Metadatos estructurales*: se trata de los datos que se refieren a la estructura del recurso y a los elementos que lo integran.

La creación de los metadatos es un trabajo profesional laborioso similar a la catalogación o indización. Pero a diferencia de esas operaciones, los elementos son difíciles de conocer, el volumen de documentos digitales generados es muchísimo mayor y hay un alto porcentaje de documentos únicos, además de existir la necesidad de actualizar los metadatos a lo largo de la vida del documento. (Gallart & Keefer, 2007)

La creación de los metadatos puede correr a cargo del personal del repositorio, de los creadores o depositantes, o pueden ser de generación automática a partir del texto o de otras fuentes externas como las bases de datos.

El empleo de metadatos se percibe como estrategia esencial de preservación para evitar o mitigar principales riesgos (derivados de amenazas tales como la longevidad, la capacidad, los costes) y, muy especialmente, aquellos vinculados a la obsolescencia y fragilidad, así como los asociados a la causa documental: autenticación, evidencia, y, por supuesto, al marco legislativo que contextualiza o en el que se supedita el objeto digital. (Keefer & Gallart, 2007)

En la declaración sobre preservación del patrimonio digital acordada en vancouver (The International Federation of Library Associations and Institutions, 2012), se insiste en la necesidad de establecer cambios vinculados a factores tecnológicos, legales, económicos, políticos y culturales. En relación a los cambios tecnológicos se incide, igualmente, en la obsolescencia de los soportes y equipos, en la pérdida de integridad de la información, en la variedad de los formatos, así como en la necesidad de normalizar los metadatos de preservación, de trabajar la preservación audiovisual y de abordar la naturaleza propietaria de la tecnología.

La lectura y comprensión de un documento en letra procesal, y su transcripción, es empleado como ejemplo por candas para subrayar la utilidad de los metadatos (Candas Romero, 2006).

En el estándar ISO/TS 23081-1:2006, se especifican las utilidades y beneficios del empleo de dicha normativa para un modelo de gestión de documentos. Destacamos, únicamente, aquellas vinculadas a la preservación, dado que se aporta una enumeración de utilidades más amplia referida a un sistema de gestión de documentos:

- a.** Proteger los documentos como evidencia y asegurar su accesibilidad y disponibilidad a lo largo del tiempo.
- b.** Facilitar la comprensión de los documentos.
- c.** Respalda las estrategias de interoperabilidad, permitiendo que se incorporen oficialmente al sistema de documentos creados en diversos entornos administrativos y técnicos y que se mantengan durante tanto tiempo como sea necesario...
- d.** Facilitar la identificación del entorno tecnológico en que los documentos digitales fueron creados o se incorporaron al sistema y la gestión del entorno tecnológico en el que se han mantenido, de modo que puedan ser reproducidos como documentos auténticos cuando se necesiten.
- e.** Favorecer la migración eficiente y exitosa de documentos electrónicos de un entorno o plataforma informáticos a otro, o cualquier otra posible estrategia de conservación”. (Cabero, 2013)
- f.** El Comité Interministerial de Metadatos de Quebec (Comité Interministériel sur les Métadonnées du Québec, 2010) incluye, además:

- Asegurar la disponibilidad de los documentos.
- Administrar la confidencialidad, la integridad y la trazabilidad de los documentos.
- Facilitar el intercambio de información.
- Los beneficios enumerados enuncian los límites conceptuales del set de metadatos de preservación.

Conceptualización y categorización

Lavoie señala que las definiciones de metadatos se asemejaban a un viejo dicho sobre normas la mejor definición es que hay muchas para elegir, nos indicaban dichos autores mientras mostraban una definición. Efectivamente, se constata un amplio número de iniciativas y proyectos de metadatos donde confluyen propuestas definitorias destacadas por su simplicidad (modelo OAIS), con otras de mayor calado significativo. En algunas de ellas, no siempre están definidos los metadatos de preservación de modo explícito y detallado. Por el contrario, se presentan como un subconjunto de elementos pertenecientes a diversas categorías. (Lavoie & Gartner, 2005).

La norma ISO/TS 23081-1 entiende por metadato (enfoque archivístico): la información sobre un recurso electrónico que explica el proceso técnico y administrativo usado para crear, manipular, usar y almacenar un documento, manteniendo su valor “de evidencia” (documento de archivo) y su preservación en el tiempo.

El Consejo Nacional de Archivos de Brasil (Conselho Nacional de Arquivos, 2011) aporta la siguiente definición de metadato:

“Datos estructurados que describan y permitan encontrar, gerenciar, comprender y/o preservar documentos archivísticos en el largo plazo”.

El metadato de preservación es definido en el diccionario de datos de PREMIS (The Library of Congress, 2008, pág. 213) como “la información que un repositorio de preservación utiliza para asegurar los procesos de preservación digital”. El modelo OAIS (2002) conceptualiza el término como “aquella información necesaria para una preservación adecuada del contenido de la información...”. (Consultative Committee for Space Data Systems, 2002). En las directrices de la unesco (UNESCO, 2004, pág. 100) se aporta una definición en la que se enumeran los objetivos siguientes:

- Vinculación del objeto digital a un programa de preservación: “define el material bajo la responsabilidad de un programa de preservación”.
- Identificación de requisitos para la preservación: “Indica qué se necesita para mantener y proteger los datos”.
- Control del historial de acciones acontecidas sobre el recurso: “registra la historia del objeto y las consecuencias de lo que vaya sucediendo”.
- Certificación de la autenticidad del objeto: “documenta la identidad y la integridad del objeto para certificar su autenticidad”.
- Aseguramiento del contexto comprensible del recurso: “permite al usuario y al programa de preservación comprender el contexto del objeto almacenado y en uso”.

En base a estas aportaciones, así como aquellas relativas al concepto de preservación, podríamos definir los metadatos de preservación como el conjunto de información esencial estructurada para asegurar a largo plazo la disponibilidad, accesibilidad e inteligibilidad de los recursos digitales, incluida aquella derivada de las acciones de preservación.

Premis

PREMIS Data Dictionary for Preservation Metadata. La versión 1.0 del PREMIS Data Dictionary fue publicada en 2005, y la actual 2.0 es de marzo de 2008. Este diccionario de datos es una traslación del modelo OAIS a unidades semánticas implementables, bajo la forma de un esquema de metadatos específicos para preservación, y sustentado en encuestas sobre sistemas reales de repositorios de preservación.

Al igual que el modelo OAIS, el esquema de metadatos PREMIS no define ninguna estrategia o método de implementación, ni prescribe una tipología de acciones, ni el modo en el que deben recogerse, almacenarse o gestionarse los datos referidos a estas acciones. Es muy conveniente utilizar el esquema PREMIS, dada la riqueza y precisión creciente de las distintas versiones de su diccionario de datos. La no existencia de un repositorio de preservación normalizado no exime de la necesidad de utilizar metadatos de preservación y en concreto PREMIS. El Diccionario de datos PREMIS define los metadatos de preservación como “la información que utiliza un repositorio para soportar el proceso de preservación digital”.

Son ejemplos de actividades de preservación y de cómo pueden soportarlas los metadatos:

- Un recurso debe almacenarse de manera segura para que nadie pueda modificarlo inadvertidamente (o malintencionadamente). La información de la suma de verificación almacenada como metadatos puede utilizarse para expresar si el archivo almacenado ha variado entre dos momentos en el tiempo.
- Los ficheros deben almacenarse en soportes que puedan leer los ordenadores actuales. Si el soporte está dañado u obsoleto (como los discos blandos de “8” utilizados en los años setenta) puede resultar difícil o imposible recuperar los datos. Los metadatos pueden apoyar la gestión de los distintos soportes mediante el registro del tipo y la edad del soporte de almacenamiento y las fechas en las que se refrescaron los ficheros por última vez.
- Transcurrido un periodo largo de tiempo, incluso los formatos de fichero más comunes pueden convertirse en obsoletos, lo que significa que las aplicaciones actuales no pueden reproducirlos. Los gestores de la preservación deben emplear estrategias de preservación que garanticen que los recursos migren de antiguos formatos a otros nuevos equivalentes (migración), o la imitación del antiguo entorno de reproducción en el nuevo hardware y software (emulación). Tanto las estrategias de emulación como las de migración requieren metadatos sobre los formatos de los ficheros originales y los entornos de hardware y software que los soportan.

- Las acciones de preservación pueden implicar modificaciones de los recursos originales o cambios en su modo de reproducción. Esto puede poner en duda la autenticidad del recurso. Los metadatos pueden ayudar a soportar la autenticidad del recurso mediante la documentación de la procedencia digital de dicho recurso, su cadena de custodia y el historial de cambios autorizados.

El modelo de datos PREMIS define cinco entidades: Entidades Intelectuales, Objetos, Agentes, Acontecimientos y Derechos (figura 8).

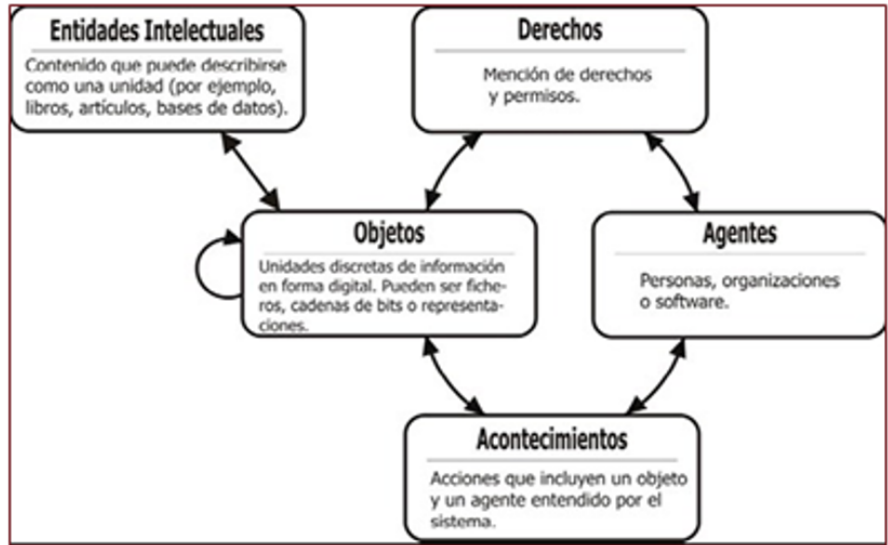


Figura 8. El modelo de datos PREMIS
Fuente. (Caplan, 2009)

Se define la entidad intelectual como “un conjunto de contenido que se considera como una sola unidad intelectual para los propósitos de gestión y descripción: por ejemplo, un libro, un mapa, una fotografía o una base de datos”. PREMIS no define los metadatos correspondientes a las Entidades Intelectuales porque existen muchos estándares de metadatos descriptivos entre los que se puede elegir. Establece que, en un sistema de preservación, un objeto debe estar asociado a la entidad intelectual que representa mediante la inclusión de un identificador de dicha entidad en los metadatos del objeto (por ejemplo, un ISBN como enlace a la Entidad Intelectual).

Mets

El formato METS es un formato estándar para codificación y transmisión de metadatos. Está pensado principalmente para el envío de los ficheros, imágenes y objetos multimedia de una biblioteca digital. METS utiliza la estructura de etiquetas tipo XML. (Library of Congress Network Development, 2016). Un documento METS está compuesto por 7 secciones principales (no son obligatorias todas ellas):

- **MetsHdr** (Mets Header). Información del documento METS: fecha y hora, nombre de la persona que lo crea, etc.
- **DmdSec** (Descriptive Metadata). Descripción del objeto al que se hace referencia en el documento METS. Los metadatos pueden estar definidos de dos maneras distintas: **1.** En forma XML en un estándar distinto a METS, podría ser en Dublin

Core o en MODS. La descripción en gredos está hecha en dublin core cualificado (DCQ) pero el formato que se visualiza es DC simple. 2. En cualquier forma textual, binaria pero codificada en Base64.

- AdmSec (Administrative Metadata). Contiene los metadatos administrativos sobre los ficheros que forman el objeto digital y la fuente del que se han obtenido dichos ficheros. Existen cuatro formas principales de metadatos administrativos disponibles para su utilización en un documento METS:
 - Metadatos técnicos: información relativa a la creación, formato y características de utilización.
 - Metadatos sobre derechos y propiedad intelectual: copyright y licencias.
 - Metadatos sobre la fuente: metadatos descriptivos y administrativos de la fuente de la que se ha derivado el objeto digital.
 - Metadatos sobre el origen digital: información sobre las relaciones origen/destino entre los ficheros del objeto digital.
- FileSec (File groups) son los ficheros que comprenden la versión electrónica del objeto digital. Estos ficheros se agrupan en <fileGrp>: por ejemplo, podría haber distintos elementos para los archivos master, versiones pdf, versiones reducidas, etc.
- StructMap (Structural Map) define la estructura jerárquica del objeto y nos permite navegar por él.

- SmLink (Structural Links) se utiliza para indicar hiperlinks con el estructural map.
- Behaviour section se utiliza para asociar comportamientos ejecutables con los contenidos del objeto METS (Library of Congress Network Development, 2016).

En la tabla siguiente se identifican las categorías reconocidas y definidas en el esquema.

Dublin Core (norma descriptiva) (Association for Information Science and Technology, 2013), en el modelo OAIS (norma internacional) (CCSD, 2012), PREMIS (especificación para preservación), en el modelo ISO/TR 23081 (International Organization for Standardization, 2011) y en el modelo METS (Contenedor de metadatos o codificador de los mismos para facilitar la transferencia de un repositorio a otro) (Library of Congress Network Development, 2016). Se incluye, igualmente la categoría establecida por la Unesco en sus Directrices de preservación (UNESCO, 2004).

Tabla 1. Relación de categorías de metadatos

Dublin Core	OAIS	Directrices UNESCO 2003	ISO 23081	METS	PREMIS
Contenido		Descubrimiento del recurso (Encontrar, evaluar y mantener accesible y comprensible el recurso)			
	Descriptivos de la información			Descriptivo	Descriptivo
Instalación					
Propiedad intelectual		De gestión del recurso digital (“administra los flujos de trabajo sobre cómo se crean, transforman y utilizan, así como los derechos asignados”)			
				Administrativos	
					Técnicos
					Estructurales
				Funcionales	
	Preservación	Preservación (“describen los medios de acceso, así como los elementos de los metadatos de gestión de recursos que son necesarios para la gestión de la preservación”)	Conservación		
			Negocio electrónico		
	Empaquetamiento				

Fuente. (Moro-Cabero, 2013)

La observación de la tabla permite vislumbrar la diversidad de categorías propuestas.

En el esquema de metadatos dublin core sobresalen metadatos vinculados a la descripción del contenido del recurso y al modo de su localización, así como a metadatos específicos a derechos y licencias. La orientación de la norma de naturaleza descriptiva, condiciona la existencia de estas categorías. No obstante, existen diferentes archivos que han utilizado el marco dublin core para la realización del esquema de metadatos, como son los esquemas de los archivos nacionales de (Comité Interministériel sur les Métadonnées du Québec, 2010). Concretamente, el estándar de este último contiene un índice de concordancia respecto a los metadatos dublin core.

En el modelo OAIS, centrado en el repositorio, destacan categorías de identificación del contenido de la información, de metadatos para la preservación y para su empaquetamiento o encapsulación. Se trata, esta última, de información sobre la descripción de la preservación asociada, que es necesaria para ayudar en la preservación del contenido de la información.

La especificación técnica ISO/TS 23081 presenta categorías orientadas a facilitar la descripción del documento digital y su recuperación, el objetivo de conservación, la gestión de sus derechos y licencias, así como una categoría específica a la gestión de las actividades de negocio en las organizaciones. Finalmente, el estándar METS, diferencia entre categoría administrativa, descriptiva y funcional.

Del conjunto de estándares analizados, únicamente dos registran directamente la categoría de metadatos de preservación, además de las orientaciones enunciadas por la Unesco, donde se detallan, a modo de ejemplo, tipologías de metadatos para la preservación empleadas por la Biblioteca Nacional de Nueva Zelanda, tales como: metadatos de descripción del objeto digital, de descripción de las características técnicas de los ficheros dentro del objeto; de descripción de los acontecimientos o procesos y de descripción de las actualizaciones de metadatos.

El modelo OAIS, incluye la categoría de preservación para asegurar en el tiempo la información.

Los metadatos vinculados a esta categoría dan muestra del pasado y presente del recurso y dan una seguridad de que el recurso es identificable de modo unívoco y no será alterado y se mantendrá comprensible en un futuro. Específicamente se señala en el estándar que este set de metadatos de preservación puede ser categorizado como “Provenence, Reference, Fixity, Context and Access Rights information”.

En el modelo ISO 23081, la especificación técnica establece los metadatos de preservación de tipo técnico, estructural, de almacenamiento y aquellos vinculados a los procesos de gestión del recurso: acceso, migración, conversión, seguridad, transferencias, etc.

El modelo PREMIS, específico a la preservación, acota el conjunto de metadatos de preservación, conformado por el subconjunto resultante de la confluencia de diferentes categorías de metadatos: técnicos, -vinculados a los formatos- descriptivos, estructurales, reglas de gestión del repositorio y otra información detallada sobre agentes, soportes, derechos, etc.

En el apartado siguiente, mediante la comparativa de propuestas, analizamos los metadatos de preservación aportados por diferentes modelos con el objetivo de determinar aquellos que se reiteran en las distintas iniciativas y que nos orientan para identificar el set de metadatos más apropiados.

Taxonomía de metadatos de preservación

En el 2006, Candas Romero nos aportaba la coincidencia de algunos de los atributos básicos a considerar sobre el objeto digital, entendidos como atributos para la preservación.

Analiza 3 iniciativas de metadatos: PREMIS v.2005, CEDARS y LoC, y demostraba con esta comparativa, que en dichas iniciativas, se percibía una tipología de metadatos que deberían de ser considerados para los objetivos siguientes: (Candas Romero, 2006)

- Identificador unívoco del recurso o información.
- Modo de asegurar la autenticación.
- Modo de establecer las relaciones contextuales.
- Características técnicas o historial evolutivo para afrontar la preservación..

- Conocimiento sobre las tareas propias de preservación (Cabero, 2013).

En la normativa OAIS estas funcionalidades son observadas al definir los atributos de la preservación digital. En la tabla nº 3 se reúnen los metadatos integrantes de la preservación vinculados a su funcionalidad, además, se definen sus tipologías: reference, provenance, fixity y context information.

Tabla 2. Funcionalidad y tipología de los metadatos de preservación-Modelo OAIS.

Funcionalidad de metadatos de preservación	Tipología de metadatos de preservación OAIS	Detalle descriptivo
Identificador y descriptor del recurso digital.	DESCRIPCIÓN-LOCALIZACIÓN	Información que identifica si es necesario describir uno o más mecanismos usados para proveer <i>identificadores</i> asignados para el contenido de la información. También provee otras identificaciones para el sistema de modo <i>unívoco</i> .
Historial evolutivo del recurso digital Conocimiento sobre el historial de preservación	PROCEDENCIA	La información que documenta la <i>historia</i> del contenido de la información. Información sobre el origen de las fuentes, así como sobre <i>cambios</i> que han ocurrido desde su origen y cómo han sido <i>custodiados</i> desde su origen.
Aseguramiento de la autenticidad del recurso (integridad + identidad)	EVIDENCIA	Documenta los mecanismos de autenticación y provee información sobre autenticación para asegurar que el contenido no sea alterado de modo no documentado.

Detalle de las relaciones Contextuales (comprensión del contexto objeto y programa de preservación)	CONTEXTO	Información que <i>documenta las relaciones</i> del contenido y su entorno. Incluye por qué fue creado y cómo se relaciona con otros.
Historial evolutivo y elementos para la preservación	DERECHOS DE ACCESO A LA INFORMACIÓN	Identifica el acceso y las restricciones de acceso al contenido de la información, incluyendo el marco legal, licencias y control de acceso.

Fuente. (Moro-Cabero, 2013)

Ambos se orientan a almacenar detalles diversos del recurso: su historial, su autenticación, su información de tipo técnico, así como los derechos y licencias a los que están sujetos los recursos u objetos digitales.

En los entornos electrónicos de archivo, además, es preciso ahondar en la causa documental. Ello se consigue con información detallada sobre el contexto (de producción y de vinculación a la agrupación correspondiente) y sobre la integridad del documento (para asegurar la evidencia).

En atención a los antedichos objetivos informativos reconocemos diversas categorías de metadatos: los que detallan su historial suelen ser reconocidos como metadatos de procedencia (provenence) o de acontecimientos (custody); aquellos que detallan la autenticación los denominamos metadatos de autenticación (“fixity”), etc.

Varias son las tipologías de metadatos que confluyen bajo el paraguas de preservación.

Así:

- Historial de todas las acciones programadas sobre el recurso, incluyendo cambios, decisiones y consecuencias (metadatos de procedencia o/y de gestión, denominados también de gestión de procesos).
- La autenticación de la información como hechos técnicos o historia de la custodia (metadatos de autenticación).
- Detalles técnicos sobre el formato, la estructura y el uso del contenido digital (metadatos técnicos o de características técnicas de ficheros y e programas de preservación).
- La responsabilidad y los derechos de la información aplicable a las acciones de preservación (metadatos de gestión derechos, a menudo incluidos bajo metadatos descriptivos o de gestión).
- Identificación del recurso como tal (metadatos de descripción o de descubrimiento del recurso).
- Metadatos de administrar la preservación (a menudo incluidos bajo el paraguas denominativo de gestión o de procedencia).

Resaltamos, como elemento de consideración, la gestión de derechos de acceso y restricción, desde el enfoque de archivo, así como las actividades de gestión a los que está sujeto, funcionalidades de gestión de archivo, seguridad, acceso, clasificación, valoración, disposición, transferencia, etc.

Los metadatos de procedencia y autenticación surgen y son vitales durante los primeros años del recurso (de 0 a 10 años), mientras que los metadatos técnicos se supeditan a las necesidades de conservación a largo plazo, esto es, en entornos electrónicos hablamos de unos 10 años. Por el contrario, los metadatos de gestión de derechos pueden ser importantes durante periodos de tiempo mayor debido a los plazos de licencias y derechos marcados en la legislación (+ de 50 años).

No obstante, obsérvese que estos plazos pueden variar en atención al tipo de recurso digital a preservar.

En su conjunto, los metadatos de preservación supeditados a las evoluciones necesarias marcadas por las necesidades de la comunidad de usuarios y de las características técnicas de los recursos o/y causa documental se mantienen en el tiempo (a largo plazo). En la tabla siguiente aportamos la confluencia de taxonomías de metadatos en diferentes modelos conceptuales.

Tabla 3. Taxonomías de metadatos en diversos modelos conceptuales

Recurso/ in-formación	Identificación	Contexto	Procedencia	Autenticación	Derechos de acceso	Técnica	Localización
Modelo OAIS (2012)	Reference	Context	Provenance	Fixity	Access Rights.		
Modelo PREMIS	Descriptivos	Estructurales Técnicos				Técnicos	Descriptivos
Modelo ISO 23081	Negocio electrónico	Estructurales y de almacena miento.	M. sobre los procesos de gestión			Técnicos	Descriptivos y de localización
Modelo e- Arq-Brasil	Elementos identificativos entidad documento (identificación)	Datos componentes digitales: formatos, dato, entidad documento: relaciones	Datos básicos entidad evento de preservación: migración, replicación	Datos básicos evento de preservación: Descifrad o Validación de firma digital Verificación de fijeza Cálculo hash	Datos básicos entidad documento: derechos de acceso	Datos básicos entidad “Componente digital”	Datos, entidad documento (recuperación)

Fuente. (Moro-Cabero, 2013)

En el modelo OAIS se registran los metadatos siguientes vinculados a la categoría descriptiva de metadatos de preservación.

Tabla 4. Taxonomía de metadatos de preservación Modelo OAIS.

OAIS	
Información de referencia (reference)	Identificadores unívocos internos y externos del recurso, de la información y del sistema.
Información de contexto (context)	Razón de la creación, versión, versiones anteriores, reemplazados por, requeridos por, referenciados por, migración, formato, formato de, formato anterior, contenido, etc.
Información de procedencia (provenance)	Historia del proceso de la ingesta: Institución, data y hora de la ingesta, tipo y descripción del evento; Historia de la custodia: institución, data y hora, tipo de acción, descripción de la acción y mecanismo técnico.
Información de autenticación (fixity)	Firma digital, marca de agua, sello de data, encriptación, documentación verificadora de autenticidad
Información sobre el Acceso (Access Rights)	Estatuto de acceso, derechos del recurso: patentes, permisos de archivo, copyrights; Condiciones de uso: acciones, agentes, detalles... Contratos y otros derechos.

Fuente. (Moro-Cabero, 2013)

En el modelo PREMIS se detallan los siguientes metadatos para la preservación

Tabla 5. Taxonomía de metadatos de preservación modelo PREMIS

PREMIS	
Metadatos descriptivos (identificadores diferenciadores del recurso)	<i>Datos básicos de la entidad objeto:</i> identificador único del objeto, tamaño, nombre original del objeto
Metadatos estructurales (describen la estructura interna del recurso y las relaciones entre sus partes)	<i>Algunos datos básicos de la entidad objeto:</i> información sobre la creación, sobre propiedades significativas, sobre soporte, sobre su formato, relación con otros objetos y otro tipo de entidades.
	<i>Datos básicos de entidad acontecimiento:</i> identificador único del acontecimiento, historia y tipo, fecha y hora, descripción detallada.
AUTENTICACIÓN	<i>Datos básicos de entidad objeto:</i> información sobre la firma digital, Fijeza de la información, como la suma de verificación (mensaje cifrado) y el algoritmo utilizado para obtenerla.
DERECHOS DE ACCESO	<i>Metadatos básicos de la entidad derechos:</i> identificador único de la mención de derechos, estado de copyrights en términos de licencia o ley, acción o acciones que permiten la mención de derechos, cualquier restricción sobre la acción, agentes implicados en la acción de derechos, etc.
Metadatos técnicos (formatos)	<i>Datos de Entidad objeto:</i> el formato del objeto, que puede especificarse directamente o mediante un enlace a un registro de formatos.
Metadatos descriptivos	Datos básicos entidad objeto: Dónde y en qué soporte se almacena.
Localización de un recurso y selección atendiendo a las necesidades	Identificador del objeto.

Fuente. (Moro-Cabero, 2013)

En el modelo ISO 23081-2 se detallan los metadatos siguientes que se registran a continuación.

Tabla 6. Taxonomía de metadatos de preservación modelo ISO 23081-2

ISO	
Metadatos para la gestión de la propiedad Intelectual.	Gestión de los derechos de propiedad intelectual de unos agentes sobre sus recursos de información como al uso de los mismos. Implica la descripción, valoración, negociación, control y seguimiento de estos derechos con metadatos que describan las 3 entidades: a) partes involucradas: creador, editor y usuario; b) el contenido en todas sus formas y los propios derechos (permisos, restricciones, retribuciones por el uso, etc.).
Metadatos estructurales y de almacenamiento.	<u>Metadatos sobre el documento en el momento de la incorporación</u> Formato y necesidades técnicas que permitan asegurar la accesibilidad y facilitar la conservación, documentar la estructura, información sobre cambios en la estructura lógica y física y en los atributos técnicos.

Metadatos sobre los procesos de gestión de documentos	ACTIVIDADES DE GESTIÓN <i>En el momento de la incorporación.-</i> Identificar funcionalidades de los documentos, documentar vínculos con otras entidades, identificar agentes, documentar normas de seguridad y de acceso. <i>Después de la incorporación.-</i> Metadatos que documenten la autenticidad, fiabilidad, integridad, disponibilidad conformidad, exhaustividad, conservación, disposición, almacenamiento y acceso. Documentar reglas para la reproducción de documentos, diferentes tipos de copias, autorizaciones de reproducción, etc. ACCESO <i>Para el acceso en el momento de la incorporación:</i> metadatos que informen sobre la ubicación del documento y su vinculación con entidades, información descriptiva que facilite el uso y comprensión: título, descriptores, resumen..., facilitar la clasificación de funciones, clasificación de documentos e indización. <i>Después de la incorporación:</i> control de metadatos sobre accesibilidad de modo continuado, cambios diversos que deben de ser registrados para explicar cambios y contextos. SEGURIDAD <i>En el momento de la incorporación.-</i> Restricciones de acceso y de ocultación del acceso. <i>Después de la incorporación.-</i> Restricciones marco ley o necesidad organizativa cambiantes a lo largo del tiempo y documentados.
Metadatos técnicos	<u>Metadatos sobre el documento en el momento de la incorporación.-</u> Datos sobre propiedad física y química, relaciones entre los datos o elementos de formato del documento, documentar los requisitos para que pueda estar disponible o ser reproducible o representable, datos sobre la posibilidad de migración a un software diferente, datos sobre la posibilidad de representación mediante emulación, datos para iniciar actividades de gestión de datos y de formato para proteger el deterioro del soporte.
Metadatos descriptivos y de localización	Metadatos sobre el documento en el momento de la incorporación Fecha y hora de creación, identificación y descripción de agentes implicados.

Fuente. (Moro-Cabero, 2013)

La preservación digital

La preservación digital o en inglés digital preservation (DP), se define como los procesos y acciones que contribuyen a garantizar el acceso continuo e indefinido a la información y los registros que existen en un formato digital. (Van der Merwe, 2009). Ferreira la define como “la capacidad de asegurar que la información digital se mantiene con las cualidades accesibles y suficientes de autenticidad, que se pueden interpretar en el futuro con uso de una plataforma tecnológica diferente utilizado al momento de su creación” (Ferreira, 2006), La preservación digital tiene como objetivo superar la debilidad del soporte físico, la obsolescencia tecnológica y la vulnerabilidad del medio digital para garantizar la autenticidad, integridad, fiabilidad, así como el acceso seguido a la información, siendo esta la única manera de garantizar y promover la memoria colectiva e institucional.

En las directrices para la preservación digital se define la preservación como las acciones destinadas a mantener la accesibilidad de los objetos digitales a largo plazo (UNESCO, 2004). En digital preservation coalition-DPC Handbook (2008) se define como las actividades necesarias para asegurar el acceso continuado a materiales digitales hasta cuando sea necesario, a pesar de los obstáculos que representan los fallos en los soportes o los cambios tecnológicos. (Digital Preservation Coalition, 2008)

En Trusted digital repositories (Research Libraries Group, 2002), indica que la preservación digital son las gestiones de actividades

necesarias para asegurar el mantenimiento a largo plazo de la cadena de bits y la accesibilidad continuada del contenido.

Desde hace más de tres décadas, casi todo el contenido fue creado en papel. Los medios de comunicación y las personas generaron entornos de almacenamiento para largos periodos de tiempo bajo una serie de condiciones adecuadas para el cumplimiento del objetivo. Los frecuentes y constantes cambios en la tecnología demandan un hardware más rápido, un software más eficiente y robusto y una serie de nuevas especificaciones de formato. Así, el contenido almacenado en los medios tradicionales, que utilicen software discontinuado y formateado con especificaciones obsoletas o caducas a menudo no tiene una oportunidad de ser útiles o legibles más de una década.

La visión sobre el futuro de la preservación digital y las actividades requeridas se describen en una serie de planes de investigación. Una de las principales observaciones de ellos es un cambio lento en responder las preguntas que ayudan a solucionar problemas en el mantenimiento y preservación de la información digital con el tiempo para asegurar que el problema no aparecerá en toda su complejidad. Con los avances en la investigación de forensia digital hasta el momento, la comunidad ha desarrollado una sólida comprensión de los problemas y los enfoques necesarios para solucionarlos, convirtiendo las actividades de preservación digital en algunas áreas, en una tarea de ingeniería desafiante que requiere una mayor atención.

La preservación de evidencia digital es con frecuencia un aspecto central de las órdenes judiciales, sin embargo, qué evidencia y cómo se preserva a menudo está abierta a interpretación; el tipo de organización, de dispositivo y la tecnología hardware y software también juega un papel clave en la capacidad de preservar y recuperar la evidencia digital, y en su admisibilidad en la corte.

Así también, la preservación digital requiere procedimientos específicos y las técnicas adecuadas para cada tipo de formato y soporte (Arellano, 2004), además, la mayoría de las estrategias propuestas, incluyendo la migración, se basan en las conversiones sucesivas de objetos digitales para nuevos formatos y que incluso algunos de estos enfoques ni siquiera intentan preservar el objeto digital en su formato original, lo que significa que se produce inevitablemente la corrupción y la degradación de la misma. (Hoorens, 2007)

Hasta el momento, los tribunales penales internacionales (International Criminal Court- ICC) han proporcionado poca orientación sobre la mejor forma de preservar la evidencia digital.

Además, la ICC no parece tomar medidas para asegurar que la información digital se ha preservada adecuadamente.

Por lo tanto, surgen preguntas en cuanto a qué métodos o modelos deben utilizarse para asegurar que la evidencia se preserva de una manera que satisfaga a los despachos legales. Es especialmente saber qué métodos o modelos de preservación son adecuadas para

las evidencias obtenidas a partir de fuentes no verificables. (Ashoire, Bower, & Warden, 2013).

La preservación digital trata sobre la mitigación de esos riesgos. Según la Asociación Americana de Bibliotecas (ALA) al referirse al campo de la preservación digital indica que “combina las políticas, estrategias y acciones que garanticen el acceso a los contenidos digitales a través del tiempo”. Jones y Beagrie lo definen como “la serie de actividades de administración necesarias para garantizar el acceso permanente a los materiales digitales para el tiempo que sea necesario” (Beagrie & Jones, 2008).

Un análisis inicial de la materia por el grupo de trabajo sobre el archivo de información digital se puede encontrar en el informe desarrollado por (Garrett, y otros, 1996). Ninguna generación había producido antes tantos documentos como la nuestra. La mayoría de los testimonios que dejamos son digitales. Nuestra preocupación es si esta documentación llegará a las generaciones futuras. Si además unimos a esto el hecho de que los soportes son frágiles y que los cambios en las tecnologías son frecuentes, el panorama no es muy alentador. (Beagrie & Jones, 2008) afirma que la información digital nunca sobrevivirá accidentalmente.

Waller y Sharpe, mencionan que la preservación digital son las acciones necesarias para asegurar un acceso continuo y pertinente a la información digital durante el tiempo que sea requerido y para cualquier finalidad legítima. (Digital Preservation Coalition, 2006)

La preservación digital se define como un conjunto de procesos dirigidos a conservar la información en formato digital. No existe preservación digital si no se mantiene la posibilidad de acceder a los recursos digitales. El objetivo de la preservación digital es permitir a los futuros usuarios recuperar, acceder, descifrar, ver, interpretar, entender y experimentar documentos y datos de forma significativa y válida. (Rothenberg J. , 1998)

Amenazas y Estrategias

Los repositorios institucionales están formados y funcionan desde hace unos años, los esfuerzos deben dirigirse ahora a afianzar y a asegurar el acceso a la información contenida en ellos en un futuro cercano y a largo plazo. Nos enfrentamos a amenazas que hay que tener en cuenta a la hora de pensar en la preservación digital:

- Los objetos digitales son inestables.
- Los equipos y los programas tienen una vida media de unos pocos años.
- Pérdidas por desastres naturales, accidentes, averías, virus...
- Barreras al acceso: claves, cifrado, acceso restringido.
- Responsabilidades poco claras.
- Falta de conocimientos o de recursos.
- Problemas legales: copyright.
- Descripción inadecuada: imposible recuperación.
- Pérdida de información sobre el contexto.

Las principales estrategias aplicadas actualmente para frenar la pérdida de información digital, debida a las causas que se han expresado anteriormente, son principalmente:

- Preservación de la tecnología.
- Migración de los datos.
- Emulación de las aplicaciones informáticas originales.

Pero, según un informe de la comunidad europea, (European Commission, DG Information Society, 2002) estas estrategias son soluciones inmediatas para un problema a largo plazo. Es decir, nuestros conocimientos actuales más punteros no nos garantizan la capacidad de preservar lo que estamos creando para un futuro medio y lejano.

No se trata solo de problemas técnicos, la razón por la que nuestros esfuerzos para preservar el objeto digital no son suficientes es que existen retos más allá de los tecnológicos que representan obstáculos más complejos que hay que superar. Son problemas de distinta índole:

- *Legales*: si no tenemos el permiso del titular no podremos preservar un recurso reproduciéndolo o reformateándolo.
- *Económicos*: si no contamos con los medios necesarios no podremos garantizar la perdurabilidad de los documentos a lo largo de los años.
- *Institucionales*: si no se asegura el compromiso institucional permanente, si no están convencidos todos los implicados de la

necesidad de colaborar, si no se puede verificar si se cumple todo lo que se promete, no podremos preservar a largo plazo.

La comunicación de la Comunidad Europea expone una situación que seguía tan precaria como la observada en el Digicult report, tres años antes: “Actualmente la experiencia con que se cuenta [...] es escasa, el marco jurídico inestable, los recursos escasean y el resultado de los esfuerzos de preservación es incierto”. (European Commission, DG Information Society, 2002)

Riesgos de preservación digital

Valiosa información científica y cultural son creadas, almacenadas, administradas y accedidas de forma digital, pero la amenaza de la pérdida de ellos a largo plazo es alta. Así, cualquier actividad de gestión de datos e información constituye una amenaza, por ejemplo, cuando se copian, se mueven, se cambia de nombre o formato. Los medios digitales son frágiles, pueden dañarse y son de corta duración.

Con el pasar del tiempo, los cambios en el entorno presentan riesgos adicionales: la tecnología de soporte y lectura se vuelve obsoleta, la tecnologías de software y hardware necesarios para acceder a ellos siguen una evolución a un ritmo rápido y caen en la obsolescencia; los formatos que se utilizan para representar los objetos digitales se discontinúan rápidamente, sobre todo, el material digital codificado en formatos propietarios son inaccesible cuando el software asociado ya no está disponible; los cambios en las prioridades culturales y financieras de las organizaciones aportan al riesgo de la continuidad

de la accesibilidad y la preservación a largo plazo de nuestros activos digitales.

Metas de preservación digital

En las Directrices para la preservación digital, la UNESCO, define a la preservación como las acciones destinadas a mantener la accesibilidad de los objetos digitales a largo plazo.

Las metas de la preservación digital son para garantizar que

- a.** El contenido digital este en el control físico del repositorio.
- b.** El contenido digital se puede identificar y recuperar en el futuro de forma única y persistente.
- c.** Que se disponga de información suficiente para que el contenido digital puede ser entendido por la comunidad designada.
- d.** Que las características significativas de los activos digitales se conservan incluso si cambian los soportes o representaciones físicas de los datos.
- e.** Que los medios físicos son cuidados y la manipulación se detecten y reparen (fijación).
- f.** Que los objetos digitales siguen siendo renderizables o ejecutables.
- g.** Que los objetos digitales permanezcan en conjunto y que está definido cómo todas las partes se relacionan entre sí (integridad).
- h.** Que los objetos digitales son lo que pretenden ser (autenticidad).

En el caso de instituciones de investigación criminal, la escena del crimen es un factor decisivo en casos judiciales, por lo que se requiere un modelo de preservación digital que considere el entorno de la evidencia al momento de preservarla.

Metodologías de preservación digital

Los profesionales de la preservación digitales deben decidir que metodología de preservación mitiga más adecuadamente el riesgo de preservación en su institución. Esto no siempre es una elección sencilla. Está determinada por sus requisitos de preservación, recursos, directrices organizacionales, habilidades y disponibilidad de las herramientas necesarias y la naturaleza del riesgo que se va a mitigar. (Bearman, 1999) Existen argumentos fundamentales a favor o en contra de ciertas decisiones de la metodología como una cuestión de principios, sobre todo entre la migración y la emulación (Stawowczyk Long, 2009).

Pero, puesto que cada metodología aborda riesgos específicos de preservación y tiene fortalezas y debilidades específicas, se entiende cada vez más que estas son metodologías complementarias (Anderson, Delve, & Pinchbeck, Toward A Workable Emulation-Based Preservation Strategy: Rationale and Technical Metadata., 2010) y que su elección es dependiente del contexto (Dappart & Farquhar, 2009); y depende de los requisitos citados en el contexto particular. Es importante para una organización definir una política de preservación clara para que pueda desarrollar la estrategia de preservación más adecuada con las opciones correctas de las metodologías de preservación.

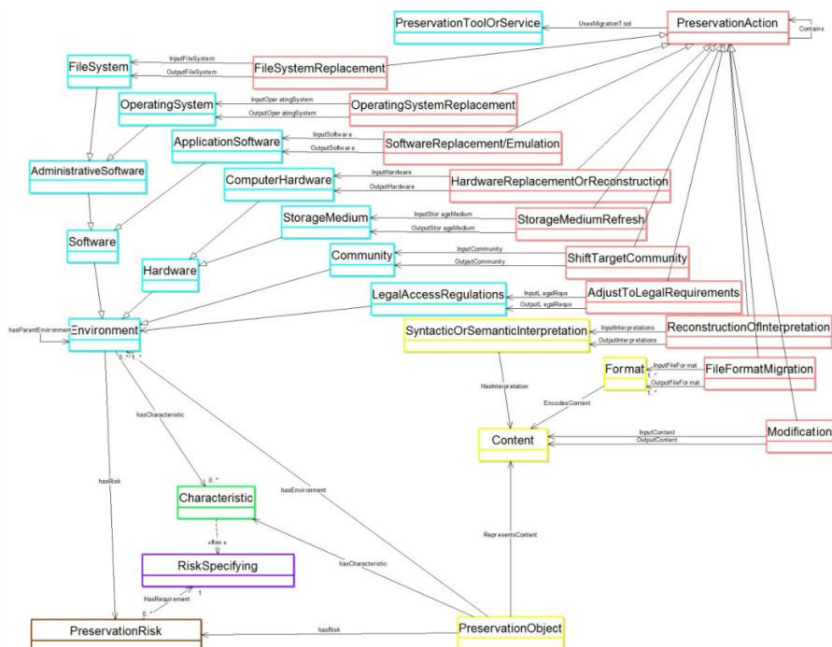


Figura 9. Ejemplo de Metodologías de Preservación y su relación con los objetos de preservación y el entorno de riesgos.

Fuente. (Dapart & Farquhar, 2009)

Opciones metodológicas:

Chue Hong sugieren siete diferentes opciones metodológicas para la preservación y sostenibilidad de los programas, en particular: (Hong & Neil, 2012).

- *Technical preservation (techno-centric).*- Preservar el hardware y el software original en el mismo estado en que son ahora.
- *Emulation (data-centric).*- Emula el entorno de hardware/operativo original, manteniendo el software en el mismo estado.
- *Migration (functionality-centric).*- Actualización del software según se requiera para mantener la misma funcionalidad.

- *Cultivation (process-centric).*- Mantener actualizado el software al pasar a un modelo de desarrollo abierto.
- *Hibernation (knowledge-centric).*- Preservar el conocimiento de cómo resucitar/recrear la funcionalidad exacta del software en una fecha posterior.
- *Deprecation.*- Retirarse formalmente el software sin salir de la opción de la reanimación/recreación.
- *Procrastination.*- No hacer nada.

Otros autores proponen a más de las especificadas las siguientes:

- *Copias de seguridad o de respaldo (backup).*- Algunos soportes de respaldo pueden ser: Cintas, DVD, CD, Blu-ray, Unidad Jaz, Pendrive, Discos virtuales. Si bien esta estrategia es válida, únicamente funciona a corto plazo pues depende de la obsolescencia del soporte físico de almacenamiento.
- *Renovación del soporte físico de almacenamiento (refresh).*- El refresco puede ayudarle a conservar por más tiempo sus respaldos. Consiste en pasar la información digital de un soporte a otro nuevo o más moderno para reducir el riesgo de pérdida debido al deterioro del soporte físico.
- *Encapsulamiento.*- El encapsulamiento consiste en preservar el recurso digital y toda la información necesaria para codificarlo y traducirlo. Se guardan datos sobre cómo interpretar el archivo en cualquier sistema futuro. Para aplicar esta estrategia se pueden utilizar estructuras como archivos XML, que mantienen

la relación entre todos los componentes de la información que se debe preservar (objeto digital, metadatos, identificador y especificaciones del software).

- *Conservación técnica.*- Conservación técnica consiste en la intención de mantener el software y hardware en el mismo estado funcional, que generalmente implica adquirir piezas de repuesto cuando sea necesario. Naturalmente, esto se convierte a menudo más costoso con el pasar del tiempo y las piezas inusuales a ser más difíciles de encontrar. Shustek y Zabolitzky, observan que el código fuente es el único artefacto que contiene toda la información sobre el funcionamiento de un producto de software, y todo lo demás es “esencialmente rumores”. (Shustek, 2006), (Zabolitzky, 2002)
- *Emulación.*- Emulación es una metodología de preservación en el que el objeto digital se mantiene (en gran medida) sin cambios, pero la plataforma sobre la que se va a trabajar ha cambiado. Puesto que un objeto digital obsoleto no puede ser usado directamente en una plataforma más moderna, un software llamado emulador recrea el ambiente de equipo original en la plataforma más moderna. (Rothenberg J. , 1998). Para los objetos digitales dinámicos, como los programas informáticos, la emulación es el método de preservación más adecuado. Todo el software que se ejecutaba en la antigua plataforma puede funcionar en la nueva con el mismo emulador. No obstante, la

emulación es una tarea muy compleja (Kuchera, 2011) y costosa. Pero el obstáculo más importante a la emulación es la posible violación de derechos de autor, de la preservación de software o hardware propietario. (Charlesworth, 2012) (Anderson D. , 2011). (Guttenbrunner & Rauber, A Measurement Framework for Evaluating Emulators for Digital Preservation., 2012)

Ejemplos de proyectos para el desarrollo de soluciones de emulación son el proyecto KEEP (KEEP Project., 2012) que ha desarrollado un marco de emulación y el proyecto Dioscurus (Van Der Hoeven, 2007). La emulación se ha defendido en el campo de la preservación digital desde la década de 1990. (Bearman, 1999). Para preservar a su vez, el software de emulación, sin crear una cadena interminable de emuladores. Rothenberg propuso crear una capa entre el emulador y la plataforma, llamada una máquina virtual de emulación, que haría que el emulador independiente de la plataforma en el futuro previsible (Van der Hoeven & van Wijngaarden, 2005). (Van Der Hoeven, 2007).

- *Migración.*- Migration (Garrett, y otros, 1996) es una metodología de preservación en el que los objetos digitales se convierte de un formato a otro. Esto puede ser una conversión de un formato de archivo a otro, o también puede ser una conversión en codificaciones de nivel superior, como, por ejemplo, de un lenguaje de programación a otro.

Estas metodologías de preservación no conservan los bits, pero si el contenido de los objetos digitales. En la práctica, generalmente, los programas que realizan la migración no se aplican correctamente o pierden las características del objeto en la conversión (Kulovits, y otros, 2009). Las migraciones son validadas, y asegura que las “características significativas”, las características que se consideran esenciales por las partes interesadas se conservan (Thaller, Heydegger, Schnasse, S., & Chudobkaite, 2008).

Migración, significa transportar información de un tipo de formato o sistema a otro. (Hoorens, 2007). Este tipo de migración implica reescribir y recompilar el código fuente de otro entorno operativo. (Hong & Neil, 2012). La reescritura puede ir desde un pequeño chequeo a una revisión completa del código en un nuevo lenguaje de programación.

- *Cultivo*.- Cultivo consiste en abrir el software para el desarrollo exterior por compartir el código fuente. Cuando se trata de hacer un formato obsoleto, el código fuente de un procesador viejo es probable que sea mucho más útil que la información contenida en un registro de formato (Rosenthal, 2010, pág. 5).
- *Hibernación*.- Hibernación consiste en colocar el producto de software completo (incluyendo documentación y propiedades significativas) en almacenamiento de información, para volver a examinarse en una fecha posterior cuando necesita para ser utilizado. En este caso, software de código abierto es una ventaja,

porque la preparación es probable que ya cerca de terminación. (Hong & Neil, 2012).

- *Degradación y demoras.*- En realidad, estos dos enfoques, no son estrategias de conservación como tal y no se discutirá en profundidad aquí. En Resumen, degradación es una manera de señalar que una función de software específica o práctica ya no se apoyará en el futuro, considera que la dilación significa “hacer nada”. (Hong & Neil, 2012). La Degradación, proporciona cierto grado de aviso de que las partes interesadas debería considerar formas de adaptación al cambio.

La siguiente tabla, indica que acción, que enfoque y cuando aplicar cada técnica de preservación.

Tabla 7. Acción enfoque y aplicación de técnica de preservación

TECNICA DE PRESERVACION	ENFOQUE	ACCIÓN	CUANDO APLICAR
Technical preservation	techno-centric	Preservar el SW y HW original hardware en el mismo estado.	Cuando se requiere recrear la evidencia exactamente el mismo entorno para determinar la acción criminal. Hay que considerar: La rápida evolución de la tecnología que cada día ofrece nuevos equipos y software con mejores funcionalidades. El alto costo económico de la conservación y mantenimiento de equipos, que la mayoría de centros de información no están en capacidad de asumir. El deterioro físico de los equipos que en algún momento hará imposible su conservación y mantenimiento. Se predispone tener un museo de infraestructura funcional por cada tipo de HW y HW
Emulation	data-centric	Emular el hardware original y las condiciones del entorno, manteniendo el software en el mismo estado;	Se debe tomar en cuenta que se reproduce el original, no requiere un seguimiento continuo del formato del recurso, es muy útil para recursos digitales complejos. Sin embargo, hay poca frecuencia en su uso, deben actualizarse por cada nuevo sistema, y es una técnica muy costosa.

Migration	functionality-centric	Actualizar el software según sea necesario para mantener la misma funcionalidad, portar/transferir antes de obsolescencia de la plataforma.	Se utiliza cuando se requiere cambiar el soporte físico, se realiza copias periódicas de los documentos digitales a soportes más estables, cuando se desea actualizar los recursos creados por un determinado software a una versión más actual, visualizar documentos en formato propietario con otra herramienta, y cuando se desea convertir a formatos estándares o más comunes con el entorno. Esto no debe afectar la propiedad intelectual o la integridad de la evidencia. Aplicar cuando sea expresamente posible.
Cultivation	process-centric	Mantener el software ‘vivo’ hacia un modelo de desarrollo más abierto, lleva a bordo más colaboradores y difusión de conocimiento del proceso;	Se utiliza cuando se desea preservar una información y esta a su vez es útil para desarrollar nueva información, permitir que el código sea abierto al público.
Hibernation	knowledge-centric	Preservar el conocimiento de cómo resucitar/recrear la funcionalidad exacta del software en una fecha posterior;	Cuando se requiere Preservar a más de la evidencia, el conocimiento de cómo recrear la funcionalidad exacta del software en una fecha posterior;
Deprecation		Retirar el software sin salir de la opción de reanimación / recreación.	Cuando se requiera preservar la evidencia sin importar la herramienta de creación. es una manera de señalar que una función de software específica o práctica ya no se apoyará en el futuro, considera que la dilación significa “hacer nada
Procrastination		No hacer nada.	Cuando no se desea preservar la evidencia para que sea admisible al largo plazo.

Backup	Información a Preservar	Las copias de seguridad o backups son de la forma más común de preservar la información.	Este proceso consiste en grabar en algún tipo de soporte físico toda la información almacenada en un computador para poder recuperarla en caso de perderla, sin aplicar técnicas de preservación. Útil con preservación de tecnología.
Encapsulamiento		El encapsulamiento consiste en preservar el recurso digital y toda la información necesaria para codificarlo y traducirlo.	Se guardan datos sobre cómo interpretar el archivo en cualquier sistema futuro. Para aplicar esta estrategia se pueden utilizar estructuras como archivos XML, que mantienen la relación entre todos los componentes de la información que se debe preservar (objeto digital, metadatos, identificador y especificaciones del software).
Refresh Renovación del soporte físico de almacenamiento.		El refrescamiento puede ayudarlo a conservar por más tiempo sus respaldos.	Consiste en pasar la información digital de un soporte a otro nuevo o más moderno para reducir el riesgo de pérdida debido al deterioro del soporte físico. La transferencia de la información digital se realiza sin hacer ningún cambio al formato de los archivos: solamente se renueva el soporte físico. La frecuencia de refrescamiento depende de: Las políticas establecidas por el centro de información, El tipo de soporte físico, El tipo de uso del soporte físico, Las condiciones de almacenamiento del soporte, Los plazos recomendados por los fabricantes del soporte físico. Esta estrategia se complementa con las copias de seguridad. Sin embargo, no soluciona el problema de la obsolescencia de los soportes físicos. Para aumentar su efectividad, se debe combinar con otras que sí lo hagan y así aumentar la efectividad de la preservación digital

Elaborado por: El autor

Como se indicó anteriormente, ninguno de estos es inherentemente preferible, pero depende de la situación individual de la preservación. Estas metodologías específicas, en forma adaptada también se aplican a los objetos digitales que no son software.

Preservación Bit

Los bits que representan información digital se almacenan en varios tipos de data carrier (o medios de almacenamiento). Los portadores de los datos pueden dañarse físicamente, y están sujetos a la pérdida de bits, que es causada por el envejecimiento del soporte de datos. La metodología obvia para la mitigación de este riesgo es la preservación de bits, el proceso de copiar el contenido de soporte de datos bit a bit en data carrier más recientes.

Las estrategias de preservación de bits escogidas dependen de los requisitos de preservación y varían para diferentes materiales digitales. Los requisitos de confidencialidad, seguridad, la disponibilidad y los costos influyen en las estrategias de preservación (Zierau & Kulovits, 2010) . Las propiedades de transporte de datos influyen en la elección del soporte de datos, y las tasas de fracaso influyen en la frecuencia de preservación (Rosenthal, 2010). Los bits se pueden copiar como imagen del medio de almacenamiento o por la copia de los bits de los archivos almacenados en medios de almacenamientos independientes del formato de codificación del “data carrier”. (Woods, 2008). (Dappert, Jackson, & Kimura, 2013)

La preservación de bits se valida a través de la fijeza, en el que las sumas hash de cada archivo antes y después de la copia se comparan para asegurarse de que el archivo no fue dañado durante la copia (Novak, 2006), así, con la comprobación de la integridad se asegura de que todos los archivos se han copiado.

Museos informáticos

Los museos informáticos abordan la preservación digital a nivel físico en el que el software y el hardware se conservan en su estado histórico (Anderson, Delve, & Powell, *The Changing Face of the History of Computing: The Role of Emulation in Protecting Our Digital Heritage.*, 2012); (Ainsworth, Avram, & Sheard, 2012) (Demant, 2010). Utilizan equipos de almacenamiento que conserva su ambiente nativo para recuperar datos de data-carrier obsoletos, a menudo la única manera de acceder a esta información, a menos que existan tecnologías de recuperación más recientes.

Las plataformas originales son también la única manera de validar si una aplicación de emulación conserva las características significativas del sistema emulado. “Es crucial para establecer si, por ejemplo, un comportamiento inesperado exhibido por un objeto digital es el resultado de un defecto introducido durante la preservación o estaba presente originalmente” (Anderson, Delve, & Pinchbeck, *Toward A Workable Emulation-Based Preservation Strategy: Rationale and Technical Metadata.*, 2010). Afirman, además, que, si bien es importante documentar cuidadosamente las características de la plataforma con

el fin de utilizar este conocimiento más adelante, por ejemplo, en la construcción de un emulador, es un hecho que todas las plataformas tienen características indocumentadas o no-documentables.

La gran ventaja de este enfoque es que la prestación o la ejecución de objetos digitales obsoletos son tan auténticas a la original como sea posible, con la restricción de los cambios inevitables para el medio ambiente original que no puede ser reproducido. Este enfoque ofrece acceso regional limitado y las partes eventualmente podrían no ser reemplazables.

Evidencia digital

Aspectos relativos a la evidencia

Evidencia se conocen como cualquier cosa que tienden a probar lógicamente o refutar un hecho de un problema en un caso judicial (Swanson, 2006). evidencia digital se define como información de valor probatorio legal que es almacenado o transmitido en forma digital (Casey, 2011). Otra definición de evidencia digital es cualquier dato almacenado o transmitido por medio de un equipo que apoya o refuta una teoría de cómo un delito ocurrió, o puede abordar un elemento crítico como intención o una coartada (Casey, 2011). La evidencia digital plantea desafíos particulares a la Corte Penal Internacional-International Criminal Court (“ICC”). Es definida como información transmitida o almacenada in formatos digitales que puede utilizarse para procedimiento en un caso judicial.

Biros y Weiser, definen forense digital como “conocimiento científico y métodos aplicados a la identificación, colección, preservación, examen y análisis de información almacenada o transmitida en forma binaria de una manera aceptable para su aplicación en asuntos legales”. (Biros, Weiser, & Mosier, 2006) Investigación forense digital requiere procedimientos definidos que cumplen con las prácticas de la industria, la práctica organizativa y leyes adecuadas, ya sea como parte de una investigación criminal o como parte de una más general respuesta ante incidentes de seguridad. La presentación de evidencia digital es un desafío legal único frente a profesionales de informática forense (Kenneally, 2005). La evidencia en casos legales es admitida o no admitida basada en el peso relativo de su valor probatorio y perjudicial. Dado que el sistema jurídico se basa en antecedentes, investigadores forenses deben introducir la cohesión y la coherencia en el creciente campo de extraer y examinar las evidencias. (Ami-Narh, 2008)

En este proceso se toman en cuenta varios aspectos como la Identificación, el Registro e incautación, La preservación, el examen, el análisis, y la presentación del informe.

Principios relativos a la evaluación de la evidencia digital

Los principios por los que se evalúa la evidencia digital, aceptados en los procedimientos judiciales, y el peso atribuido varían ampliamente de una jurisdicción a otra. Los países con una ley de fondo común, que incluye el Reino Unido, Australia y EE.UU., comparten una serie de principios comunes.

En 1998, Sommer describe los siguientes principios básicos para evaluar la aceptabilidad de los nuevos tipos de evidencia no considerados previamente por los tribunales: (Schatz, 2007)

- Auténtica- la evidencia debe ser: “específicamente vinculada a las circunstancias y las personas acusadas, y producido por alguien que pueda responder a las preguntas acerca de ellos”. (Romano, 2005)
- Exacta - la evidencia debe ser “libre de cualquier duda razonable sobre la calidad de los procedimientos utilizados para recoger el material, analizar el material si es adecuado y necesario y, finalmente, a introducirlo en la corte - y producido por alguien que pueda explicar lo que tiene ha hecho”.
- Completa - la evidencia debe ser “capaz de decir, dentro de sus términos, una historia completa de un conjunto particular de circunstancias o eventos”.

Principios de los procedimientos relativos a la evidencia digital

Para ayudar a crear la cooperación entre los EE.UU. y otros países, el Grupo G-8 de las principales naciones industrializadas han propuesto seis principios para los procedimientos relacionados con la evidencia digital (Vacca, 2005):

1. Cuando se trata de la evidencia digital, todos los principios forenses y de procedimiento generales deben aplicarse.
2. Al incautar evidencia digital, las medidas adoptadas no deben cambiar esas evidencias.

3. Cuando sea necesario para que una persona para acceder a la evidencia digital original, esa persona debe estar capacitado para tal fin.
4. Toda actividad relacionada con la incautación, el acceso, el almacenamiento o la transferencia de la evidencia digital debe estar completamente documentado, conservado y disponible para su revisión.
5. Un particular es responsable de todas las acciones tomadas con respecto a las evidencias digitales, mientras que la evidencia digital es en su posesión.
6. Cualquier agencia, que es responsable de la incautación, acceder, almacenar o transferir evidencia digital es responsable del cumplimiento de estos principios. (Guo, 2010)

Este conjunto de principios puede actuar como una base sólida. Sin embargo, como un principio establece que si alguien debe tocar las evidencias que deben estar debidamente capacitados. Capacitación ayuda a reducir la probabilidad de que la alternancia no intencional de evidencias.

También aumenta la credibilidad de una en un tribunal de justicia si es llamado a declarar sobre las medidas adoptadas antes de la llegada y/ o la participación de la policía. (Xuejia Lai, 2010)

Muchos de estos principios son similares a la Guía de Buenas Prácticas de la Asociación británica de Jefes de Policía-ACPO. (Association of Chief Police Officers, 2005)

- a. *Principio 1:* ninguna acción tomada por las fuerzas del orden o de sus agentes deben cambiar los datos almacenados en un soporte informático o almacenamiento que posteriormente pueda ser invocada en los tribunales.
- b. *Principio 2:* en circunstancias excepcionales, cuando una persona se ve obligado a acceder a los datos originales en poder de una computadora o en un medio de almacenamiento, esa persona debe ser competente para hacerlo y ser capaz de prestar una declaración con énfasis en la importancia y las implicaciones de sus acciones.
- c. *Principio 3:* una pista de auditoría u otro registro de todos los procesos aplicados a las evidencias electrónicas computer-based deben ser creados y conservados. Una tercera parte independiente debe ser capaz de examinar los procesos y lograr el mismo resultado.
- d. *Principio 4:* la persona a cargo de la investigación (el oficial de caso) tiene la responsabilidad general de garantizar que la ley y estos principios se cumplen.

Características de la evidencia

Dos características principales de la evidencia son peso y relevancia. La relevancia del término se refiere a la relación entre la evidencia y el hecho de ser probado. Una pieza de evidencia es relevante cuando hace más o menos probable el hecho de que se trate. Si las evidencias no cambian la probabilidad del hecho, la evidencia es irrelevante.

El peso de la evidencia es la medida de cuánto la evidencia cambia la probabilidad de que el hecho. La relevancia y el peso de una pieza de evidencia están determinados por la corte sobre la base de conocimientos generales.

Preservación de evidencia

Preservación de evidencias es otro aspecto importante de la investigación forense. La naturaleza dinámica de los datos almacenados, y la operación de rutina de la tecnología de las computadoras pueden modificar o eliminar información. Por lo tanto, es fundamental para hacer frente a la preservación de evidencias a principios de una investigación (Air Force Office of Special Investigations, 2002). El investigador forense conserva evidencias forenses para asegurar que esa evidencia no es destruida o dañada.

La evidencia digital puede ser muy frágil, y sí tiene varios desafíos a diferencia de la evidencia encontrada durante las investigaciones tradicionales (Kroll Ontrack Inc., 2006). Los programas residentes en memoria se pueden perder cuando el sistema está apagado; La evidencia digital puede ser manipulado durante la recolección, el análisis y la presentación de las evidencias; La evidencia digital puede ser alterado sin rastros; Sistemas informáticos evidencia almacenada digitales se puede acceder varias veces; A veces es difícil atribuir una actividad de la computadora a un individuo, debido a que la evidencia digital es circunstancial.

La evidencia debe protegerse de la infección por el virus, mecánicos y electromecánicos influencias. El investigador forense debe ser capaz de demostrar que las evidencias no se altera de ninguna manera antes o durante su recogida o posteriormente. En *Weiller v. New York Life Ins. Co.*, el acusado en una demanda colectiva en Nueva York recibió la orden de conservar los documentos. El acusado también afirmó que la preservación de la información de la computadora costaría una cantidad considerable de dinero. Sin embargo, el tribunal de Nueva York determinó que las órdenes de conservación federales no eran protección suficiente para el demandante. (Westlaw , 2006)

Del mismo modo, en un litigio de múltiples distritos por Vioxx Productos responsabilidades litigiosas, el tribunal ordenó a todas las partes a preservar las evidencias pertinentes al litigio que incluye información impresa y copia software. (Patzakis, 2008)

En otro caso civil, *Kucala Enterprises, Ltd. v. Auto Wax Co., Inc.*, el tribunal de distrito desestimó el caso del demandante porque el demandante no preservar las evidencias, sino que destruyeron evidencias con el uso de evidence eliminator. El demandante también fue condenado a pagar los honorarios del abogado de la parte demandada y el costo incurrido en relación con la sanción. (Gladyshev, 2007)

Integridad probatoria

El peso de una pieza de evidencia depende de cómo se demuestra o garantiza que la evidencia es un hecho cierto y o falso. Una pieza de

evidencia que originan alteraciones a partir de la existencia del hecho de ser demostrado, no tiene peso en demostrar el hecho.

Para conservar el peso de la evidencia, debe reducirse al mínimo la posibilidad de manipulación. Esto se llama preservar integridad probatoria. Con este mecanismo de integridad probatoria se preserva la evidencia de la manipulación y se examina las evidencias de una manera que no lo cambiaría. Toda manipulación y/o examen deben realizarse con testigos que acuerden las partes o el juez.

Demostrar la integridad de las evidencias, suele ser una parte del examen de la admisibilidad. Para demostrar que no hay alteración, debe presentarse todo el historial de cada pieza de evidencia y su registro desde el momento en que se recoge hasta el momento que se presenta en la corte. Este proceso se llama la cadena de custodia (Fredesvinda, Lázaro Herrero, & García González, 2008).

Admisibilidad

En países con tradición de derecho común cada pieza de evidencia debe pasar examen de admisibilidad antes de que pueda ser utilizado en la corte.

El examen de admisibilidad es especificado por la ley. La admisibilidad de una evidencia depende del tipo de conflicto y cómo se relaciona la evidencia con el hecho de ser probada. En general, una pieza de evidencia es inadmisibile si no tiene relevancia al hecho de ser probado. Sin embargo, un elemento relevante y pesado de las

evidencias puede ser excluido porque viola alguna regla formal.

Dependiendo de qué hechos se supone, la evidencia digital para probar, pueda caer en diferentes clases de evidencias.

- *Evidencia real*: software presentado en la corte para probar el hecho de la posesión o imágenes digitales.
- *Evidencia documental*: mensajes de correo electrónico presentados como evidencia de su contenido son la evidencia documental.
- *Evidencia circunstancial*: los archivos de registro, sellos de tiempo de archivo, todo tipo de información del sistema utilizado para reconstruir la secuencia de eventos son evidencias circunstanciales.
- *Testimonio*: documentos digitales notariales mediante firma digital.

El uso de la información digital en disputas legales es complicado por una serie de problemas técnicos, que reducir el peso de la evidencia por computadora o incluso que sea irrelevante. Las subsecciones siguientes introducen cada uno de los problemas.

Opiniones manifestadas por los actores sociales implicados en el proceso de recolección, presentación y admisión de evidencias electrónicas para un juicio, así como el vacío judicial dominante, generan una inseguridad jurídica y profesional.

La admisión de evidencia en formato electrónico en tribunales europeos se regula a través de disposiciones generales aplicables a la evidencia tradicional, sin ninguna regulación nacional específica en el viejo continente. (Brenes Arias Abogados, 2015)

La evidencia digital es frágil y volátil. La información residente en los medios de almacenamiento electrónico puede ser borrada, cambiada o eliminada sin dejar rastro, lo cual limita la labor del investigador forense en informática tendiente a identificar y encontrar elementos clave para esclarecer los hechos relevantes de una investigación.

En este sentido, las evidencias digitales son piezas probatorias básicas que requieren una revisión detallada sobre cómo se crean, recolectan, aseguran y, finalmente, cómo se presentan en la corte a efecto de aportar, con claridad y precisión, factores que orienten las decisiones en casos donde sean parte fundamental.

Al ser un objeto relativamente fácil de manipular, generado por dispositivos electrónicos de los cuales no sabemos nada sobre su funcionamiento, la susceptibilidad a las fallas, entre otras características, nos advierte que el conocimiento técnico es tan fundamental como el forense y el de técnicas probatorias.

En razón de lo anterior, es preciso indagar sobre estrategias para implantar reglas mínimas que le permitan a la corte validar o no evidencias digitales. Si bien esta labor requiere un entendimiento técnico de los medios electrónicos, también establece un reto a los

fiscales y jueces para involucrarse en los cambios que establece una sociedad digital, donde la delincuencia también ha evolucionado en sus métodos y estrategias delictivas.

La evidencia es la razón, argumento, instrumento u otro medio con que se pretende mostrar y hacer patente la verdad o falsedad de algo (inteco, 2003), la evidencia se considera aquella información que se presenta ante un jurado o juez para mostrar la verdad o falsedad de un hecho por lo que evidencia y la evidencia son consideradas sinónimos.

El concepto de evidencia electrónica sacado de la página oficial del Instituto Nacional de Tecnologías de la Información-INTECO de España indica: “Las evidencias electrónicas son datos que de manera digital se encuentran almacenados o fueron transmitidos mediante equipos informáticos y que son recolectados mediante herramientas técnicas especializadas empleadas por un perito en una investigación informática. Tienen la función de servir como evidencia física (por encontrarse dentro de un soporte) de carácter intangible (no modificables) en las investigaciones informáticas”.

Las evidencias son obtenidas por expertos informáticos llamados peritos que además de conocer sobre tecnología deben conocer sobre derecho, su trabajo radica en utilizar herramientas artefactos que sean de utilidad en la investigación informática para obtener evidencia electrónica o digital que sirvan de evidencia para resolver los casos en investigación.

Normativa legal de admisibilidad de la evidencia

El uso de la evidencia digital en los tribunales penales internacionales debe entenderse a la luz del enfoque general para la admisión de evidencias en procedimientos judiciales.

Los tribunales penales internacionales incorporan elementos del derecho consuetudinario y las tradiciones de derecho civil en diversos grados. En general, el sistema de derecho común contiene más prohibiciones y normas sobre exclusión de evidencia de que es irrelevante o poco fiable, mientras que en el sistema de derecho civil la mayor parte de la evidencia es admitido y los jueces posteriormente evalúan su valor probatorio (Decision on the admission into evidence of materials contained in the prosecution's list of evidence., 2010).

El Estatuto de Roma creó un sistema que “evitan en general las formalidades técnicas del sistema de derecho consuetudinario de la admisibilidad de la evidencia a favor de la flexibilidad del sistema de derecho civil.”

La Regla 69 de las Reglas de la ICC- International Criminal Court, de procedimiento y evidencias dirige a los jueces a admitir evidencias, “teniendo en cuenta, entre otras cosas, el valor probatorio de las evidencias y cualquier perjuicio que pueda suponer para un juicio justo o para la justa evaluación del testimonio de un testigo.” (Decision on Confirmation Charges, 2007). De conformidad con la Regla 63, jueces de la ICC determinan el valor probatorio y el “peso adecuado” de los

medios de evidencia admitidos en el final de un caso, cuando consideran la evidencia como un todo. Sólo hay dos situaciones en las que existe un derecho específico para los jueces para hacer un pronunciamiento sobre la admisibilidad de las evidencias. Estas disposiciones están redactadas de manera restrictiva y no prevén la exclusión automática de evidencias.

Del mismo modo, tribunales como el de Yugoslavia y Rwanda han evitado en gran medida las normas de derecho común de exclusión de evidencias, porque se desarrollaron estas normas para limitar la evidencia considerada por jurados y por lo tanto no se aplican a los ensayos en la tradición inquisitorial. La evidencia debe satisfacer “normas mínimas de relevancia y fiabilidad” para ser admitido. La admisión de evidencias no en sí mismo una señal de que la evidencia es exacta; los jueces evalúan su peso por separado. Por lo tanto, al examinar las evidencias, los tribunales ad hoc se centran en si la evidencia es admisible, y qué peso probatorio tiene la evidencia.

Mientras que el umbral para la admisión de evidencias puede ser bajo, los tribunales penales internacionales todavía tienen preferencias por los tipos de evidencias introducidas. La ICC favorece generalmente evidencia a viva voz o testimonios orales y ha desarrollado un conjunto de normas que son específicas de la evidencia digital.

Las evidencias y el material digital deben ajustarse a un “Protocolo de e-corte”, incluso antes de que se presente en la Audiencia de

Confirmación. El Protocolo está diseñado para “asegurar la autenticidad, exactitud, confidencialidad y conservación de las actas. “El Protocolo requiere metadatos que se adjunta, incluyendo la cadena de custodia en orden cronológico, la identidad de la fuente, el autor original y la información del destinatario, y el autor y respectivas organizaciones de beneficiarios. Mientras que el protocolo ofrece algunas orientaciones para facilitar el uso de la evidencia digital, y almacenamiento, pero no apunta a una preservación adecuada de la evidencia.

Legislación internacional

En el contexto internacional, son pocos los países que cuentan con una legislación apropiada sobre delitos informáticos y preservación de la evidencia. A continuación, se mencionan algunos aspectos relacionados con la ley en los diferentes países.

Según las Naciones Unidas, cuando se trata de procesar evidencias digitales, los parámetros están determinados básicamente por aquellos lineamientos establecidos en 1966 por el artículo 9 de la Ley Modelo sobre el Comercio Electrónico de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional “UNCITRAL” por sus siglas en inglés-: “Al valorar la fuerza probatoria de un mensaje de datos se habrá de tener presente la fiabilidad de la forma en la que se haya generado, archivado o comunicado el mensaje, la fiabilidad de la forma en la que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente”.

En México, son especificados en el artículo 210-A del Código Federal de Procedimientos Civiles de esa nación, que es dónde se establece, primero, que “Para valorar la fuerza probatoria de la información digital, se estimará primordialmente la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada y, en su caso, si es posible atribuir a las personas obligadas”; y segundo que: “Cuando la ley requiera que un documento sea conservado y presentado en su forma original, ese requisito quedará satisfecho si se acredita que la información generada, comunicada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología, se ha mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y ésta pueda ser accesible para su ulterior consulta”

En República Dominicana, La promulgación de la nueva Ley No.126-02 sobre comercio electrónico, documentos y firmas digitales, de fecha 29 de septiembre de 2002, regula toda relación comercial, estructurada a partir de la utilización de uno o más documentos digitales o mensajes de datos o de cualquier otro medio similar.

El plazo de 40 años está establecido en la Ley No.126-02 en su artículo 52, el cual dispone lo siguiente: “Art. 52.- Término de conservación de los registros. Los registros de certificados expedidos por una entidad de certificación deben ser conservados por el término de cuarenta (40) años, contados a partir de la fecha de la revocación o expiración del correspondiente certificado”.

En Colombia, el Artículo 236: “el indiciado o imputado está transmitiendo o manipulando datos a través de las redes de telecomunicaciones, ordenará a policía judicial la retención, aprehensión o recuperación de dicha información, equipos terminales, dispositivos o servidores que pueda haber utilizado cualquier medio de almacenamiento físico o virtual, análogo o digital, para que expertos en informática forense, descubran, recojan, analicen y custodien la información que recuperen.

Los certificados digitales deben cumplir con el estándar UIT X.509 V3 y las disposiciones de campos mínimos requeridos, definidas por la Ley 527 de 1999, el Decreto 1747 de 2000 y la Circular Única No.10 de la Superintendencia de Industria y Comercio, y demás disposiciones legales inherentes a entidades de certificación digital en Colombia Ley 527. ART. 11. Criterio para valorar probatoriamente un mensaje de datos. “Para la valoración de la fuerza probatoria de los mensajes de datos a que se refiere esta ley, se tendrán en cuenta las reglas de la sana crítica y demás criterios reconocidos legalmente para la apreciación de las evidencias. Por consiguiente, habrán de tenerse en cuenta: la confiabilidad en la forma en la que se haya generado, archivado o comunicado el mensaje, la confiabilidad en la forma en que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente”.

En Perú.- El Proyecto de ley Nro. 3003/2013-CR, aprobado en diciembre del 2013, que crea el sistema de defensa y preservación

digital en el archivo de la nación, en su artículo 6 indica “Las entidades oficiales del archivo general de la nación, serán responsables de la gestión de documentos y todo el proceso de escaneado técnico y de la administración de sus archivos y ejercerán el control de la documentación durante todo el proceso de defensa y preservación digital.” Y en el artículo 7 “La duplicidad, extracción y adulteración de los archivos digitales o documentos electrónicos durante el proceso de preservación digital o en cualquier otro momento, se reprime como delito...”

En Ecuador, existe la ley de comercio electrónico y el manual de manejo de evidencias digitales y entornos informáticos. Versión 2.0, en el punto 4, indica “Se debe llevar una bitácora de todos los procesos adelantados en relación a la evidencia digital. Cuando se hace una revisión de un caso por parte de una tercera parte ajena al mismo, todos los archivos y registros de dicho caso y el proceso aplicado a la evidencia que fue recolectada y preservada, deben permitir a esa parte recrear el resultado obtenido en el primer análisis.”, y en el punto 5: “A fin de que los investigadores forenses tengan una idea de dónde buscar evidencia digital, éstos deben identificar las fuentes más comunes de evidencia. (Acurio, 2008)

En Estados Unidos, este país adoptó en 1994 el Acta Federal de Abuso Computacional que modificó al Acta de Fraude y Abuso Computacional de 1986. Con la finalidad de eliminar los argumentos hipertécnicos acerca de qué es y que no es un virus, un gusano, un

caballo de troya y en que difieren de los virus, la nueva acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, a los sistemas informáticos, a las redes, información, datos o programas. La nueva ley es un adelanto porque está directamente en contra de los actos de transmisión de virus. Asimismo, en materia de estafas electrónicas, defraudaciones y otros actos dolosos relacionados con los dispositivos de acceso a sistemas informáticos, la legislación estadounidense sanciona con pena de prisión y multa, a la persona que defraude a otro mediante la utilización de una computadora o red informática.

En Alemania, este país sancionó en 1986 la Ley contra la Criminalidad Económica, que contempla los delitos de espionaje de datos, estafa informática, alteración de datos y sabotaje informático.

En Austria, la ley de reforma del código penal, sancionada el 22 de diciembre de 1987, sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos. Además, contempla sanciones para quienes comenten este hecho utilizando su profesión de especialistas en sistemas.

En Gran Bretaña, debido a un caso de hacking en 1991, comenzó a regir en este país la Computer Misuse Act (Ley de Abusos Informáticos).

mediante esta ley el intento, exitoso o no, de alterar datos informáticos es penado con hasta cinco años de prisión o multas. Esta ley tiene un apartado que especifica la modificación de datos sin autorización.

En España, en el código penal español se puede ver lo que en España se entiende por delito informático: ataques que se producen contra el derecho a la intimidad; las infracciones a la propiedad intelectual a través de la protección de los derechos de autor; las falsedades y sabotajes informáticos; los fraudes informáticos, las amenazas y calumnias e injurias, la pornografía infantil, y sobre la legislación en relación con las telecomunicaciones.

En Holanda, el 1º de marzo de 1993 entró en vigencia la Ley de Delitos Informáticos, en la cual se penaliza los siguientes delitos: El hacking, El phreaking, La ingeniería social, La distribución de virus.

En Francia, en enero de 1988, este país dictó la ley relativa al fraude informático, en la que se consideran aspectos como: intromisión fraudulenta que suprima o modifique datos; la conducta intencional en la violación de derechos a terceros que haya impedido o alterado el funcionamiento de un sistema de procesamiento automatizado de datos; la conducta intencional en la violación de derechos a terceros, en forma directa o indirecta, en la introducción de datos en un sistema de procesamiento automatizado o la supresión o modificación de los datos que éste contiene, o sus modos de procesamiento o de transmisión; la impresión o modificación de datos contenidos en el sistema, o bien en

la alteración del funcionamiento del sistema (sabotaje).

En Chile, fue el primer país latinoamericano en sancionar una Ley contra delitos informáticos, la cual entró en vigencia el 7 de junio de 1993. Esta ley se refiere a los siguientes delitos: La destrucción o inutilización de los de los datos contenidos dentro de una computadora es castigada con penas de prisión. Asimismo, dentro de esas consideraciones se encuentran los virus; la conducta maliciosa tendiente a la destrucción o inutilización de un sistema de tratamiento de información o de sus partes componentes o que dicha conducta impida, obstaculice o modifique su funcionamiento; la conducta maliciosa que altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información.

**MODELO CONCEPTUAL DE PRESERVACIÓN DIGITAL
APLICABLE A LA MEJORA DE LA PRESERVACIÓN
DE EVIDENCIA DIGITAL EN INSTITUCIONES
DE INVESTIGACIÓN CRIMINAL - PREDECI**

Capítulo 3

MODELO CONCEPTUAL DE PRESERVACIÓN DIGITAL APLICABLE A LA MEJORA DE LA PRESERVACIÓN DE EVIDENCIA DIGITAL EN INSTITUCIONES DE INVESTIGACIÓN CRIMINAL - PREDECI

Propósito y alcance

El propósito de este aporte es definir un modelo de referencia que lo denominamos PREDECI para la preservación de la evidencia digital en instituciones de investigación criminal que tienen la responsabilidad de custodiarla al largo plazo con el objeto de aumentar la admisibilidad de la evidencia digital en la corte o la disponibilidad de la evidencia a una comunidad designada para el manejo de evidencia y garantiza la fidelidad e integridad de la misma al largo plazo. Responde a un conjunto de responsabilidades determinadas en leyes y normativas para este entorno, basándose en el modelo de preservación OAIS y conceptos de metadatos.

De la revisión de literatura se determina un conjunto de aspectos mínimos necesarios que aplicados efectivamente al modelo OAIS, genera un marco de referencia para aumentar la admisibilidad de la evidencia digital en el largo plazo.

Según Molina & Rodríguez, en investigaciones anteriores, (Molina & Rodriguez, 2015a) (Molina & Rodriguez, Preservation of Digital Evidence: Application in Criminal Investigation., 2015b). (Molina &

Rodriguez, The preservation of digital evidence and its admissibility in the court., 2017b). (Molina & Rodriguez, MODEL FOR DIGITAL EVIDENCE PRESERVATION IN CRIMINAL RESEARCH INSTITUTIONS – PREDECI, 2017c), indica que catorce aspectos son necesarios incluir en el modelo OAIS para su aplicabilidad en el entorno de investigación criminal, estos son:

1. *Legalidad de la evidencia.*- Que la evidencia cumpla la disposición legal para la preservación. (Thomson, 2011)
2. *Confidencialidad.*- Es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información. La confidencialidad ha sido definida por la Organización Internacional de Estandarización (ISO) en la norma ISO/IEC 27002 como “garantizar que la información es accesible sólo para aquellos autorizados a tener acceso”. (ISO, 2012)
3. *Control de calidad ingesta.*- Permite la validación de formatos, contenidos o aplicaciones activas (ej.: virus). (Alvarez, 2004)
4. *Ingesta parcial.*- Permite recibir información o contenido dividido en partes. Se permite heredar datos o recibe nuevos datos de otros sistemas de confianza. Permite actualizar datos incrementales (una vez que se realiza el proceso de admisión, aumenta su contenido o metadatos). (Gómez L. , 2013). (Dappart A. , 2013)

5. *Metadatos del entorno de la evidencia a preservar.*- Provee información técnica y descriptiva sobre el medio ambiente de la colección de las evidencias, permite para demostrar que datos tienen un soporte legal, que hay alguien a cargo de los contenidos de los datos y hay una especificación completa del medio ambiente donde se generó la evidencia digital. (Dappart A. , 2013)
6. *AIP, SIP, DIP. Transmisión.*- Transmisión de evidencia digital, dentro del proceso de preservación. (Ashoire, Bower, & Warden, 2013)
7. *Museo de herramientas.*- Permite para conservar herramientas utilizadas para acceder a los objetos digitales. Los metadatos del objeto mantienen información acerca de la herramienta que se utilizará. (Acurio, 2008)
8. *Garantizar la integridad del original.*- Establece técnicas adicionales para la seguridad, integridad, fiabilidad y accesibilidad de los datos (impuestas por la organización). Documentos de los mecanismos de autenticación y proporciona información de autenticación para garantizar que el contenido no es modificado de una manera no documentados. Permite certificar los datos originales o implementar otro mecanismo de supervisión para el acceso. (Rao, 2014)
9. *Almacenamiento distribuido.*- Permite almacenar datos en repositorios compartidos. (Castillo, 2008)

10. *Terminología*.- Permite usar términos de interpretación que son únicos para este entorno. (Acurio, 2008)
11. *Evaluación de riesgos*.- Permite determinar, supervisión o alertas de riesgos (amenazas, consecuencias, umbral). (Acurio, 2008)
12. *Tiempo de preservación*.- Determina el horizonte de tiempo de conservación (ej.: hasta que el cambio en la tecnología, sólo hasta la discontinuación del uso, para un número limitado de años, “para siempre”). (UNESCO, 2004)
13. *Certificaciones de la estrategia*.- Establece los certificados digitales con una estrategia de conservación aplicada o una combinación de ellos. (migración, emulación, encapsulación, enfoques de reingeniería, no digitales). (ISO, 2012)
14. *Trazabilidad y Continuidad de la preservación*.- Capacidad para reconstruir el historial de la utilización o la localización de un artículo o producto mediante una identificación registrada”, control y registro de toda transacción. (Thomson, 2011)

Además, se elimina del modelo OAIS toda opción de actualización de contenidos ya ingresados, pues por definición la evidencia debe permanecer intacta.

Predecí proporciona un marco para la comprensión y mayor conciencia de los conceptos necesarios para la preservación de la evidencia digital al largo plazo, incluyendo la terminología y conceptos, para describir y comparar las arquitecturas y operaciones de evidencias

digitales actuales y futuras, considerando las diferentes estrategias de preservación a largo plazo.

El modelo aborda las funciones de preservación del modelo OAIS incluyendo los aspectos fundamentales en el entorno de instituciones de investigación criminal, manteniendo la estructura global como la ingesta, administración de preservación, almacenamiento, administración de datos, plan de preservación, acceso. También se aborda la preservación del entorno de creación de evidencia, y la capacidad de incrementar evidencia, así como administrar evidencia digital en repositorios de confianza externos, muy diferente a tener un solo archivo, una sola técnica o una sola estrategia como lo plantea OAIS.

Aplicabilidad

El modelo predecí puede ser aplicable a cualquier archivo digital, especialmente aplicable a las organizaciones con la responsabilidad de poner a disposición evidencia digital a largo plazo. Esto incluye organizaciones con otras responsabilidades, como el procesamiento y distribución en respuesta a necesidades programáticas.

Justificación

El crecimiento computacional, ha dado lugar a una explosión de organizaciones que manejan información digital y por lo tanto un crecimiento de los delitos digitales. Las transacciones se realizan por medio de formularios digitales que reemplazan a los medios más tradicionales como el papel.

Preservar la evidencia en forma digital es mucho más difícil que preservar información en formas tales como papel y película e información digital general como libros, historias clínicas u otra.

La evidencia digital y el marco legal que la envuelve tienen un tratamiento específico, que se refleja en este marco de referencia. Junto con las muchas ventajas en términos de trazabilidad y replicación, la propagación de la tecnología digital en todos los campos trae ciertas desventajas. La rápida obsolescencia de las tecnologías digitales crea peligros técnicos considerables, particularmente un riesgo mucho mayor que en el pasado de perder la posibilidad de restaurar, representación o interpretación adecuada de la información, mucho más aun en procesos legales donde la evidencia y su adecuada preservación dentro de la cadena de custodia, pueden llevar al desestimamiento del caso o fallos erróneos. Para ello se consideran punto de vista técnico, organizacional, legal, industrial, científico y cultural.

Se espera que este modelo de referencia predecí, mediante el establecimiento de requisitos mínimos para entornos de investigación criminal, proporcione un marco común desde la cual se determinen desafíos de preservación a largo plazo de evidencia digital específicamente.

Naturalmente, predecí permite adecuaciones específicas a organizaciones que requieran mayores características de seguridad o aspectos relevantes propios del entorno de aplicación. Así, predecí

no determina un diseño o una implementación, sino un marco de referencia para un entorno específico y una guía de implementación para un caso de estudio.

Ambiente predecí

Para la determinación del modelo propuesto en este trabajo, se realiza un análisis teórico de técnicas y métodos y modelos de preservación digital existentes, un análisis de los requerimientos de preservación en instituciones de investigación criminal, y un análisis de preservación de evidencia digital, con la finalidad de incrementar la tasa de admisibilidad de la evidencia en la corte, mismos que pueden ser revisados en publicaciones anteriores de los autores, tanto en conferencias internacionales en Londres y Portugal, como en revistas con factor de impacto. (Molina & Rodriguez, 2015a). (Molina & Rodriguez, Preservation of Digital Evidence: Application in Criminal Investigation., 2015b). (Molina & Rodriguez, The preservation of digital evidence and its admissibility in the court., 2017b), con estos estudios, se realiza una propuesta de un modelo de preservación de evidencia digital para instituciones de Investigación criminal, basado en el modelo de preservación OAIS, del que utiliza funciones y procesos útiles para este entorno, finalmente se realiza un estudio de una muestra de 74 personas relacionadas en el proceso judicial, y se valida el aporte del modelo con un proceso estadístico que es detallado en la parte de resultados.

En el documento se presentan figuras que representan las entidades funcionales del modelo, utilizando el color blanco para indicar el aporte del investigador.

Este modelo fue publicado en una revista de impacto disponible en (Molina & Rodriguez, MODEL FOR DIGITAL EVIDENCE PRESERVATION IN CRIMINAL RESEARCH INSTITUTIONS–PREDECI, 2017c)

Predecí está basado en OAIS, es una adaptación de OAIS a entornos de instituciones de investigación criminal, así el nivel 0, o entorno inicial se muestra en la Figura 10.

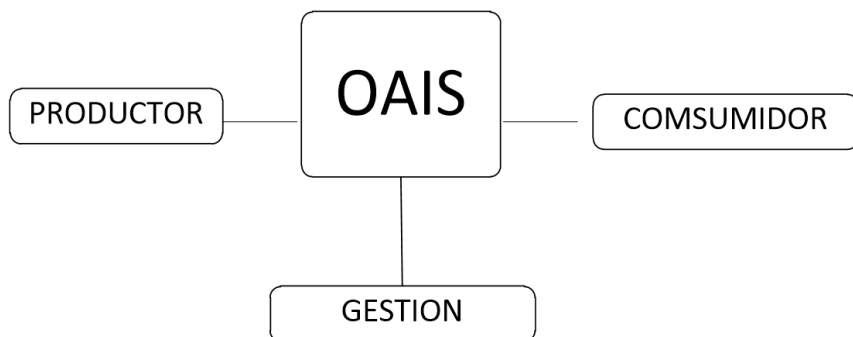


Figura 10. Entorno de PREDECÍ (basado en OAIS)
Fuente. (Consultative Committee for Space Data Systems, 2012)

Productor: son las personas, peritos, investigadores, agentes o sistemas de cliente, que proporcionan la evidencia a ser preservado.

La gestión: es el papel desempeñado por aquellos que establezca políticas de preservación. La gestión no está involucrada en las operaciones diarias de preservación.

El consumidor: son las personas, peritos, investigadores, agentes o sistemas de cliente, que interactúan con los servicios para encontrar y adquirir la evidencia de interés. Una clase especial de los clientes es la comunidad designada. Un determinado individuo o sistema puede actuar en el papel de un productor y un consumidor.

Funciones tomadas de OAIS

Predecí utiliza algunas funciones y procedimientos del modelo OAIS:

- a. De la entidad funcional “INGEST”, usa las funciones de “Receiving your shipping”, “Quality Assurance”, “Descriptive Information Generator”, la base “AIP generate”, y procesos como Format Validation y Application Validation.
- b. De la entidad funcional “DATA MANAGEMENT”, usa las funciones de “Report Generator”, “Administrator Database”, “Queries Perform”.
- c. De la entidad funcional “ACCESS” usa las funciones de “Coordinate access activities”, “Legality and Validation of Profile”, “Generate DIP”, y procesos como “Liability Responsibilities”.
- d. De la entidad funcional “STORAGE”, usa las funciones de “Data provider”, “Media for original”, “Duplicate for backup”, “Failure Recovery”, “Error Checking”, “Media-temporal storage-”, “Data receiving”.
- e. De la entidad funcional “PRESERVATION PLANNING”, usa las funciones de “Package Design Development”, “Monitor designated community”, “Technology Monitor”, “Preservation

plan development”, y procesos como “alerts technology, risk analysis, operation policies, procedures, standards, statistical data, customer reviews, preservation strategies”.

En todas las entidades funcionales se mantienen las relaciones entre las entidades consideradas por OAIS.

Modelo funcional

El propósito de esta sección es proporcionar una vista más detallada del modelo de las entidades funcionales de predecí, para ayudar el entendimiento e implementación de aplicaciones.

Predecí, en la figura 11 se presenta estructurado en ocho entidades funcionales e interfaces relacionadas. Se muestran sólo los flujos de información importante. Las líneas que unen las entidades identifican vías de comunicación sobre qué información fluye en ambas direcciones. Las líneas entrecortadas representan un proceso adicional entre las entidades y el cuadro transversal etiquetado con M, representa un proceso continuo de monitoreo de las acciones realizadas, procedimiento que registra cada transacción de consulta, actualización o inserción, en todo el proceso. Nombre de usuario autorizado, transacción realizada, hora, fecha, registro de autorización. Siempre se manipulará el archivo duplicado. El original nunca será accedido, salvo orden directa de la autoridad competente. Definir en políticas de la organización o ley del país.

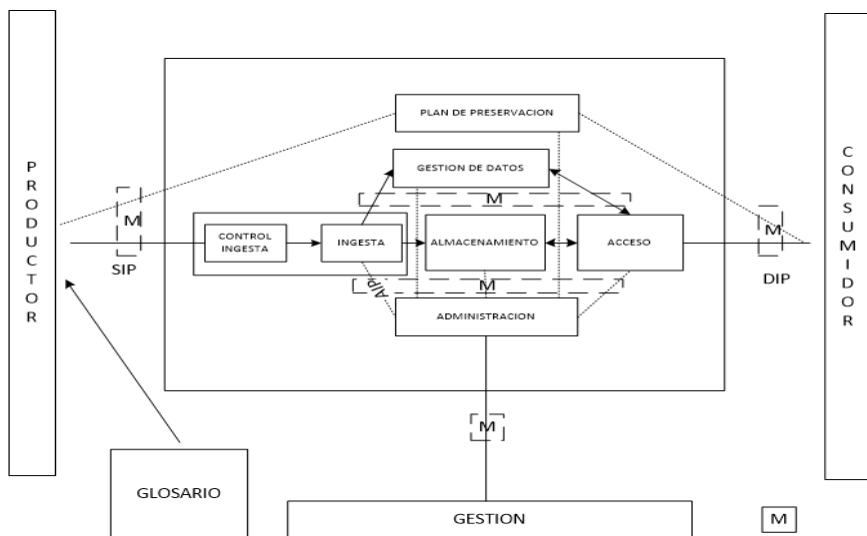


Figura 11. Entidades Funcionales Predecí
Elaborado por: los autores (basado en OAIS)

La entidad glosario, proporciona una guía permanente de los términos que utiliza predecí, lo que permite una correcta operación y administración del modelo y de la evidencia digital a preservar.

La entidad funcional control de ingesta proporciona un filtro de ingreso de la información, permite la validación de formatos, contenidos o aplicaciones activas (ej.: virus).

La entidad funcional ingesta proporciona los servicios y funciones para aceptar paquetes de información de envío (SIP) de los productores y preparar los contenidos para el almacenamiento y gestión dentro del modelo. Ingesta incluye funciones de recepción de SIPs, aseguramiento de calidad en SIPs, legalización y validación del perfil del productor, generar un paquete de información (AIP) de la evidencia, que contiene

un arreglo de evidencia relacionada, información de entorno y de la herramienta de creación, extraer información descriptiva de las AIPs para su inclusión en la base de datos de archivo, y coordinar el almacenamiento y administración de datos.

La entidad funcional almacenamiento proporciona los servicios y funciones para el almacenamiento, mantenimiento y recuperación de la AIPs. Esta función incluye la recepción de AIPs de la evidencia de ingesta y añadirlos al almacenamiento temporal, luego de una verificación de políticas de almacenamiento, enviarlo a un almacenamiento permanente, y generar un almacenamiento duplicado destinado para el acceso, y un respaldo para recuperación de fallos. Incluye funciones de comprobación especial de errores, recepción y selección de herramientas, proporciona capacidades de recuperación ante desastres y proporciona acceso a AIPs.

La Entidad funcional de gestión de datos proporciona los servicios y funciones para poblar, mantener y acceder a la información descriptiva que identifica la evidencia y los datos administrativos que se utilizan para gestionar la evidencia. Incluyen funciones de gestión la base de datos; realizar consultas sobre la evidencia para generar las respuestas requeridas y la generación de informes.

La Entidad funcional de administración proporciona los servicios y funciones para el funcionamiento general de predecí, que incluyen la determinación de acuerdos con productores, auditoría de las evidencias

para asegurar que cumplen con las normas de archivo y funciones de mantenimiento y configuración de software y hardware del sistema.

También proporciona funciones de ingeniería del sistema para supervisar y mejorar las operaciones de la evidencia, es responsable además de establecer, revisar y mantener los estándares de archivo y políticas, y finalmente ofrecer soporte al cliente, manteniendo un registro de las peticiones y recomendaciones.

La entidad funcional plan de preservación proporciona los servicios y funciones para monitorear el entorno de predecí, y emite recomendaciones y planes de preservación para garantizar que la evidencia sea accesible y comprensible por la comunidad designada en el largo plazo, incluso si el entorno informático original llegara a ser obsoleto. Incluyen funciones de evaluación del contenido de la evidencia y recomendar periódicamente las actualizaciones de información archivística, normas y políticas, con la emisión de informes de análisis de riesgo periódico y monitorear los cambios en el entorno de la tecnología. Además, proporciona una especificación de estrategias y estándares, certificación de estrategias, tiempo de preservación.

La entidad funcional de acceso proporciona las funciones que apoyan a los clientes en la determinación de la existencia, descripción, ubicación y disponibilidad de la evidencia preservada en predecí permitiendo a los clientes solicitar y recibir productos de información

y servicios. Incluyen la comunicación con los clientes para recibir las solicitudes, aplicación de controles para limitar el acceso a la información especialmente protegida verificando la legalidad y validez del perfil, coordinar la ejecución de solicitudes para completar con éxito, generando respuestas para los clientes.

En todas las entidades existe un procedimiento transversal que registra todas las actividades de operación, ingesta, almacenamiento, consultas, administración, gestión de datos y toda actividad que realiza un usuario, con un registro de identificación de perfil como: datos de acceso, fecha, hora, dirección ip, acción realizada, autorización y demás datos que permitan determinar las acciones realizadas.

Descripción detallada de las entidades funcionales

Se determinan flujos específicos de información entre las entidades funcionales. Las descripciones detalladas y funcionales de las subdivisiones están acompañadas por las figuras que muestren sólo los datos importantes y flujos dentro y entre las entidades.

Al final de este numeral, se presenta la figura del modelo completo, que integra todos los detalles de las entidades funcionales para demostrar coherencia general.

Sin embargo, esto no es debe ser tomado como un diseño único u obligatorio, pues se podrá optar por combinar otras funciones o retirar enlaces de funcionalidad diferente, según la especificidad del entorno u organización lo requiera.

Función ingesta

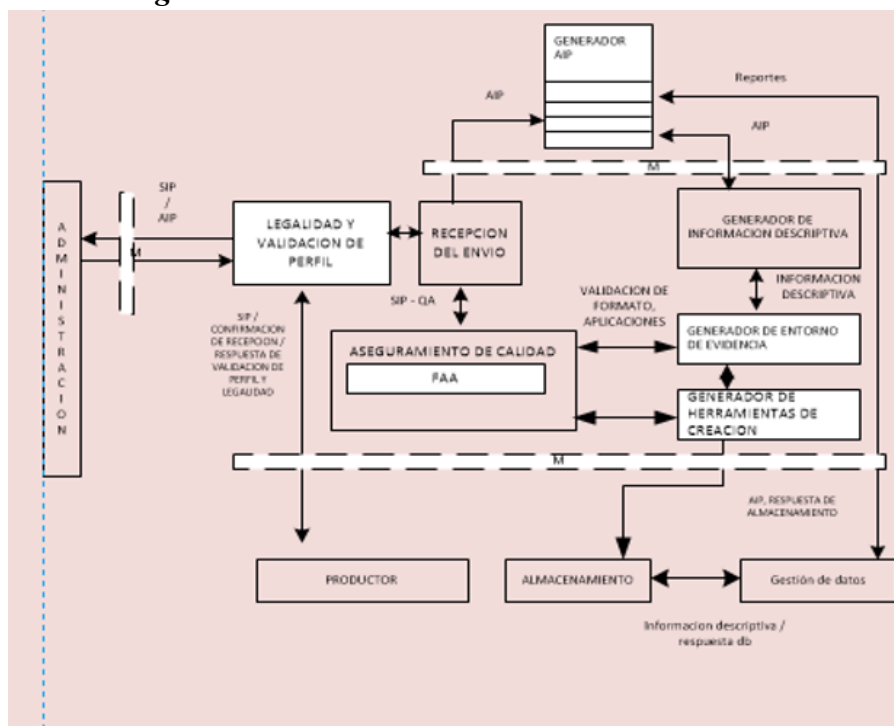


Figura 12. Entidad Funcional INGESTA
Elaborado por: los autores (basado en OAIS)

La función recepción del envío proporciona la capacidad de almacenamiento de información adecuado o dispositivos para recibir un SIPs del productor (o de administración). Los SIPs digitales pueden ser entregados vía transferencia electrónica (por ejemplo, FTP), cargado de medios entregados al archivo, o simplemente montado (por ejemplo, CD-ROM) en el sistema de archivos de acceso. Esta función puede representar a una transferencia legal de custodia de la información contenido en el SIP y puede requerir

que controles especiales de acceso especial sobre el contenido. Esta función proporciona una confirmación de la recepción de un SIPs al productor, que puede incluir una petición para volver a enviar un SIP en el caso de errores derivados del envío de los SIP. El productor proporciona evidencias de autenticidad como parte de la PDI en el envío, y esta evidencia es mantenida, actualizada, o incrementada por predecir en el tiempo. La evidencia puede expresar una evaluación de la autenticidad de sus tenencias, basado en la práctica de comunidad y recomendaciones, sin embargo, el consumidor puede hacer su propio juicio de la autenticidad a partir de la evidencia obtenida de PDI.

La función de legalidad y validación del perfil proporciona la capacidad de verificar que la evidencia cumpla la disposición legal para ser preservación, orden de la autoridad competente y una validación del perfil del productor, administrador y consumidor o comunidad designada. Existe un manifiesto que garantiza la disposición legal de preservar la evidencia y la autorización a personal autorizado para su procesamiento de preservación.

La función de generar AIP transforma uno o varios SIPs en uno o más AIPs que mantienen datos sobre formatos, normas y estándares de documentación de la evidencia digital. Esto no puede implicar conversiones de formato de archivo. Esta función envía SIP o AIPs para auditar a la administración y recibe un informe de auditoría.

Genera un AIP por cada archivo que incremente la evidencia relacionada a un caso existente. Ej. Nueva evidencia de un caso. Se considera como un arreglo o vector de AIP.

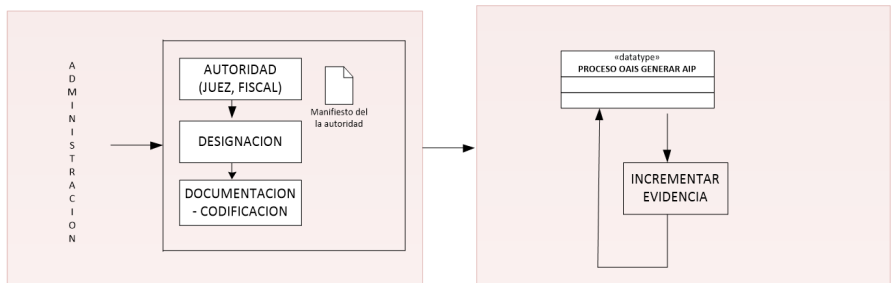


Figura 13. Validación de Perfil y Generación de AIP
Elaborado por: los autores (basado en OAIS)

La función de aseguramiento de la calidad valida la transferencia exitosa de la SIP para el área de almacenamiento temporal. Para presentaciones digitales, estos mecanismos podrían incluir controles de redundancia cíclica (CRC) o las sumas de control asociados a cada archivo de datos o el uso de archivos de registro de sistema para registrar e identificar los errores de lectura/escritura de archivo transferencia o los medios de comunicación. El archivo recibido pasa por un proceso de control de calidad, para validar formatos acordes a las herramientas de creación, control de aplicaciones activas, no solo validación de contenidos y de lectura y escritura. Se determina un procedimiento FAA, que verifica formatos, y aplicaciones activas.

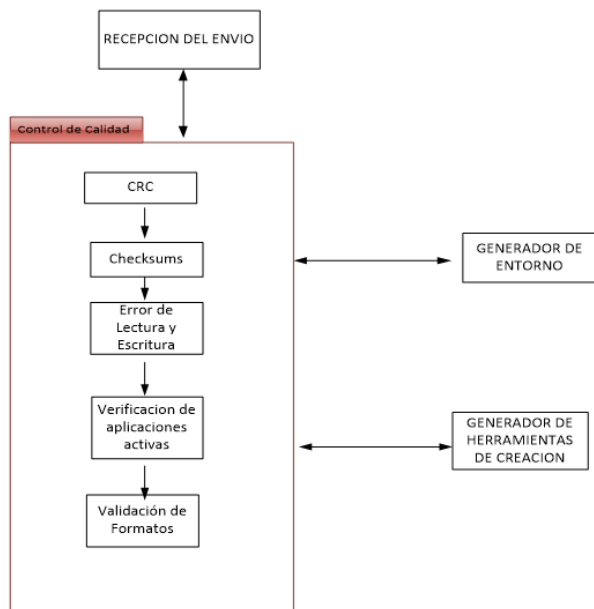


Figura 14. Control de Calidad
Elaborado por: los autores (basado en OAIS)

La función de generar información descriptiva extrae información descriptiva de la AIPs y recopila información descriptiva de otras fuentes para coordinar las actualizaciones y en definitiva la gestión de datos. Esto incluye metadatos para apoyar la búsqueda y recuperación de AIPs (por ejemplo, quién, qué, cuando, donde, por qué) y podría incluir también productos especiales (miniaturas, imágenes) para ser utilizado por el AIPs.

La función de generador de entorno y generación de herramientas de creación, registra en entorno o medio ambiente de recogida de evidencia, para una futura posible reconstrucción de los hechos, y

Registra la herramienta con la que fue creado o manipulado el archivo o evidencia.

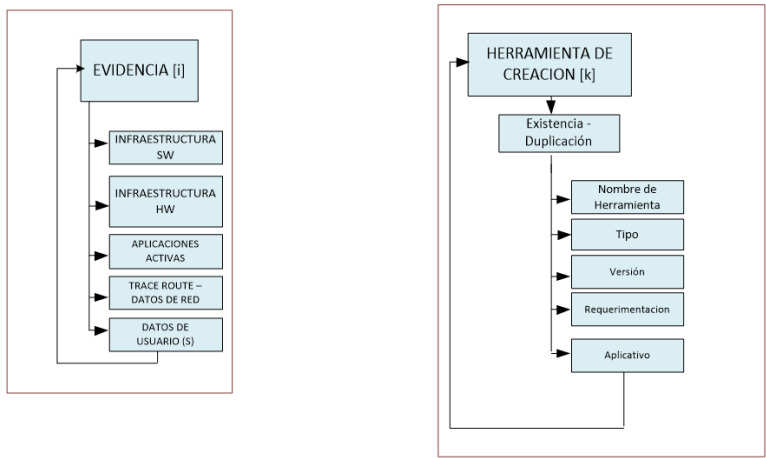


Figura 15. Función generador de entorno y generador de herramienta de creación
Elaborado por: los autores (basado en OAIS)

Función almacenamiento

Las funciones de la entidad funcional almacenamiento de información se ilustran en la figura 16 el término ‘media’ se utiliza para designar a uno o varios mecanismos, locales o remotos, para almacenar información codificada digitalmente.

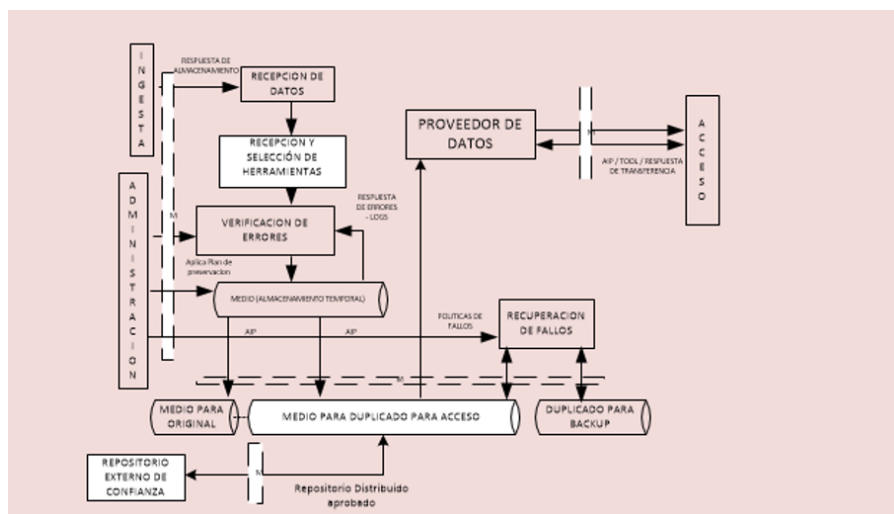


Figura 16. Función almacenamiento
Elaborado por: los autores (basado en OAIS)

La función de recepción de datos recibe una petición de almacenamiento y un AIP de ingesta y mueve la AIP para almacenamiento permanente dentro del archivo. La solicitud de transferencia deberá indicar la frecuencia esperada de la utilización de los objetos de datos que componen la AIP para la selección y almacenamiento adecuado de la AIP.

Esta función selecciona el tipo de medio, prepara los dispositivos o los volúmenes y realiza a la transferencia física de los volúmenes de almacenamiento de evidencia. Sobre la terminación de la transferencia, esta función envía un mensaje de confirmación de almacenamiento a la ingesta, incluyendo la identificación de almacenamiento de información de la AIP.

La función recepción y selección de herramientas determina la tecnología de entorno que fue ingresada con la evidencia, específicamente software, y verifica su existencia en la base de datos, si no existe lo almacena.

En el medio de almacenamiento para duplicado, se realiza una copia de los datos a preservar, tanto del medio original como de la evidencia relacionada que se reciba de otro repositorio «Aprobado» o de confianza, del archivo original aplicado la técnica y la estrategia de preservación. Sobre este duplicado se realizan todas las acciones de acceso y operación del repositorio. El archivo original permanece en un medio aparte, y podrá ser accedido con una solicitud especial, validado su autorización. Puede almacenarse o accederse a información de un repositorio externo de confianza.

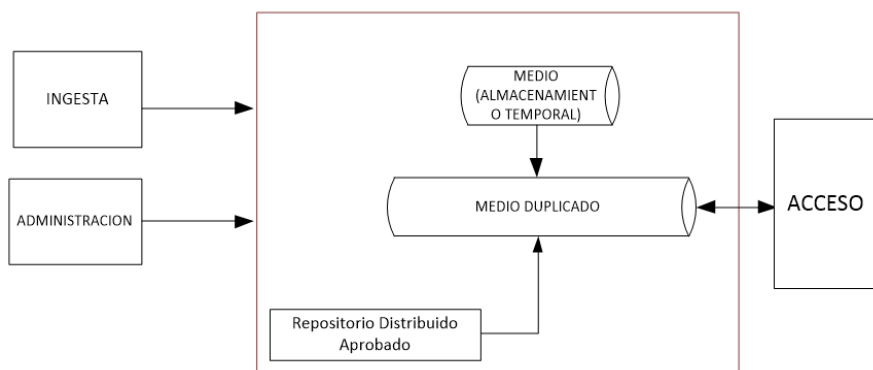


Figura 17. Medio duplicado para acceso
Elaborado por: los autores (basado en OAIS)

La función de verificación de errores garantiza que ningún componente de la AIP está dañado en almacenamiento o durante cualquier transferencia interna de datos de almacenamiento. Esta función requiere que todo el hardware y software proporcionen notificaciones de posibles errores, estos errores son enrutados a registros de error que son revisadas por el personal de almacenamiento.

La función de recuperación de fallos proporciona un mecanismo para duplicar el contenido digital de la colección del archivo y, por ejemplo, almacenar el duplicado en instalaciones separadas físicamente.

Esta función se realiza normalmente por copiar el contenido del archivo a alguna forma de medios de almacenamiento extraíbles (por ejemplo, cinta digital lineal, CD-ROM), pero también se puede realizar mediante hardware transporte o red de transferencia de datos. Los detalles de las políticas de recuperación ante desastres son especificados por la administración.

La función de proveedor de datos proporciona copias de AIPs almacenados a acceso. Esta función recibe una solicitud de AIP que identifica a la AIP solicitada(s) y las transfiere a un área de almacenamiento temporal.

Esta función también envía un aviso de transferencia de datos de acceso sobre la terminación de un pedido.

Función de gestión de datos

La función de gestión de base de datos es responsable de mantener la integridad de la gestión de la base de datos, proporciona un mecanismo de almacenamiento de información. La información descriptiva identifica y describe las propiedades del archivo, y la información del sistema se utiliza para apoyar las operaciones de archivística.

Esta función es responsable de crear cualquier esquema o tabla de definiciones necesarias para apoyar las funciones de administración de datos; para proporcionar la capacidad de crear, mantener y acceder a vistas de usuario personalizada de los contenidos de este almacenamiento; y para proporcionar validación interna (por ejemplo, la integridad referencial) de los contenidos de la base de datos. La función de administrar base de datos se realiza conforme a las políticas que recibió de la administración.

La función de operador de consultas recibe una solicitud de consulta de acceso y ejecuta la consulta para generar una respuesta de consulta que se transmite al solicitante.

Entidad funcional administración

Las funciones de la entidad de administración se ilustran en la fig. siguiente.

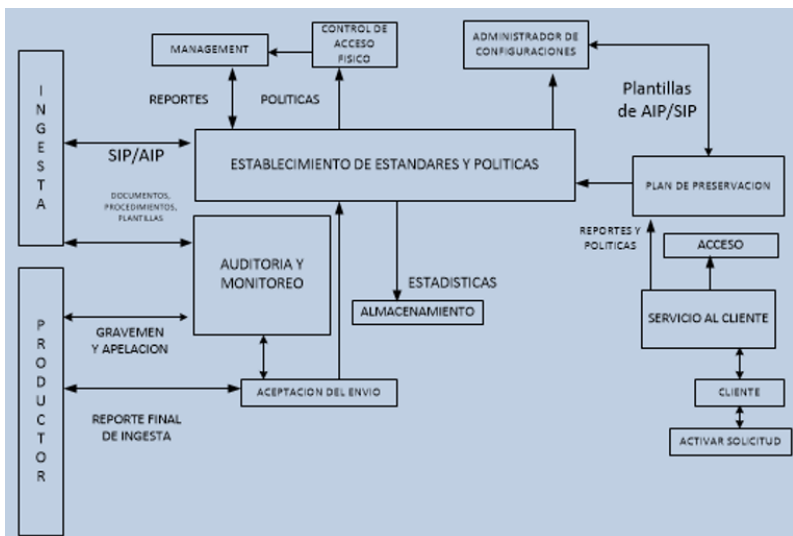


Figura 19. Entidad funcional administración
Elaborado por: los autores (basado en OAIS)

La función de aceptación del envío solicita archivos deseables para preservar y negocia con los productores. Esta función también negocia un calendario de presentación de datos con el productor. Mantiene un calendario de sesiones esperadas de envíos de datos, determinando los requerimientos que se necesitarán para transferir uno o varios SIPs a predeci y los recursos necesarios para apoyar su ingesta. Esta función recibe AIP/SIP en plantillas sugeridas por planificación de preservación y los envía a la función de auditoría como parte del proceso de aprobación de envío. También envía SIP y AIP a la función de establecimiento de estándares y políticas para su posterior utilización

por la función de la ingesta. Los formatos de presentación de datos y los procedimientos deben documentarse claramente en las políticas de envío de datos del archivo, y las entregas deberán identificarse por el productor en el acuerdo de envío.

La función de control de acceso físico proporciona mecanismos para restringir o permitir el acceso físico (puertas, cerraduras, guardias) a los elementos del archivo, según lo determinado por las políticas de archivo.

La función de establecimiento de estándares y políticas es responsable de establecer y mantener las políticas y normas del sistema de archivo. Recibe información del presupuesto y políticas, ámbito de aplicación, las pautas de utilización de recursos y políticas de precios de gestión. Proporciona administración con informes periódicos. Recibe las recomendaciones para la mejora del sistema de archivo, propuestas de nuevos estándares de datos de archivo e informes de análisis de riesgo periódicos emitidos por planificación de la preservación. Debe gestionar los riesgos de acontecimientos imprevistos y tomar las decisiones adecuadas para minimizar el riesgo de no cumplir con los compromisos de la entrega de evidencia.

Los estándares incluyen formato estándares de documentación y los procedimientos que deben seguirse durante el proceso de ingesta.

En respuesta a las recomendaciones de planificación de preservación en actualizaciones del AIP proporciona normas aprobadas a la

planificación de la preservación. Desarrollará políticas de recuperación ante desastres. También determinará las políticas de seguridad para el contenido del archivo, incluyendo aquellas que afectan al control de acceso físico, como el DRM y la aplicación de técnicas de control de error en el archivo.

La función de auditoría y monitoreo verificará que los envíos (SIP o AIP) cumplen con las especificaciones del acuerdo de envío. Esta función recibe comentarios AIP/SIP desde la planificación de preservación y puede también implicar a un comité externo (por ejemplo, ciencia y revisión técnica); Estos comentarios un informe sobre si las plantillas de AIP/SIP han aplicado correctamente en la ingesta. El proceso de auditoría debe verificar que la calidad de los datos cumple con los requisitos de archivo y el comité de revisión.

Debe verificar que no hay información adecuada representación y PDI para asegurar que la información contenido sea comprensible y utilizable independientemente a la comunidad señalado. El trámite de la revisión variará dependiendo de las políticas internas de archivo. Se proporciona un informe de auditoría para la ingesta. Después de completar el proceso de auditoría, se reportan cualquier gravamen al productor, que luego vuelva a enviar el SIP a ingesta o apelar la decisión de la administración.

La función de servicio al cliente crea y mantiene cuentas de consumo. Recogerá información de facturación de acceso y a envía facturas y

debe cobrar el pago de los clientes para la utilización de los recursos de predecí. Esta función también recogerá y responderá a los comentarios sobre productos y servicios de acceso y debe resumir estos comentarios y hacerlos disponibles.

Entidad Plan de Preservación

Las funciones de la entidad funcional plan de preservación se ilustran en la figura 20.

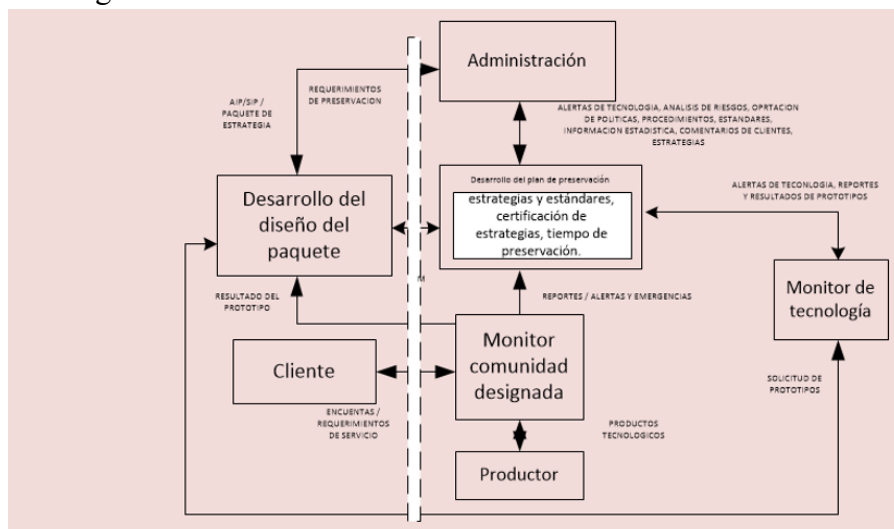


Figura 20. MODELO PREDECI-Entidad funcional plan de preservación
Elaborado por: los autores (basado en OAIS)

La función de monitor de comunidad designada interactúa con los clientes y productores y brinda un seguimiento a los cambios en sus requerimientos de servicio y disponibles tecnologías de producto. Estos requisitos pueden incluir formatos de datos, opciones de medios de comunicación, las preferencias de paquetes de software, nuevas plataformas de computación y mecanismos para la comunicación

con el archivo. Esta función puede ser lograda mediante encuestas, mediante un proceso de revisión periódica formal, mediante talleres comunitarios donde la retroalimentación es solicitada o interacciones individuales. Proporciona informes, alertas de los requisitos y estándares emergentes para la función de desarrollar estrategias de preservación.

La función monitor de tecnología es responsable del seguimiento de las nuevas tecnologías digitales, estándares de información y plataformas (es decir, hardware y software) para identificar las tecnologías que podrían causar obsolescencia en el entorno informático del archivo e actualizar el banco de software.

La función de desarrollo del diseño del paquete desarrolla nuevos diseños de paquete de información detallado y prototipos, para implementar las directrices y políticas de la administración. Esta actividad también ofrece asesoramiento sobre la aplicación de estos diseños de paquete de información. Esta función también ofrece personalización asesoramiento y revisión AIP/SIP a la administración sobre la aplicación de los diseños. Si esta función se encuentra con presentaciones que no están cubiertas por las normas y procedimientos existentes, puede enviar temas a desarrollar estrategias de conservación y las normas y recibir consejos, incluyendo nuevos estándares, para ayudar a satisfacer los nuevos requisitos de presentación.

La función de desarrollo del plan de preservación es responsable de desarrollar y recomendar estrategias y normas y para la evaluación de riesgos, para habilitar el archivo hacer intercambios informados ya que establece las normas, establece las políticas y gestiona su infraestructura del sistema. Esta función proporciona informes de análisis de riesgo periódicos a administración abordar los riesgos previstos y su mitigación posible, para funcionamiento de las políticas, normas y procedimientos. Esta función recibe informes, alertas de los requisitos y estándares emergentes desde el monitor de comunidades designadas y del monitor de tecnologías, y recibe las políticas, procedimientos y normas de funcionamiento, información sobre la performance, informes de inventario y resumidos comentarios del consumidor de la administración.

Este proceso se basa en las políticas de preservación de la organización y de las leyes vigentes, y la certificación en las políticas propias de cada técnica, estrategia y plan de largo plazo.

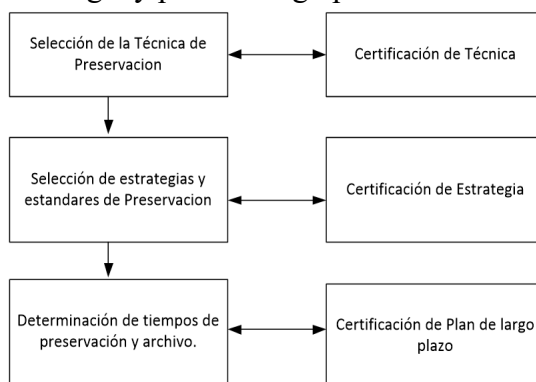


Figura 21: Plan de Preservación PREDECI
Elaborado por: los autores (basado en OAIS)

Función acceso

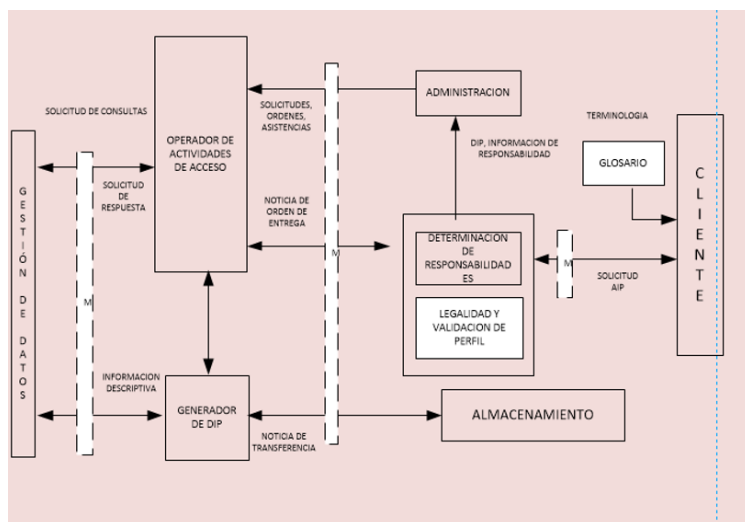


Figura 22. Entidad Funcional Acceso
Elaborado por. El autor (basado en OAIS)

La función de operador de actividades de acceso proporciona una o más interfaces a las explotaciones de evidencias. Esta interfaz será normalmente vía red informática o enlace telefónico para un servicio en línea, pero también puede aplicarse en forma de una instalación walk-in, servicio pedido catálogo impreso. Se distinguen tres categorías de las peticiones del consumidor: las solicitudes de consulta, que se ejecutan en la gestión de datos y devolver inmediatas respuestas de la consulta para su presentación al usuario; solicitudes de informe, que puede requerir un número de consultas y producir con formato de informes para la entrega al consumidor; y órdenes, que podrán acceder a uno o ambos gestión de datos y almacenamiento de archivos para preparar un paquete de difusión de la información (DIP) para

la entrega. Una orden puede ser una orden ad hoc que se ejecuta una sola vez, o un orden basado en el evento que será mantenido por la función de activar las solicitudes en la administración e iniciada por una petición de difusión que pueda resultar en entregas periódicas de los artículos solicitados.

La función de generar DIP acepta una solicitud de difusión, recupera la AIP de almacenamiento y mueve una copia de los datos a una zona de almacenamiento temporal para su posterior procesamiento. Esta función también transmite una solicitud de informe de gestión de datos para obtener información descriptiva para la inmersión. Si se requiere un procesamiento especial, la función de generar DIP tiene acceso a los objetos de datos en el almacenamiento temporal y aplica los procesos solicitados. Los tipos de operaciones que pueden llevar a cabo incluyen funciones estadísticas, sub muestreo en dimensiones temporales o espaciales, conversiones entre diferentes tipos de datos o formatos de salida, y otro especializado procesamiento. Insertar información de DRM y filtrado de los datos personales para asegurar la consistencia con los derechos de usuario. Esta función coloca la respuesta de inmersión completa en el área de almacenamiento temporal y notifica a la función de coordinar las actividades de acceso que la evidencia está lista para la entrega. Cabe señalar que en algunas implementaciones de la AIP podrían mantenerse en el almacenamiento temporal de disponibilidad inmediata.

La función de dar respuesta y marca de copia autorizada se encarga de dar respuesta y establecer una marca de copia autorizada en la evidencia tanto on-line y off-line de las entregas de las respuestas a los clientes. Con una autorización especial, se puede excluir el procedimiento de marcado de la copia. Para la entrega en línea, acepta una respuesta de coordinar las actividades de acceso y lo prepara para la distribución en línea en tiempo real a través de enlaces de comunicación. Identifica el destinatario, determina el procedimiento de transmisión solicitado, coloca la respuesta en el área de almacenamiento temporal para transmitirse y soporta la transmisión en línea de la respuesta. Para la entrega fuera de línea recupera la respuesta de la función de coordinar las actividades de acceso, prepara listas de embalaje y otros registros de envío y luego envía la respuesta. Cuando la respuesta ha sido enviada, una notificación de orden de envío es devuelta.

Diagramas de flujo de datos

Muestra los flujos de datos más importantes de predecí, donde se mantiene la estructura general de OASIS.

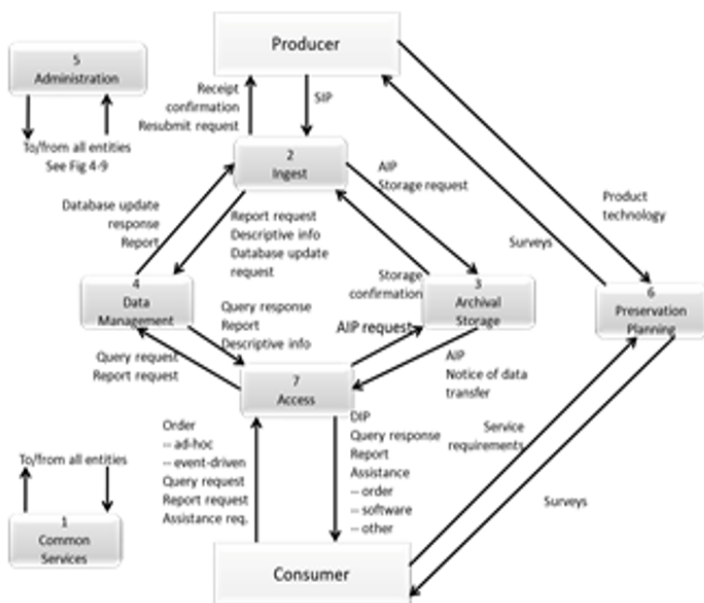


Figura 23: Diagrama de Flujo de Datos

Fuente: OAIS (Consultative Committee for Space Data Systems, 2012)

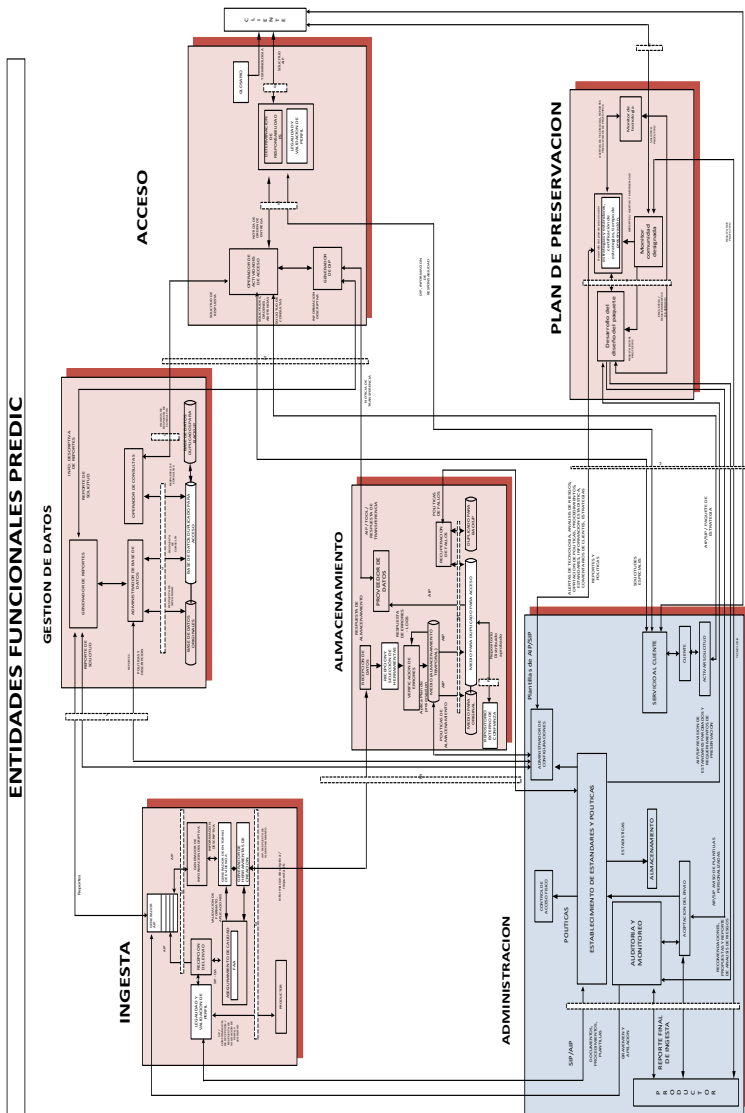


Figura 24. ENTIDADES FUNCIONALES PREDEC



GUÍA DE IMPLEMENTACIÓN

Capítulo 4



GUÍA DE IMPLEMENTACIÓN

Guía de implementación del modelo predecí

Con el fin de proporcionar una guía que facilite la implementación del modelo de preservación de evidencia digital para instituciones de investigación criminal, se documenta una guía de implementación del modelo predecí, la base para la presente guía de implementación del modelo predecí, es la planteada por OAIS y NESTOR, y consta de tres niveles (planes) y ocho marcos de trabajo.

Nivel 1: Plan de implementación

1. Marco Político

- Obtener el compromiso de la alta dirección.

2. Marco de Inicio

- Determinar el estado actual.
- Establecer el estado futuro deseado.

Nivel 2: Plan de desarrollo

3. Marco organizativo

- Determinar la gobernabilidad y viabilidad organizativa.
- Determinar la estructura organizacional y personal.
- Definición de objetivos.
- Definición de criterios para la selección de objetos digitales.
- Definición de responsabilidad de preservación a largo plazo.
- Definición de comunidad o comunidades designadas.
- Determinación de normas legales y contractuales.
- Establecimiento de financiamiento adecuado del repositorio

digital.

- Establecimiento del personal calificado y suficiente.
- Determinación de políticas de alertas tempranas.
- Definición de aspectos de gestión de la calidad.
 - Definir procesos y responsabilidades.

4. Marco Administración

- Definición de Políticas de aseguramiento de la integridad de los objetos digitales.
- Definición de políticas de aseguramiento de la autenticidad de los objetos digitales.
- Definición del plan estratégico de preservación.
- Definición de criterios de aceptación de objetos digitales de los productores.
- Determinación de especificaciones de archivo de los objetos digitales.
- Determinación de criterios de usabilidad de los objetos digitales.
- Determinación de aspectos de gestión de datos.
 - Configurar la gestión de la información.
 - Configurar la gestión de acceso.

5. Marco de infraestructura y seguridad

- Determinación de infraestructura adecuada.
- Determinación de seguridad de la infraestructura y objetos digitales.

6. Marco de instituciones de investigación criminal

- Configurar la gestión de evidencia en instituciones de investigación criminal.

7. Marco de generación de herramientas

- Creación del aplicativo.
- Instalación y configuración.

Nivel 3: Plan de evaluación de la implementación

1. Marco de evaluación

- Evaluación del estado final
- Capacitación
- Informe final

Proceso de aplicación de la guía de implementación del modelo Predecí

Nivel 1: Plan de implementación

1. Obtener el compromiso de la alta dirección

- Objetivo.

Obtener el apoyo de la alta dirección y difundir entre las partes interesadas (stakeholders) la decisión de la implementación del modelo de preservación de evidencia digital a través de los medios habituales de divulgación interna.

- Actividades
 - Presentar el Modelo PREDECI a la alta dirección.
 - Explicar el alcance del proyecto.

- Definir los roles y los responsables de la implementación del proyecto.
- Definir un plan de implementación.
- Definir un cronograma de implementación.
- Informar a las partes interesadas.
- Entregables
 - Documento con el apoyo y compromiso de la alta dirección en la implementación del proyecto.
 - Documento con el plan de implementación, los roles y responsables de cada actividad y el cronograma de implementación del proyecto.

2. Determinar el estado actual

- Objetivo
 - Determinar, por medio del modelo PREDECI de una autoevaluación propuesto, un estado actual de la preservación de evidencia digital.
- Actividades
 - El responsable de TI debe leer y entender la guía para el diligenciamiento de la autoevaluación descrito en el anexo 5.
 - El responsable de TI debe diligenciar la autoevaluación propuesta, la cual se encuentra en el anexo 2.
 - Trasladar los resultados numéricos a una nueva columna “estado actual” de la autoevaluación, al formato de análisis de resultados basado en el anexo 6, para observar gráficamente los resultados.

- Entregables
 - Documento de la autoevaluación de preservación de evidencia digital en la institución.
 - Documento de análisis de resultados de la valoración de la situación actual.

3. Establecer el estado futuro deseado

- Objetivo:
 - Determinar, con la ayuda del modelo PREDECI de autoevaluación propuesto, un estado futuro deseado según el modelo de preservación de evidencia digital PREDECI.
- Actividades
 - El responsable de TI debe leer y entender la guía para el diligenciamiento de la autoevaluación descrito en el anexo 5.
 - Teniendo especial atención en una nueva columna de “nivel deseado”, el responsable de TI debe diligenciar la autoevaluación, la cual se encuentra en el anexo 2.
 - Trasladar los resultados numéricos de la columna “nivel deseado” de la autoevaluación, al formato de análisis de resultados propuesto en el anexo 6 para observar gráficamente los resultados.
- Entregables
 - Documento de la autoevaluación de preservación de evidencia digital en la institución.
 - Documento de análisis de resultados de la valoración de la situación deseada.

Nivel 2: Plan de desarrollo

1. Marco organizativo

El repositorio digital actúa dentro de un marco organizativo que es determinado por los objetivos definidos, las condiciones legales y los recursos financieros y personales disponibles.

Debe tener un concepto claro de sus objetivos. Debe determinarse las acciones para que tareas y los principios cumplan los objetivos. Esto es crucial, pues la confiabilidad no es un término absoluto, entonces depende de los objetivos definidos por la institucionalidad. Deben transparentarse los objetivos para que los usuarios puedan medir la confiabilidad por sí mismos.

- Objetivo
 - Establecer las condiciones mínimas de gobernabilidad y de organización de la institución para una adecuada implementación del modelo predecí.
- Actividades
 - Determinar la gobernabilidad y viabilidad organizativa, la estructura organizacional y personal.
 - Definición de objetivos.
 - Definición de criterios para la selección de objetos digitales.
 - Definición de responsabilidad de preservación a largo plazo.
 - Definición de comunidad o comunidades designadas.
 - Determinación de normas legales y contractuales.
 - Establecimiento de financiamiento adecuado del repositorio digital.

- Establecimiento del personal calificado y suficiente.
- Determinación de políticas de alertas tempranas.
- Definición de aspectos de gestión de la calidad.
 - Definir procesos y responsabilidades.
- Entregables
 - Documento de políticas de gobernabilidad y organización.
 - Documento de objetivos, directrices de colección, criterios de selección, criterios de evaluación o criterios de generación de evidencia.
 - Documento de declaración explícitamente y de responsabilidad para la preservación a largo plazo de los objetos digitales ingeridos. Preservación a largo plazo aquí significa retención permanente de la usabilidad de la información representada por los objetos digitales (cf. el modelo OAIS de información).
 - Documento de definición de la comunidad o comunidades designadas. Esto incluye el conocimiento de las necesidades específicas de ellas, que influyen en la selección de los servicios a prestarse y en la accesibilidad de las comunidades a los objetos digitales en el largo plazo. Si la comunidad o comunidades designadas o sus requerimientos cambian con el tiempo, deben definirse políticas de cambio o de adaptación de sus servicios.
 - Documento de las condiciones de uso y costos de recursos.
 - Documento de normas legales y reglas contractuales con los

productores, consumidores que aseguren la seguridad de la preservación, archivo y uso de los contenidos de los objetos digitales.

- Documento de garantía financiera en el corto y largo plazo, y de disponibilidad de personal.
- Documento de políticas de alerta temprana de cambios legales, sociales, de demandas y expectativas de las comunidades designadas, de progresos tecnológicos. Incluye un plan de contingencia en caso de funcionar en un marco organizativo diferente, para garantizar su funcionalidad.
- Documento de definición de gestión de la calidad, para asegurar que se alcanzan los objetivos planteados, estableciendo estructuras de proceso adecuadas que deben ser controladas por el sistema de gestión de calidad. La gestión de la calidad debe ser un proceso transversal que cubre todas las partes del repositorio.
- Documento de definición de los procesos y sus, en particular que individuos se haya asignado la responsabilidad de los procesos. Esto también se aplica a procesos externos (outsourcing).

2. Marco administración

El repositorio digital debe analizar sus objetivos y estrategias y especificar todos los requisitos para la gestión de objetos digitales durante el tiempo de preservación. Las principales fases que

corresponden en el modelo de referencia predecí, son los procesos de ingesta, almacenamiento, implementación de medidas de preservación a largo plazo y el acceso. La administración de objetos se basa en la entidad funcional de información del modelo de referencia OAIS y define paquetes de información de presentación adecuada (SIP), archivos de paquetes de información (AIP) y paquetes de información de difusión (DIPs).

La integridad y autenticidad de la información a ser recibida son conceptos básicos de confiabilidad. La integridad y autenticidad deben garantizarse en todo momento de la operación del modelo predecí. Para transparentar la confiabilidad deben definirse normas específicas para la ingesta, almacenamiento, preservación y uso. El repositorio lleva a cabo la gestión de datos de una manera transparente, basado en metadatos, para cumplir con los requisitos de integridad, autenticidad y admisibilidad. Estos requisitos deben ser considerados al definir la seguridad de la infraestructura.

- Objetivos.
 - Definir políticas, planes, criterios y especificaciones que permitan determinar el proceso adecuado de gestión de la información y de los usuarios involucrados.
- Actividades
 - Definición de políticas de aseguramiento de la integridad de los objetos digitales.

- Definición de políticas de aseguramiento de la autenticidad de los objetos digitales.
- Definición del plan estratégico de preservación.
- Definición de criterios de aceptación de objetos digitales de los productores.
- Determinación de especificaciones de archivo de los objetos digitales.
- Determinación de criterios de usabilidad de los objetos digitales.
- Determinación de aspectos de gestión de datos.
 - Configurar la gestión de la información.
 - Configurar la gestión de acceso.
- Entregables
 - Documento que defina las políticas de aseguramiento de la integridad de los objetos digitales. Los criterios de integridad son las características de un objeto digital que le permite ser aceptable para su preservación. Debe definirse políticas para evitar riesgos a la integridad, sea por la actividad humana (maliciosa o accidental), por imperfección técnica o robo de la infraestructura técnica. Incluir la obligatoriedad de generar un informe en caso de existir algún inconveniente con el sistema de aseguramiento de la integridad, en todas las entidades del modelo predecí.

- Documento que defina las políticas de aseguramiento de la autenticidad de los objetos digitales. Autenticidad significa que el objeto es genuino, es decir, representa lo que pretende representar. Debe incluirse la documentación completa de todas las transformaciones a los objetos digitales que se preservan. Debe definirse los métodos para evaluar y asegurar la autenticidad.
- Documento de definición del plan estratégico de preservación que enliste todas las tareas pendientes o esperadas y el tiempo de su realización. Esta planificación estratégica debe especificarse en el nivel de objeto. Tales medidas deben mantener el ritmo de evolución técnica constante (cambio a soportes de datos, formatos de datos, usuario demandas etc....). Deben definirse medidas para la preservación física de los datos (integridad, autenticidad), su accesibilidad y la conservación de su interpretabilidad a largo plazo de la información representada por objetos digitales sus contenidos y metadatos.
- Documento de definición de criterios de aceptación de objetos digitales de los productores. Las directrices de la colección general, criterios de selección, criterios de evaluación o criterios para la generación de evidencia y los objetivos generales de conservación a largo plazo deben especificarse en el nivel de objeto. La transferencia puede efectuarse

mediante la presentación de los objetos por la parte emisora o a través de la colección manual o automática por parte de otro repositorio. Debe especificarse en común acuerdo con los productores o proveedores, que objetos digitales y metadatos deben ser ingeridos y que flujo de trabajo utilizarse. Estas especificaciones son la base para el control de calidad de los objetos. Documento que determine el alcance de las características de los objetos a ser preservados, considerando las posibilidades técnicas, las restricciones legales, los costos de preservación a largo plazo y las necesidades de la comunidad o comunidades designadas.

- Documento de determinación de especificaciones de archivo de los objetos digitales. Esto cubre la definición de los paquetes de archivos, almacenamiento de las AIPs y aplicación de las medidas de preservación a largo plazo. La definición de los paquetes de información de archivo debe incluir la determinación de las estructuras de paquete y objeto utilizado, además de ubicaciones de almacenamiento conveniente y formatos. Determinar los criterios de selección de los paquetes de información archivística, por tipos de objeto y las características de los objetos a preservar. Debe determinarse como el repositorio garantiza el almacenamiento y la legibilidad de los paquetes de información archivística. Determinar las medidas de preservación a largo plazo y monitoreo de plan de preservación.

- Documento que determine los criterios de uso de los objetos digitales, en el cual debe evidenciarse los criterios de que o quienes pueden usar los objetos preservados, criterios de búsqueda y acceso con respecto a los paquetes o unidades de información. Debe determinarse los criterios de difusión de los paquetes de información dependiendo de la comunidad o comunidades designadas, por medio de copias o derivados (posiblemente en combinación con otra información) que ayudan a la interpretación. Esto podría ser una descripción técnica, software de aplicación adicional o software de emulación. Para intercambiar datos con otros repositorios digitales, o para migrar los datos a una infraestructura técnica diferentes es necesario transformar partes, o todo el contenido del repositorio en un formato de exportación documentada, estandarizada. La información así puede conservarse más allá de la vida de repositorio digital. Los paquetes de información de difusión deben ser derivados de los paquetes de información archivística según un procedimiento definido.
- Documento que determine la definición de aspectos de gestión de datos. Gestión de datos es un proceso transversal que apoya los procesos de ingesta, almacenamiento, preservación y acceso, garantizando la integridad y autenticidad en todas las etapas del proceso. El alcance del sistema de gestión de datos se basa en los objetivos del repositorio.

En la gestión de datos debe realizar las siguientes tareas:

- Identificación de los objetos digitales y sus relaciones.
- La condición para encontrar y acceder a objetos digitales por medio de una descripción formal de su contenido y estructura.
- Garantizar la interpretación y la integridad y planificación e implementación de medidas de preservación, con la descripción técnica de los objetos.
- Generar la documentación de todos los cambios a los objetos digitales para asegurar la autenticidad de los datos.
- Grabación de todas las restricciones legales y su base para asegurar que los requisitos legales se observan a lo largo de la tramitación.

Estas tareas se cumplen en la actualidad por la generación y el almacenamiento de metadatos. Los Metadatos pueden grabarse de forma estructurada en un plan de metadatos. Se han establecido varios esquemas de metadatos para diferentes propósitos (por ejemplo, metadatos descriptivo, estructural, técnico, administrativo, legal).

Se debe tratar de aplicar un estándar nacional o internacional de un esquema de metadatos para propender a una sostenibilidad de los datos, y un adecuado intercambio de datos y la cooperación entre los productores/proveedores, y los usuarios. Debe determinarse reglas para el llenado de los campos con contenido (como el uso de terminología controlada).

3. Marco de infraestructura y seguridad

La infraestructura debe proteger los objetos digitales de peligros externos y basados en el sistema. Los riesgos basados en el sistema podrían surgir por ejemplo debido a problemas de hardware o la falta de medios de almacenamiento de información individuales.

Externamente se debe proteger contra amenazas naturales (fuego, agua, actividad sísmica) y también contra los riesgos causados por los seres humanos. Los objetos pueden ser dañados directamente por los empleados o a través de programas nocivos de contrabando en el sistema (por ejemplo, virus). Protección de los datos también implica evitar el envío accidental de la información por programas (troyanos) o personas (espionaje). La protección debe cubrir los objetos, las instalaciones utilizadas por el repositorio, el hardware, software y, no menos importante, el personal. Los diferentes riesgos deben ser contrarrestados por un conjunto de técnicas (por ejemplo, programas antivirus) y organizativos (p. ej. restricciones de acceso) medidas.

- Objetivo
 - Determinar la configuración de la infraestructura de TI adecuada y los aspectos de seguridad.
- Actividades
 - La infraestructura es adecuada.
 - La infraestructura implementa los requisitos de gestión objeto.

- La infraestructura implementa los requisitos de seguridad del sistema de seguridad de ti.
- La infraestructura protege el repositorio digital y sus objetos digitales.
- Entregables
 - Documento que determine la infraestructura adecuada. La infraestructura de TI debe poner las especificaciones para el manejo de los objetos a la práctica en los niveles de tecnología y seguridad. Es responsable de la totalidad de los objetos. Debe especificarse los requisitos a ser implementados con respecto a la manipulación de objetos por el aplicativo en todas las etapas del proceso. Esto incluye los principales procesos de ingesta, almacenamiento para archivo, acciones de preservación y el acceso y la gestión de datos.
 - Los requisitos de seguridad de gestión de objeto que deben tenerse en cuenta durante la realización.
 - Aseguramiento de la integridad de los objetos, es decir, protegiéndolas de modificaciones ilegales derivados de acciones humanas deliberadas y no intencionales y de imperfecciones técnicas.
 - Garantizar la autenticidad de los objetos.
 - Asegurar la confidencialidad de los objetos, es decir, excluyendo la posibilidad de adquisición no autorizada de información.

- Garantizar la disponibilidad de los objetos a través de la disponibilidad del objeto de las funciones de gestión (protección contra sabotajes, errores del sistema etc....)

4. Marco de instituciones de investigación criminal

- Implementación de los aspectos necesarios para la aplicabilidad en el entorno de investigación criminal, (Molina & Rodriguez, 2015a).
- Objetivos.
 - Establecer la inclusión de los requerimientos del modelo predecí en la institución.
- Actividades
 - Establecer la legalidad de la evidencia.
 - Garantizar la confidencialidad.
 - Controlar la calidad de la ingesta.
 - Configurar la ingesta parcial.
 - Determinar los metadatos del entorno de la evidencia a preservar.
 - Registrar la transmisión AIP, SIP, DIP.
 - Almacenar museo de herramientas.
 - Garantizar la integridad del original.
 - Definir el almacenamiento distribuido.
 - Establecer una terminología.
 - Determinar la evaluación de riesgos.
 - Establecer el tiempo de preservación.

- Generar certificaciones de la estrategia.
- Definir la trazabilidad y Continuidad de la preservación.
- Entregables
 - Documento que indique el procedimiento de legalidad de la evidencia a preservar, esto es que la evidencia cumpla la disposición legal para la preservación. El repositorio debe almacenar el documento de autorización, código de acceso, validación del acceso.
 - Documento que establezca políticas de confidencialidad del repositorio, es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información. La confidencialidad ha sido definida por la Organización Internacional de Estandarización (ISO) en la norma ISO/IEC 27002 como “garantizar que la información es accesible sólo para aquellos autorizados a tener acceso”. Registro completo del usuario y evidencia o evidencias que pueda acceder.
 - Documento que determine las acciones de control de calidad ingesta, el repositorio debe permitir la validación de formatos, contenidos o aplicaciones activas (ej.: virus). Validación de ingesta, antivirus de aplicaciones activas, formatos existentes, disponibilidad de herramientas de accesibilidad, responsabilidad de la información.

- Documento que indique el mecanismo de aplicación de ingesta parcial, el repositorio debe permitir recibir información o contenido dividido en partes. Se permite heredar datos o recibe nuevos datos de otros sistemas de confianza. Permite actualizar datos incrementales (una vez que se realiza el proceso de admisión, aumenta su contenido o metadatos).
- Documento que determine los aspectos o características de los metadatos del entorno de la evidencia a preservar. El repositorio debe preservar además información técnica y descriptiva sobre el medio ambiente de la colección de las evidencias, permite para demostrar que datos tienen un soporte legal, que hay alguien a cargo de los contenidos de los datos y hay una especificación completa del medio ambiente donde se generó la evidencia digital, para garantizar una recreación del entorno para uso de la evidencia preservada.
- Documento del procedimiento de transmisión de AIP, SIP, DIP. Debe registrarse la transmisión de la información dentro del proceso de preservación, o entre unidades de almacenamiento y entre repositorios.
- Documento de manejo de la estrategia de preservación de preservar las herramientas de creación de las evidencias preservadas, el repositorio debe permitir conservar herramientas utilizadas para acceder a los objetos digitales preservados. Los metadatos del objeto mantienen información acerca de la herramienta que se utilizará.

- Documento que indique las políticas de para garantizar la integridad del original, el repositorio maneja técnicas adicionales para la seguridad, integridad, fiabilidad y accesibilidad de los datos (impuestas por la organización). Debe generar informes de los mecanismos de autenticación y proporcionar información de autenticación para garantizar que el contenido no es modificado de una manera no documentada. Permite certificar los datos originales o implementar otro mecanismo de supervisión para el acceso.
- Documento que determine como implementar el almacenamiento distribuido de los objetos digitales del repositorio, este debe permitir almacenar datos en repositorios compartidos, definidos previamente como de confianza.
- Documento que defina la terminología a utilizar el repositorio, este debe disponer de un glosario de términos para la interpretación de las acciones y procesos, que son únicos para este entorno.
- Documento de estrategias de evaluación de riesgos, que permita determinar, la supervisión o alertas de riesgos (amenazas, consecuencias, umbral).
- Documento de tiempo de preservación, que determina el horizonte de tiempo de preservación (ej.: hasta que el cambio en la tecnología, sólo hasta la discontinuación del uso, para un número limitado de años, “para siempre”).

- Documento de certificación de la estrategia que permita establecer los certificados digitales de una estrategia de preservación aplicada o una combinación de ellos. (migración, emulación, encapsulación, enfoques de reingeniería, no digitales).
- Documento para determinar la trazabilidad y continuidad de la preservación para disponer la capacidad de reconstruir el historial de la utilización o la localización de una evidencia mediante una identificación registrada, se requiere el control y registro de toda transacción.

5. Marco de generación de herramientas

Diseño, creación e instalación del aplicativo o aplicativos necesarios para la operativización del modelo, cumpliendo estrictamente las instrucciones del modelo predecí.

- Objetivos
 - Establecer un aplicativo los lineamientos de la guía de implementación del modelo predecí, y ponerlo en operación.
- Actividades
 - Establecer los requerimientos del aplicativo, en base al modelo predecí.
 - Crear el aplicativo, de manera directa, contrato de desarrollo o contrato de outsourcing, u otro.
 - Instalar el aplicativo y capacitar en su uso.

- Entregables
 - Documento que establezca los requerimientos del aplicativo en base al modelo de referencia predecí. Autorizados por el personal competente.
 - Aplicativo instalable, con manual de usuario y técnico.
 - Documento de capacitación a usuarios y administradores del aplicativo.

Nivel 3: Plan de evaluación de la implementación

1. Marco de evaluación

Es la evaluación del cumplimiento de la guía de implementación y el cumplimiento del estado deseado especificado en el punto tres de esta guía.

2. Evaluación del estado Final

- Objetivo
 - Determinar, con la ayuda del modelo de autoevaluación propuesto, un estado final según el modelo de preservación de evidencia digital predecí.
- Actividades
 - El responsable de TI debe leer y entender la guía para el diligenciamiento de la autoevaluación descrito en el anexo 5.
 - Teniendo especial atención en la columna de “nivel final”, el responsable de TI debe diligenciar la autoevaluación, la cual se encuentra en el anexo 6.

- Comparar los resultados numéricos de las columnas “valoración actual”, “valoración deseada” y “valoración final” de la autoevaluación, realizar un análisis gráfico.
- Entregables
 - Documento de análisis de resultados del estado inicial, deseado y final.
 - Documento que informe los resultados de la aplicación de los instrumentos de validación del repositorio.

Consideración de Capacitación

- Objetivo
 - Determinar un plan de capacitación a todo el personal de la institución que puede ser productor, consumidor o administrador del modelo predecí.
- Actividades
 - Desarrollar un plan de certificaciones de capacitación para el personal institucional.
 - Establecimiento de un plan de soporte permanente. Puede ser asistencia personal, telefónica o recursos online.
- Entregables
 - Documento de capacitación institucional ejecutado.
 - Manual de Usuario online.
 - Establecimiento de la estrategia de soporte permanente.

Consideración del informe final

- Objetivo
 - Generar un documento que indique todo el proceso de implementación del modelo predecí y del aplicativo para historial de TI y futuras auditorías e implementaciones.
- Actividades. -
 - Desarrollar un documento que evidencie el cumplimiento de la guía de implementación.
- Entregables
 - Documento final de la implementación de modelo predecí.
Es una recopilación de todos los entregables generados en la implementación del modelo predecí.

Flujo de trabajo de la guía



Figura 25. Flujo de trabajo de la guía de implementación
Elaborado por: los autores

Glosario de términos

Hay muchos términos que se utilizan en este modelo de referencia y que es necesario disponer del significado adecuado para su comprensión. Algunos términos pueden coincidir con otros o pueden diferir entre ellos, por eso la necesidad de especificarlos. Estos términos se definen a continuación.

- *Análisis forense.*- Técnica de análisis informático que permite extraer información de un soporte digital total o parcialmente.
- *AIP edición.*- Un AIP cuyo contenido información o descripción preservación ha sido actualizado o mejorado con la intención de no conservar la información, sino para incrementar o mejorar. Una edición de la AIP no se considera ser el resultado de una migración.
- *AIP versión.*- Un AIP cuyo contenido información o descripción preservación ha experimentado una transformación en una fuente de AIP y es un candidato para sustituir la fuente AIP. Una versión AIP se considera ser el resultado de la migración digital.
- *Archivo.*- En el contexto de preservación digital es una organización que pretende conservar la información para el acceso y uso por una comunidad señalado.
- *Archivos cooperantes.*- Los archivos que tienen las comunidades designadas con relacionados con sus intereses. Pueden ordenar y recopile datos de unos a otros. Como mínimo, los archivos deben acordar apoyar por lo menos un paquete de información

de envío (SIP) y paquete de difusión de la información (DIP) comunes para las solicitudes entre archive.

- *Autenticidad.*- El grado al cual una persona (o sistema) refiere a un objeto como lo que es pretendió ser. Autenticidad se juzga en base a evidencia.
- *Base de conocimientos.*- Un conjunto de información, constituida por una persona o un sistema, que permite a esa persona o sistema entender la información recibida.
- *Calidad.*- La calidad de un DR es el grado al que un número de propiedades inherentes caracterización satisfacer los requisitos especificados. Los requisitos aquí son prerrequisitos o las expectativas que están previstas y que generalmente se da por sentado u obligatorio.
- *Colección access.*- Una colección de AIPs que se define por una descripción de la colección y para que allí no es ninguna información de empaquetado para la colección en almacenamiento de archiving.
- *Colocación.*- Entidad que proporciona los servicios y funciones que gestionan el paquete de información de envío (SIP) proporcionado por el fabricante (o elementos internos bajo la supervisión de la administración) y preparan el contenido para almacenar y administrar los archivos.
- *Computación forense.*- Es la aplicación legal de métodos, protocolos y técnicas para obtener, analizar y preservar evidencia digital relevante para una materia en investigación.

- *Comunidad designada.*- Identificado un grupo de clientes potenciales que deben ser capaces de comprender un conjunto particular de información. La comunidad designada puede estar compuesta de múltiples comunidades de usuarios. Se define una comunidad designada por el archivo y esta definición puede cambiar con el tiempo.
- *Confidencialidad.*- Protección contra la divulgación no autorizada de los datos.
- *Consumidor.*- El papel desempeñado por aquellas personas, o sistemas de cliente, que se relacionan con servicios OAIS para preservar información de interés y tener acceso a esa información en detalle. Esto puede incluir otras OAIS, así como internos OAIS personas o sistemas.
- *Contenido información.*- Un conjunto de información que es el objetivo original de conservación o que incluye todo o parte de esa información. Es un objeto de información compuesta por su contenido objeto de datos y la información de su representación.
- *Coste.*- Relacionado con la preservación digital, precio valorado en unidades monetarias que hay pagar para preservar datos digitalmente.
- *Datos.*- Representación de la información que le permite ser interpretado, procesado e intercambiado.
- *Descripción asociada.*- La información que describe el contenido de un paquete de información desde el punto de vista de una ayuda de acceso particular.

- *Descripción de la colección.*- Un tipo de descripción del paquete que es especializado para proporcionar información sobre una recopilación de información del archivo para su uso por acceso.
- *Descripción de miembro.*- Una descripción asociada que describe a un miembro de una colección.
- *Diccionario de datos.*- Un repositorio oficial de los términos utilizados para describir datos.
- *Disponibilidad.*- El tiempo que los datos están disponibles para el usuario.
- *Emulación.*- Técnica informática que permite mediante un software generar otro archivo que imite uno anterior.
- *Estrategia de preservación.*- La estrategia es un procedimiento de acciones de preservación para mantener una colección de objetos digitales. La estrategia de preservación por lo tanto contiene una descripción detallada de las acciones de preservación que deben tomarse, incluyendo
- *Fiabilidad.*- Fiabilidad es la capacidad de un sistema para funcionar conforme a sus objetivos y especificaciones (es decir, hace exactamente lo que se dice que hace). La fiabilidad de un DR puede ser probada y evaluada sobre la base de un catálogo de criterios.
- *Fijeza información.*- La información que documenta los mecanismos que aseguren que el objeto contenido información no ha sido alterado de manera indocumentada. Un ejemplo es

un código compruebe de redundancia cíclica (CRC) para un archivo.

- *Gestión de datos.*- Los datos creados y almacenados en almacenamiento persistente de gestión de datos que se refieren al funcionamiento de un archivo. Algunos ejemplos de estos datos son datos contables para el consumidor de facturación y autorización, política de datos, datos de orden basado en el evento (suscripción) para las solicitudes de repetición, preservación proceso historia datos y datos estadísticos para la generación de informes de administración de archivos.
- *Gestión.*- En el contexto de preservación digital es quien decide las políticas globales del modelo de preservación como componentes de una política más general.
- *Independientemente comprensible.*- Una característica de la información que está suficientemente completo para permitir que ser interpretado, entendido y utilizado por la comunidad señalado sin tener que recurrir a los recursos especiales no está ampliamente disponibles, incluyendo individuos llamados.
- *Información de contexto.*- La información que documenta las relaciones de la información contenido a su entorno. Esto incluye el por qué fue creada la información de contenido y cómo se relaciona con otros objetos de contenido de la información.
- *Información de descripción de preservación (PDI).*- La información que es necesario para la adecuada preservación de la información de contenido y que pueden ser categorizados

como procedencia, referencia, fijeza, contexto y la información de los derechos de acceso.

- *Información de los derechos de acceso.*- La información que identifica a las restricciones de acceso relativas a la información de contenido, incluyendo el marco legal, licencias, control de acceso y condiciones. Contiene las condiciones de acceso y distribución establecidas dentro del acuerdo de sumisión, relacionados con preservación y uso final (por parte del consumidor). También incluye las especificaciones para la aplicación de las medidas de observancia de los derechos.
- *Información de procedencia.*- La información que documenta la historia de la información de contenido. Esta información indica el origen o la fuente de la información, los cambios que pueden haber tomado lugar desde que se originó, y que ha tenido la custodia de ella desde que se originó. El archivo es responsable de crear y preservar información de procedencia desde el punto de ingesta. Sin embargo, debe proporcionarse información de procedencia anterior por el productor. Información de procedencia se suma a las evidencias que apoyan la autenticidad.
- *Información de referencia.*- La información que es utilizada como un identificador para la información de contenido. También incluye identificadores que permiten sistemas externos para referirse claramente a una determinada información. Un ejemplo de información de referencia es un ISBN.

- *Información descriptiva.*- Conjunto de datos, en su mayoría compuesta por descripciones de paquetes proporcionadas a la entidad de gestión de datos para ayudar a los usuarios buscar, clasificar y recuperar la información de la OAIS.
- *Largo plazo.*- Unidad de tiempo que se considera en un archivo digital para preservar digitalmente objetos. Se consideran largo plazo períodos superiores a 10 años. Este tiempo es suficientemente largo para ser conscientes de los impactos de los cambios tecnológicos, incluyendo soporte para nuevos medios y formatos de datos además de los cambios en una comunidad de usuarios sobre la información que está siendo retenida por un repositorio.
- *Metadatos.*- Datos sobre otros datos.
- *Migración.*- Técnica informática mediante la cual un objeto digital se convierte en otro de forma que permita ser accedido por un software más moderno. En el proceso de migración puede haber pérdidas de forma.
- *Modelo de referencia.*- Un marco para la comprensión de las relaciones significativas entre las entidades de un entorno y para el desarrollo de normas consistentes o especificaciones que apoyan ese ambiente. Un modelo de referencia se basa en un número pequeño de conceptos unificadores y puede usarse como base para la educación y explicar las normas a un no-especialista.
- *Objeto de datos.*- O un físico objeto o un objeto digital.

- *Objeto de datos de contenido.*- El objeto de datos, que junto con representación información asociada, comprende la información contenido.
- *Objeto de información.*- Un objeto de datos junto con su representación información.
- *Objeto digital.*- Unidad lógica discreta de datos digitales. Esto podría ser un simple objeto que consta de un solo archivo (por ejemplo, un documento PDF) o un objeto complejo que consta de un número de diferentes archivos (por ejemplo, una revista electrónica que consta de artículos individuales guardados como archivos). Información adicional (metadatos) puede añadirse a la información que representa el contenido (datos de contenido) que sirve por ejemplo la descripción formal y de contenido, la descripción estructural, la interpretación o la preservación a largo plazo del contenido (cf. presentación paquete, paquete archivado, paquete de acceso).
- *Objeto físico.*- Un objeto (por ejemplo, una roca de la luna, bio-espécimen, portaobjetos de microscopio) con propiedades físicamente observables que representan la información que se considera adecuado para ser adecuadamente documentado para conservación, distribución y uso independiente.
- *Orden adhoc.*- Una solicitud que se genera por un consumidor de información ha indicado la OAIS está actualmente disponible.

- *Paquete de información de difusión (DIP).*- Unidad de información derivados de AIPs uno o más y que un usuario recibe como respuesta a una consulta al RD. Consiste en un paquete de acceso a los datos que representan el contenido y cuando proceda, la información necesaria para la interpretación (por ejemplo, un archivo en formato .csv y descripción de la estructura de datos; un programa DOS en código y emulación de software para el sistema operativo del DOS).
- *Paquete de información de envío (SIP).*- Un paquete de información que se entrega por el productor a la OAIS para su uso en la construcción o actualización de uno o más AIPs y/o la información descriptiva asociada.
- *Planificación de Preservación.*- Entidad que proporciona los servicios y funciones relacionadas con monitoreo ambiental y la producción de direcciones OAIS para asegurar que la información almacenada en la OAIS siendo acceso a largo plazo señalado comunidad de usuarios, aunque el entorno informático original llega a ser obsoleto. La entidad de planificación de conservación no formaba parte de las pautas originales establecidas por CCSDS OAIS. (Consultative Committee for Space Data Systems, 2012) (medidas de preservación a largo plazo): la totalidad de todos los métodos utilizados específicamente para archivar objetos digitales indefinidamente y para que estén disponibles durante un período sostenido. Esto incluye métodos para la conservación

física de los datos y también el uso de técnicas de migración y emulación para cambiar los objetos archivados o sus entornos para garantizar su uso futuro.

- *Políticas de preservación.*- Una declaración formal de dirección u orientación acerca de cómo una organización llevará a cabo su mandato de preservación, funciones o actividades, motivadas por intereses determinados o programas.
- *Presentación acuerdo.*- El acuerdo alcanzado entre un OAIS y el productor que especifica un modelo de datos y cualquier otro arreglo necesario, para la sesión de presentación de datos. Este modelo de datos identifica el formato/contenido y los constructos lógicos utilizados por el productor y cómo se representan en cada entrega de los medios de comunicación o en una sesión de telecomunicaciones.
- *Preservación a largo plazo.*- El acto de mantener la información, independientemente comprensible por una comunidad designada y con evidencias que apoyen su autenticidad, por el término largo.
- *Preservación digital.*- Conjunto de técnicas o procesos que se ejecutan en una entidad de preservación de datos digitales y que contempla todo el ciclo de vida de un objeto digital y que permite acceder a la información de objetos digitales tecnológicamente obsoletos.

- *Productor.-* El papel desempeñado por aquellas personas o sistemas cliente que proporcionen la información a ser preservado. Esto puede incluir otros OAIS o interna OAIS personas o sistemas. Cualquier sistema cliente o persona que genera o proporciona la información a conservarse. Personas o cliente sistemas que transferir objetos digitales al repositorio para la preservación a largo plazo. No son necesariamente los creadores; también podrían ser los proveedores de los objetos digitales.
- *Propiedad de información.-* Esa parte de la información contenido según lo descrito por la descripción de la propiedad de información. La expresión detallada, o un valor de esa parte del contenido de la información es transmitida por las partes apropiadas del objeto de datos de contenido y su información de representación.
- *Propiedad de transformación de la información.-* Una propiedad de información la preservación del valor de los cuales se considera necesaria pero no suficiente para comprobar que cualquier transformación NonReversible ha conservado adecuadamente contenido de información. Esto podría ser importante como contribuyendo a las evidencias de autenticidad. Una propiedad tal información es dependiente sobre información específica de la representación, incluyendo información semántica, para denotar cómo está codificado y lo que significa. (A veces se usa

el término ‘importante propiedad’, que tiene varias definiciones en la literatura, de manera que sea consistente con su ser una propiedad de información transformacional).

- *Red de representación.*- El sistema de representación de información que describe completamente el significado de un objeto de datos. Información de representación en formularios digitales necesita información adicional de representación así sus formas digitales pueden ser entendidos en el largo plazo.
- *Reenvasado.*- A la migración digital en el que hay una alteración en la información de empaquetado del AIP.
- *Refresco.*- A la migración Digital donde el efecto es reemplazar a una instancia de medios con una copia que es lo suficientemente exacta que todo software y hardware de almacenamiento de archivos continúa su funcionamiento como antes.
- *Replicación.*- A la migración digital donde no hay ningún cambio en la información de empaquetado, la información de contenido y la PDI. Los bits utilizados para representar estos objetos de información se conservan en la transferencia a la instancia misma o nuevos medios de comunicación.
- *Repositorio digital (DR).*- Señalado de una organización (consistente en la gente y los sistemas técnicos) que ha asumido la responsabilidad de la conservación a largo plazo y la disponibilidad a largo plazo de datos digitales y su disposición para una determinada comunidad. “A largo plazo” significa aquí

dura más allá de los cambios tecnológicos (duro y software) y también los cambios a la comunidad designado (por ejemplo, para las generaciones futuras, indefinidamente).

- *Representación información.*- La información que se asigna a un objeto de datos en conceptos más significativos. Un ejemplo de representación de información para una secuencia de bits que es un archivo de ajustes podría consistir en los ajustes estándar que define el formato además de un diccionario que define el significado en el archivo de palabras clave que no forman parte de la norma.
- *Representación software.*- Un tipo de software que muestra información de representación de un objeto de información en forma comprensible para los seres humanos.
- *Resumen descripción.*- Una especialización de la descripción de la colección que describe la colección como un todo.
- *Transformación.*- A la migración digital en el que hay una alteración en el contenido de la información o PDI de un paquete de información archivística. Por ejemplo, cambiar códigos ASCII a UNICODE en un documento de texto que se conserva es una transformación.
- *Transformación irreversible.*- Una transformación que no puede
- *Transformación reversible.*- Una transformación en el cual la nueva representación define un conjunto o un subconjunto de entidades resultantes que son equivalentes a las entidades

resultantes definidas por la representación original. Esto significa que hay una asignación unívoca a la representación original y su conjunto de entidades de base.

- *Trazabilidad*.- Capacidad de seguimiento y reconstrucción de acciones efectuadas por los usuarios en un sistema.
- *Unidad de información archivística (AIU)*.- Un paquete de información archivística donde el archivo elige no descomponer la información contenido en otros paquetes de información archivística. Un AIU puede consistir en varios objetos digitales (por ejemplo, varios archivos).
- *Usuario*.- En el contexto de preservación digital, es cualquier persona natural o cliente que interactúan con los servicios de OAIS para obtener la información almacenada y para acceder a esta información en detalle.

Siglas y abreviaturas

Tabla 8. Siglas y abreviaturas

AIC	Recopilación de información archivística
AIP	Paquete de información archivística
AIU	Unidad de información archivística
API	Interfaz de programación de aplicaciones
ASCII	American Standard Code for Information Interchange
CCSDS	Comité consultivo para sistemas de datos espaciales
CDO	Objeto de datos de contenido
CRC	Comprobación de redundancia cíclica
DBMS	Sistema de gestión de base de datos
DIP	Paquete de información de difusión
DRM	Gestión de derechos digitales

FTP	File Transfer Protocol
HFMS	Sistema de gestión de ficheros jerárquico
ISO	International Organization for Standardization
OAIS	Sistema de información Archival abierto
PDF	Formato de documento portátil
PREDECI	Modelo de preservación de evidencia digital para instituciones de investigación criminal
PDI	Información de la descripción de preservación
QA	Aseguramiento de la calidad
PI3	Paquete de presentación información
UNICODE	Código universal
VHS	Sistema casero vídeo
XFDU	Unidad de datos con formato XML
XML	Extensible Markup Language

ACERCA DE LOS AUTORES

FERNANDO TIVERIO MOLINA GRANJA



Posdoctorado en Ciencias de la Informática con especialidad en Preservación de Evidencias Digitales. Doctorado en Ingeniería de Sistemas e Informática. Maestría en Informática Aplicada. Egresado de Maestría en Educación a Distancia. Magíster en Educación a Distancia E-Learning. Ingeniero en Sistemas. Experto en Procesos Elearning. Docente Agregado Titular Tiempo Completo Unach (Actual). Perito Informático Consejo de la Judicatura (Actual). Gerente Instituto de Investigaciones Informáticas y Forenses del Ecuador (Actual). Presidente Administrativo Sociedad Comercial Scallmo–Investigación Ingeniería y Desarrollo. Miembro del Consejo Politécnico de la Espoch. Director de Carrera de Ingeniería de Sistemas y Computación de la Unach. Presidente del Colegio de Ingenieros en Sistemas Informática y Computación de Chimborazo. Coordinador Académico Istra. Director Departamento de Soluciones Informáticas y Telemáticas Unidec. Evaluador externo con fines de acreditación Facultad de Ciencias Pecuarias - Espoch.

Presidente Administrativo Computec Movecoya y Cia. Coordinador de Maestrías. Ha publicado varios artículos en revistas con factor de impacto libros y proyectos de investigación en el area Informática e Informática Forense. Revisor de revistas indexadas. Participación en varios congresos como expositor. Speaker y miembro del Comité. Mas de 20 Años de experiencia en educación superior.

JUAN CARLOS SANTILLÁN LIMA



Ingeniero en Electrónica y Telecomunicaciones (UNACH, 2012). Magíster en Redes de Comunicaciones (PUCE, 2015). Candidato a Doctor en Ciencias Informáticas (UNLP, Argentina). Estudiante del Doctorado en Ingeniería (UNLP, Argentina). Es becario SENESCYT. Fue parte del grupo de investigadores del Instituto de Investigación ICITS de la UNACH. Fue docente de la UNACH desde el 2013 hasta el 2016. En la UEB fue Docente Investigador y Administrador de la Red de Telecomunicaciones desde el 2016 hasta el 2019. Desde el 2019 es investigador doctoral del instituto LEICI de la UNLP. Ha publicado más de 20 obras de relevancia a nivel nacional e internacional. Sus intereses de investigación son informática forense, preservación digital de datos, procesamiento estadístico de señales, redes de comunicaciones y educación.

WASHINGTON GILBERTO LUNA ENCALADA



Ingeniero Mecánico. Maestría en Informática Aplicada. Maestría en Educación a Distancia. En diciembre del 2018 obtuvo el Doctorado en Ingeniería en Sistemas e Informática. Es profesor de la Facultad de Informática y Electrónica de la Escuela Superior Politécnica de Chimborazo desde hace ya veinte y dos años. Actualmente ocupa el cargo de Decano. Es coordinador del proyecto de investigación “Modelos, metodologías y marcos tecnológicos para la implementación y uso de laboratorios virtuales”, de la ESPOCH. Autor de varios artículos científicos y libros en el área de la informática y computación.

RAÚL MARCELO LOZADA YÁNEZ



Licenciado en Ciencias de la Educación. Profesor de Informática Aplicada a la Educación (Universidad Nacional de Chimborazo, 2006). Magíster en Interconectividad de Redes (Escuela Superior Politécnica de Chimborazo, 2012). Magíster en Tecnologías para la Gestión y Práctica Docente (Pontificia Universidad Católica del Ecuador, 2015). Egresado del Programa de Doctorado en Ingeniería y Sistemas (Universidad Nacional Mayor de San Marcos, Lima-Perú). Docente del Colegio Daniel León Borja (Pungalá-Ecuador). Docente del Instituto Juan de Velasco (Riobamba-Ecuador). Docente de aula y miembro de la Unidad de Planificación Académica de la Universidad Nacional de Chimborazo (Riobamba-Ecuador). Docente de aula y director de la Academia Linux-ESPOCH de la Escuela Superior Politécnica de Chimborazo (Riobamba-Ecuador).

REFERENCIAS BIBLIOGRÁFICAS

- Instituto Nacional de Estadística y Censos. (2015). MANUAL DE ARCHIVO GENERAL Y GESTION DOCUMENTAL. Quito: Instituto Nacional de Estadística y Censos.
- Nestor working Group. (2009). Catalogue of Criteria for Trusted Digital Repositories. Version 2. Frankfurt: Nestor working Group Trusted Repositories.
- Acurio, S. (2008). Manual de Manejo de evidencias Digitales y entornos Informáticos. Recuperado el 17 de 12 de 2015, de https://www.oas.org/juridico/spanish/cyber/cyb47_manual_sp.pdf
- Ainsworth, A. B., Avram, C., & Sheard, J. (2012). The Monash University Museum of Computing: Ten Years On. History of Computing: Learning from the Past. Germany.: Ed. A. Tatnall. .
- Air Force Office of Special Investigations. (2002). “Preservation of Fragile Digital Evidence by First Responders”. Tudi [Query: May 6, 2014]. Digital Forensics Research Workshop. Recuperado el 6 de 01 de 2016, de <https://pdfs.semanticscholar.org/d82a/de2502c5a53f4a35d5f5560ebfe661740636.pdf>
- Allinson, J. (2006). OAIS as a reference model for repositories. An Evaluation. Obtenido de <http://eprints.whiterose.ac.uk/3464/>
- Alvarez, B. R. (2004). Avances en criptología y seguridad de la información. Ediciones Díaz de Santos.
- American Society of Crime Laboratory Directors. (2011). American Society of Crime Laboratory Directors. Recuperado

el 13 de 10 de 2014, de <http://www.asclld.org/>

- Ami-Narh, J. T. (2008). Digital forensics and the legal system: A dilemma of our times. Australian Digital Forensics Conference. Edith Cowan University. Obtenido de <http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1040&context=adf>
- Anderson, D. (2011). A layman's guide to the KEEP legal studies. KEEP Project deliverable. Portsmouth,: Keeping Emulation Environments Portable . Obtenido de <http://www.keep->
- Anderson, D., Delve, J., & Pinchbeck, D. (2010). Toward A Workable Emulation-Based Preservation Strategy: Rationale and Technical Metadata. New Review of Information Networking. Portsmouth, UK: Routledge. doi:DOI:10.1080/13614576.2010.530132.
- Anderson, D., Delve, J., & Powell, V. (2012). The Changing Face of the History of Computing: The Role of Emulation in Protecting Our Digital Heritage. (Vol. Vol. 387). Union Europea, ISBN 978-3-642-33898-4: Tantall.
- Arellano, M. A. (2004). reservação de documentos digitais. Ciência da Informação reservação de documentos digitais. Ciência da Informaçã. reservação de documentos digitais. Ciência da Informaçã. vol. 33. Recuperado el 2015, de <http://www.scielo.br/pdf/ci/v33n2/a02v33n2.pdf>
- Arias, J. (2008). ANÁLISIS PARA LA CREACIÓN ORGANIZACIÓN Y DESARROLLO DE LA BIBLIOTECA

DIGITAL DE COLOMBIA. Murcia: UNIVERSIDAD DE MURCIA.

- Asamblea Nacional del Ecuador. (12 de 09 de 2014). <http://www.datospublicos.gob.ec>. Recuperado el 16 de 10 de 2019, de LEY DEL SISTEMA NACIONAL DE REGISTRO DE DATOS: <http://www.datospublicos.gob.ec/wp-content/uploads/downloads/2017/05/LEY-ORGANICA-DEL-SISTEMA-NACIONAL-DE-REGISTRO-DE-DATOS-PUBLICOS.pdf>
- Ashoire, A., Bower, C., & Warden, C. (2013). An Overview of the Use of Digital Evidence in Internactional Criminal Courts. Salzburg Workshop on Cyber Investigations:. Berkeley.
- Association for Information Science and Technology. (30 de 6 de 2013). The Metadata Community — Supporting Innovation in Metadata Design, Implementation & Best Practices. Recuperado el 14 de 1 de 2015, de <http://dublincore.org/>
- Association of Chief Police Officers. (01 de 2005). Guidelines on the exchange of information between the Police & Insurance Companies and Loss Adjusters. Recuperado el 17 de 01 de 2015, de <https://www.abi.org.uk/globalassets/sitecore/files/documents/publications/public/2013/acpo-abi-memorandum-of-understanding.pdf>
- Banos, V., Freyre, E., Giaretta, D., Guercio, D., Hemmje, M., Ross, S., . . . Teruggi, D. (2011). Research on Digital Preservation within projects co-funded by the European Union in the ICT

programme. Europa.

- Beagrie, N., & Jones, M. (2008). Preservation Management of Digital Materials: The Handbook. Obtenido de Digital Preservation Coalition: <http://www.dpconline.org/graphics/handbook/>
- Bearman, D. (1999). Reality and Chimeras in the Preservation of Electronic Records. D-Lib Magazine, 5(4). Recuperado el 18 de Agosto de 2015, de D-Lib Magazine Vol. 5 N4: <http://www.dlib.org/dlib/april99/bearman/04bearman.html>
- Beavers, A. (enero de 2013). escritos. 21(46). Recuperado el 4 de 1 de 2016, de <http://www.scielo.org.co/pdf/esupb/v21n46/v21n46a03.pdf>
- Biros, D., Weiser, M., & Mosier, G. (2006). Development of a national repository of digital forensic intelligence. Journal of Digital Forensics, Security and Law,, 1(2), 5-17.
- Borck, J. (2001). Leave the Cybersleuthing to the Experts. InfoWorld 23, no. 54.
- Brenes Arias Abogados. (12 de 05 de 2015). Obtenido de <http://www.brenesariasabogados.com/contenido/>
- Byrne-Haber, S. (2 de 09 de 2015). THE DIGITAL ACCESSIBILITY MATURITY MODEL: DAMM AUDIT – FINAL REPORTING AND FOLLOW-ON ACTIVITIES. (LEVEL ACCESS) Recuperado el 1 de 10 de 2019, de <https://dev-level-access.pantheonsite.io/the-digital-accessibility->

maturity-model-damm-audit-final-reporting-and-follow-on-activities/

- Campos, F. (2002). La relevancia de la custodia de la evidencia en la investigación judicial.
- Candas Romero, J. (2006). El papel de los metadatos en la preservación digital. *El Profesional de la Información*, v. 15, nº 2, pp. 126-132.
- Cano, J., Rueda, S., & Torres, D. (2004). Consideraciones Técnicas y de Procedimiento para la Investigación de Delitos Informáticos. *Avances en Criptología y Seguridad de la Información. Actas de la VIII Reunión Española de Criptología y Seguridad de la Información*, (págs. 293-302). España.
- Caplan, P. (2009). Understanding Premis. *D-Lib Magazine*, Vol. 15, No. 3/4.
- Capurro, R. (2007). Epistemología y ciencia de la información. *Revista Venezolana de Información Tecnología y Conocimiento*, 4(1), 11-29.
- Casey, E. (2011). *Digital Evidence and Computer Crime*, 3d ed. London: Academic Press.
- Castillo, J. M. (2008). Emmagatzematge distribuït i preservació digital : una panoràmica d'alternatives. *Textos universitaris de biblioteconomia*.
- CCSD. (2012). *Reference Model for an Open Archival Information System (OAIS) 650.0-M-2*. Washington, DC, USA.

- Charlesworth, A. (2012). Intellectual Property Rights and Preservation. York: Digital Preservation Coalition 2012. Obtenido de <http://www.dpconline.org/advice/technology-watch-reports>
- Chivers, L. A.-B. (1 de 5 de 2019). www.planets-project.eu. The Open Planets Foundation. Obtenido de Retrieved from Integrating Planets and Fedora Commons:: <https://planets-project.eu/docs/casestudies/IntegratingPlanetsandFedoraCommons.pdf>
- Comité Interministériel sur les Métadonnées du Québec. (2010). Profils de metadonnéss gouvernementaux. Dossiers et documents. Version 2.0. Québec: Bibliothèque et archives Nationales. Obtenido de <http://collections.banq.qc.ca/ark:/52327/bs2007084#xml=http://services.banq.qc.ca/pdf>
- Condo, L., & Pazmiño, J. (2015). Diseño experimental en el desarrollo del conocimiento científico (Vol. 1). Riobamba: La Caracola Editores.
- CONSEJO DE EDUCACION SUPERIOR. (2016). Reglamento del Sistema de Archivos del Consejo de Educación Superior. QUITO: CONSEJO DE EDUCACION SUPERIOR.
- Conselho Nacional de Arquivos. (2011). Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos. Rio de Janeiro: Câmara Técnica de Documentos Eletrônicos.
- Consultative Committee for Space Data Systems. (2002). Reference Model for an Open Archival Information System

(OAIS) - BLUE BOOK. (C. C. Systems, Ed.) Washington, DC: CCSDS. Obtenido de <http://public.ccsds.org/publications/archive/650x0b1s.pdf>

- Consultative Committee for Space Data Systems. (2012). Reference Model for an Open Archival Information System (OAIS). Obtenido de <https://public.ccsds.org/pubs/650x0m2.pdf>
- Consultative Committee for Space Data Systems. (2012). Reference Model for an Open Archival Information System (OAIS) 650.0-M-2. Washington, DC, USA: CCSDS. Obtenido de <http://public.ccsds.org/publications/archive/650x0m2.pdf>
- Crow, R. (2002). The Case for Institutional Repositories: A SPARC position paper. Obtenido de Research on Institutional Repositories (IRs): http://works.bepress.com/ir_research/7/
- Cruz, R. C. (2016). Sistema de Información de Archivo Abierto (OAIS): luces y sombras de un modelo de referencia. Investigación bibliotecológica: archivonomía, bibliotecología e información, 30(70), 221-247. doi:10.1016/j.ibbai.2016.10.010
- Đaltur, Vahidin and Hajdarevic, Kemal. (2014). Digital Forensic Investigation, Collection and Preservation of Digital Evidence. International Symposium on Sustainable Development.
- Dappart, A. (2013). DePICT - a conceptual model for digital preservation. UNITED KINGDOM. Obtenido de <http://eprints.port.ac.uk>

- Dappert, A., & Farquhar, A. (2009). Significance is in the Eye of the Stakeholder. Obtenido de http://www.planets-project.eu/docs/papers/Dappert_Significant_Characteristics_ECDL2009.pdf
- Dappert, A., Jackson, A. N., & Kimura, A. (2013). Developing a Robust Migration Workflow for Preserving and Curating Hand-held Media. arXiv preprint arXiv:1309.4932. Obtenido de <http://arxiv.org/ftp/arxiv/papers/1309/1309.4932.pdf>
- DCC. (2009). CASPAR. Recuperado el 16 de 12 de 2014, de <http://www.dcc.ac.uk/resources/briefing-papers/technology-watch-papers/caspar>
- De Gius, M. R. (2014). Una metodología de evaluación de repositorios na digitales para asegurar la preservación en el tiempo y el acceso a los contenido. La Pla: Universidad Nacional de La Plata.
- Decision on Confirmation Charges, Case No. ICC-01/04-01/06 (International Criminal Court 29 de Enero de 2007). Obtenido de <https://www.icc-cpi.int/drc/lubanga/Documents/LubangaEng.pdf>
- Decision on the admission into evidence of materials contained in the prosecution's list of evidence., Case No. ICC-01/05-01/08 (19 de Noviembre de 2010). Obtenido de https://www.icc-cpi.int/CourtRecords/CR2010_10652.PDF
- Demant, D. (2010). Why the Real Thing is Essential for Telling

our Stories. History of Computing: Learning from the Past.

- Digital Preservation Coalition. (2006). Mind the gap: Assessing digital preservation needs in the UK. York: The Digital Preservation Coalition Innovation Centre. Recuperado el 15 de 1 de 2016, de https://www.google.com.ec/l?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjY2ePQjffQAhXM5yYKHUH3C7YQFggdMAA&url=http%3A%2F%2Fwww.dpconline.org%2Fcomponent%2Fdocman%2Fdoc_download%2F340-mind-the-gap-assessing-digital-preservation-needs-i
- Digital Preservation Coalition. (2008). Preservation Management of Digital Materials: The Handbook. Glasgow: Digital Preservation Coalition. Recuperado el 13 de 12 de 2015, de <http://www.dpconline.org/pages/handbook/docs/DPCHandbookIntro.pdf>
- Dobratz, S., & Schoger, A. (2007). Trustworthy digital long-term repositories: The Nestor approach in the context of international developments. Research and Advanced Technology for Digital Libraries. 4675, págs. 210-222. Hungary: Springer Berlin Heidelberg.
- Echeverria, P., & Ureta, A. (2009). Retos a superara en la administración de justicia ante los delitos informaticos en Ecuador. Ecuador: ESPOL.
- EcuRed. (2019). Auditoría de información. (EcuRed)

Recuperado el 5 de 11 de 2019, de https://www.ecured.cu/Auditoría_de_información

- Elliot, V. (20 de 9 de 2007). CLOCKSS Controlled LOCKSS (Lots of Copies Keep Stuff Safe). Recuperado el 10 de 09 de 2014, de <http://www.caul.edu.au/content/upload/files/preservation/caul20072clockss.pdf>
- European Commission, DG Information Society. (2002). Digicult report: technological landscapes for tomorrow's cultural economy; unlocking the value of cultural heritage. Belgium: Office for Official Publications of the European Communities. Obtenido de ftp://ftp.cordis.lu/pub/ist/docs/digicult/full_report.pdf
- Farquhar, A. &.-Y. (2008). Planets: Integrated services for digital preservation. *International Journal of Digital Curation*, 2(2).
- Federal Bureau of Investigation. (2013). Laboratory Division - FORENSIC SCIENCE COMMUNICATIONS. Recuperado el 17 de 4 de 2014, de <https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm>
- Ferreira, M. (2006). *Introdução à Preservação Digital: Conceitos, estratégias e actuais consensos*. doi:ISBN 9728692307
- Floridi, L. (2004). Open problems in the philosophy of information. *Metaphilosophy*, . (Vol. 35). Oxford: Oxford University Press.
- Floridi, L. (2013). *The Ethics of Information* (Vol. two of the

tetralogy). Oxford: Oxford University Press .

- Fredesvinda, I. M., Lázaro Herrero, C., & García González, N. (2008). “Electronic Judicial Evidence in the Struggle Against Cybercrime: A European Project”. . Revista Venezolana de Información, Tecnología y Conocimiento, 5(2), 139-152.
- Gallart, N., & Keefer, A. (2007). Preservació de dipòsits digitals. . Barcelona: Consorci de Biblioteques Universitàries de Catalunya. Recuperado el 18 de agosto de 2015, de <http://www.padicat.cat/es/conocenos/que-es-padicat/preservacion-del-patrimonio-digital>
- Garrett, J., Waters, D., Gladney, H., Andre, P., Besser, H., Elkington, N., & Hedstrom, M. (1996). Preserving Digital Information . Report of the Task Force on Archiving of Digital Information, commissioned by The Commission. Obtenido de <http://www.oclc.org/resources/research/activities/digpresstudy/final-report.pdf>
- Gingrande, A. (2011). The Long-term Preservation of Digital Evidence.
- Gladney, H. (2011). LONG - TERM DIGITAL PRESERVATION : WHY IS PROGRESS LAGGING? Saratoga.
- Gladney, H. M. (2005). Trustworthy 100-year digital objects: durable encoding for when it's too late to ask. ACM Transactions on Information Systems, 23(3), 229-324. Obtenido de <http://doi.acm.org/10.1145/1080343.1080346>
- Gladyshev, P. (2007). Formalising Event Reconstruction in

Digital Investigations.

- Gómez, D. (2003). Sistema de detección de Intrusiones. Recuperado el 14 de 12 de 2016, de https://www.dgonzalez.net/papers/ids/IDS_v1.0.pdf
- Gómez, L. (2013). Delitos, prueba y evidencia digital. Obtenido de <http://listas.hackcoop.com.ar/archivos/bla/attachments/20131026/b708d60b/attachment.pdf>
- Gómez, L. Á. (2010). Computer forensics, a tool to combat cybercrime.
- Guttenbrunner, M., & Rauber, A. (2012). A Measurement Framework for Evaluating Emulators for Digital Preservation. (ACM Transactions on Information Systems (TOIS) TOIS. Volume 30 Issue 2, Ed.) New York. Recuperado el 18 de Agosto de 2015, de <https://dl.acm.org/purchase.cfm?id=2180876&CFID=659863800&CFTOKEN=67254384>
- Guttenbrunner, M., Wieners, J., Rauber, A., & Thaller, M. (2010). Same Same But Different – Comparing Rendering Environments. .
- Harvey, D. R. (2005). Preserving digital materials. Society of American Archivists. Obtenido de <http://www.jstor.org/stable/40294335>
- Hedges, R. J. (2013). ELECTRONIC DISCOVERY: TRENDS AND DEVELOPMENTS UNDER THE FEDERAL RULES OF CIVIL PROCEDURE AND BEYOND. New Jersey.

- Hendley, T. (1998). Comparison of methods and costs of digital preservation. n British Library Research and Innovation Report.
- Holdsworth, D., & Wheatley, P. (2010). Emulation, Preservation and Abstraction. Recuperado el 12 de 10 de 2014, de <http://sw.ccs.bcs.org/CAMiLEON/dh/ep5.html>
- Hong, C., & Neil, P. (2012). Where does it go from here? The place of software in digital repositories. En T. U. Edinburgh (Ed.), The 7th International Conference on Open Repositories. Edinburgh, United Kingdom. Recuperado el 18 de Agosto de 2015, de http://www.research.ed.ac.uk/portal/files/6039037/Chue_Hong_Where_does_it_go_from_here_The_place_243_a.pdf
- Hoorens, R. V. (2007). Addressing the uncertain future of preserving the past: Towards a robust strategy for digital archiving and preservation. California: RAND Corporation. Obtenido de http://www.rand.org/pubs/technical_reports/TR510.html
- Insa, F. (2007). The Admissibility of Electronic Evidence in Court (A.E.E.C.): Fighting against High-Tech Crime—Results of a European Study. Journal of Digital Forensic Practice, 285-289.
- inteco. (2003). Inteco. Recuperado el 2015, de http://www.inteco.es/wikiAction/Security/Observatory/area_juridica_seguridad/Enciclopedia/Articulos_1/evidencia_electronica_es.
- International Organization for Standardization. (09 de 2001).

- ISO 15489-1:2001. (M. L. Vita-Finzi, Editor, & I. 4. 11, Productor) Recuperado el 15 de 10 de 2014, de <https://www.iso.org/standard/31908.html>
- International Organization for Standardization. (8 de 2011). ISO/TR 23081-3:2011 . (M. L. Vita-Finzi, Editor, & ISO/TC 46/ SC 11) Recuperado el 11 de 10 de 2014, de <https://www.iso.org/standard/57121.html>
 - International Organization for Standardization. (09 de 2012). Space data and information transfer systems -- Open archival information system (OAIS) -- Reference model. Recuperado el 21 de 11 de 2014, de <https://www.iso.org/standard/57284.html>
 - ISO. (2012). Space data and information transfer systems -- Audit and certification of trustworthy digital repositories. ISO 16363:2012.
 - Jenkins, C. (16 de 4 de 1998). The CEDARS Project CURL Exemplars in Digital ARchiveS. Obtenido de <http://www.ukoln.ac.uk/services/elib/projects/cedars/>
 - John, J. L. (2009). The future of saving our past. *Nature*, 459(7248), 775-776. . Great Britain: Published Digital Preservation Coalition in association with Charles Beagrie Ltd. doi:doi:10.1038/459775a
 - Joint Technology Committee. (2014). Developing an Electronic Records Preservation and Disposition Plan. Version 1.0. Williamsburg: JTC Resource Bulletin.

- Keefer, A., & Gallart, N. (2007). La preservación de recursos digitales. El reto para las bibliotecas del siglo XXI. . Barcelona: Editorial UOC.
- KEEP Project. (2012). Keeping Emulation Environments Portable. Recuperado el 18 de Agosto de 2015, de KEEP: <http://www.keep-project.eu/ezpub2/index.php>
- Kenneally, E. (2005). Risk sensitive digital evidence collection. Digit Investigation. The Digital Forensic Research Conference., 2(2), 101-109.
- Khaleel, Y. F. (2019). Assessing the Knowledge Level of Teachers of Children with Autism Spectrum Disorder about the Importance of Applied Behavior Analysis (ABA) Strategies in Zarka City. International Education Studies, 12(5). doi:10.5539/ies.v12n5p120
- Knight, G. (2009). InSPECT Framework Report. London: The NationalArchives. Obtenido de <http://www.significantproperties.org.uk/inspect-framework.pdf>
- Kroll Ontrack Inc. . (2006). Cyber Crime & Computer Forensics News.
- Kuchera, B. (2011). Accuracy takes power: one man's 3GHz quest to build a perfect SNES emulator. Obtenido de arstechnica: <http://arstechnica.com/gaming/2011/08/accuracy-takes-power-one-mans-3ghz-quest-to-build-a-perfect-snes-emulator/>
- Kulovits, H., Rauber, A., Kugler, A., Brantl, M., Beinert, T., &

- Schoger, A. (2009). From TIFF to JPEG 2000? Preservation Planning at the Bavarian State Library Using a Collection of Digitized 16th Century Printings. D-Lib Magazine, 15(11). Recuperado el 18 de Agosto de 2015, de D-Lib Magazine: <http://www.dlib.org/dlib/november09/kulovits/11kulovits.html>
- LA CAMARA NACIONAL DE REPRESENTANTES. (2009). Ley del Sistema Nacional de Archivos. Quito: LA CAMARA NACIONAL DE REPRESENTANTES. Obtenido de https://www.quito.gob.ec/lotaip2011/a2/Ley_del_Sistema_Nacional_de_Archivos.pdf
 - Lavoie, B., & Gartner, R. (2005). Technology Watch Report. Preservation Metadata. Oxford: Oxford University Library Services and Digital .
 - Lawrence, G., Kehoe, W., Rieger, Y., Walters, H., & Kenney, A. (2000). Risk Management of Digital Information: A File Format Investigation . Council on Library and Information Resources.
 - LeFurgy, W. (2009). NDIIPP partner perspectives on economic sustainability. Library Trends 413-426.
 - Library of Congress Network Development. (9 de 2 de 2016). Metadata Encoding and Transmission Standard. Recuperado el 25 de 3 de 2016, de <http://www.loc.gov/standards/mets/mets-profiles.html>
 - Lluca, C. (2006). Archivando la Web, el proyecto Padicat (Patrimonio Digital de Cataluña). El Profesional de la

Información, 15(6), 473-478. Obtenido de <http://hdl.handle.net/10760/8399>

- Lorie, R. A. (2001). Long Term Preservation of Digital Information. En I. A. Center (Ed.), Proceedings of the 1st ACM/IEEE- CS Joint Conference on Digital Libraries (JCDL '01)., (págs. pp. 346–352.). Roanoke, Virginia, USA. Obtenido de <http://old.hki.uni-koeln.de/teach/ss06/DL/material/p346-lorie.pdf>
- Lynch, C. (2003). Institutional Repositories: Essential Infrastructure For Scholarship In The Digital Age. Recuperado el 17 de Agosto de 2015, de Libraries and the Academy: http://muse.jhu.edu/login?auth=0&type=summary&url=/journals/portal_libraries_and_the_academy/v003/3.2lynch.pdf
- Martínez, R. (04 de 1 de 2012). La importancia de la evidencia y el análisis forense digital. Obtenido de <http://www.bsecure.com.mx/opinion>
- McCray, A. T., & Gallagher, M. E. (2001). Principles For Digital Library Development. Recuperado el 18 de Agosto de 2015, de <http://lhncbc.nlm.nih.gov/archive/20120315/publication/lhncbc-2001-017>
- McDowell, C. (2007). Evaluating Institutional Repository Deployment in American Academe Since Early 2005. Obtenido de D-Lib Magazine: <http://www.dlib.org/dlib/september07/mcdowell/09mcdowell.html>

- McHugh, A., Innocenti, P., & Ross, S. (15–18 de September de 2008). Assessing risks to digital cultural heritage with DRAMBORA. International Documentation Committee of the International Council of Museums (CIDOC). Athens, Greece,.
- McKemmish, R. (1999). “What Is Forensic Computing”, Australian Institute of Criminology--Trends and Issues in Criminal Justice.
- Mercer, L. D. (2004). Computer Forensics - Characteristics and Preservation of Digital Evidence. The FBI Law Enforcement Bulletin.
- Molina, F., & Rodriguez, G. (2015a). Digital Preservation and Criminal Investigation: A Pending Subject. En F. Molina Granja, & G. Rodriguez, New Contributions in Information Systems and Technologies (págs. pp 299-309). United State: Springer International Publishing. doi:978-3-319-16485-4
- Molina, F., & Rodriguez, G. (2015b). Preservation of Digital Evidence: Application in Criminal Investigation. Science and Information Conference. (págs. 1284 - 1292). London, United Kingdom.: Springer. doi:DOI: 10.1109/SAI.2015.7237309
- Molina, F., & Rodriguez, G. (2017b). The preservation of digital evidence and its admissibility in the court. nt. J. of Electronic Security and Digital Forensics., 9(1), 1-18.
- Molina, F., & Rodriguez, G. (2017c). MODEL FOR DIGITAL EVIDENCE PRESERVATION IN CRIMINAL RESEARCH

INSTITUTIONS – PREDECI. Int. J. of Electronic Security and Digital Forensics., 9(2), 150-166.

- Morán, A. (21 de 07 de 2015). Humanidades Digitales. Recuperado el 07 de 02 de 2017, de Red de Humanidades Digitales de México: <http://humanidadesdigitales.net/blog/2015/07/21/que-es-la-filosofia-de-la-informacion/>
- Moro-Cabero, M. (2013). TAXONOMÍA DE METADATOS DE PRESERVACIÓN. PontodeAcesso, 7(1), 132-153. Obtenido de www.pontodeacesso.ici.ufba.br
- National Digital Stewardship Alliance. (2014). NDSA National Agenda for Digital Stewardship. Recuperado el 28 de 10 de 2014, de <http://www.digitalpreservation.gov/ndsa/documents/2014NationalAgenda.pdf>
- National Digital Stewardship Alliance. (2015). National Digital Stewardship Alliance.
- Neifeald, E., & Nissim, Y. (2019). Co-Teaching in the “Academia Class”: Evaluation of Advantages and Frequency of Practices. International Education Studies, 12(5). doi:10.5539/ies.v12n5p86
- NESTOR. (2012). Obtenido de NESTOR : Network of Expertise in Long-Term Storage of Digital Resources: <http://www.langzeitarchivierung.de/index.php?newlang=eng>
- Nestor working Group. (2009). Catalogue of Criteria for Trusted Digital Repositories. Version 2. Frankfurt: Nestor working

Juan Carlos Santillán Lima
Group Trusted Repositories - Certification.

Washington Gilberto Luna Encalada

- Novak, A. (2006). Fixity Checks: Checksums, Message Digests and Digital Signatures. Raúl Marcelo Lozada Yáñez
ILTS Digital Preservation Committee.
Retrieved from. Yale: ILTS Digital Preservation Committee.
Obtenido de http://www.library.yale.edu/iac/DPC/AN_DPC_FixityChecksFinal11.pdf
- Open Archives. (2002). Open Archives Initiative. Obtenido de <http://www.openarchives.org/documents/FAQ.html>
- Open Planets Foundation . (2007). PLANETS. Obtenido de <http://www.planets-project.eu>
- Open Planets Foundation . (31 de mayo de 2010). PLANETS - PRESERVATION AND LONG-TERM ACCESS THROUGH NETWORKED SERVICES. Recuperado el 23 de 12 de 2014, de <http://planets-project.eu/>
- PANDORA, Australia's Web Archive. (24 de agosto de 2011). PADI : preserving access to digital information. (N. L. Australia., Editor) Recuperado el 6 de 10 de 2014, de PANDORA, Australia's Web Archive: <http://pandora.nla.gov.au/tep/10691>
- Patzakis, J. (2008). New Incident Response Best Practice.
- PREMIS Data Dictionary. (2012). Obtenido de <http://www.loc.gov/standards/premis/v2/premis-2-2.pdf>
- Proença, D. V. (2017). Information Governance Maturity Model Final Development Iteration. International Conference on Theory and Practice of Digital Libraries (págs. 128-139).

Springer.

- Rao, V. (2014). Immerging Digital Preservation Technology: It's Design, Initiatives and Challenges. International Journal of Innovate Research & Development.
- Research Libraries Group. (2002). Trusted Digital Repositories: Attributes and Responsibilities. California: RLG, Inc. Recuperado el 15 de 12 de 2016, de <http://www.oclc.org/programs/ourwork/past/trustedrep/repositories.pdf>
- Rimage. (2011). Digital Evidence Preservation and Distribution: Updating the Analog System for the Digital World.
- Rivera-Donoso, M. A. (2009). Directrices para la creación de un programa de preservación digital. Serie Bibliotecología y Gestión de Información, (43), 1-63(43), 1-63. Recuperado el 5 de 8 de 2019, de http://eprints.rclis.org/12989/1/Serie_N%C2%B043_Preservacion_digital.pdf
- Romano, L. V. (2005). VI. Electronic Evidence and the Federal Rules. Los Angeles: Loyola of Los Angeles Law Review.
- Rosenthal, D. (2010). Bit Preservation: A Solved Problem? The International Journal of Digital Curation., 5(1), 3. doi:doi:10.2218/ijdc.v5i1.148
- Rothenberg, J. (1998). Avoiding Technological Quicksand: Finding a Viable Technical Foundation for Digital Preservation. Obtenido de Council on Library and Information Resources: <http://www.clir.org/pubs/reports/rothenberg/contents.html>

- Rothenberg, J. (1999). Avoiding Technological Quicksand: Finding a Viable Technical Foundation for Digital Preservation. Washington,: Council on Library and Information Resources. Obtenido de <http://www.clir.org/pubs/reports/rothenberg/pub77.pdf>
- Rothstein, B. J., Hedges, R. J., & Wiggins, E. C. (2007). Digital forensics and the legal system: A dilemma of our times. Obtenido de [http://www.fjc.gov/public/pdf.nsf/lookup/eldscpkt.pdf/\\$file/eldscpkt.pdf](http://www.fjc.gov/public/pdf.nsf/lookup/eldscpkt.pdf/$file/eldscpkt.pdf)
- Sanchez, S., & Melero, R. (2006). REPOSITARIOS INSTITUCIONALES UNIVERSITARIOS: EVOLUCIÓN Y PERSPECTIVAS. Obtenido de <http://digital.csic.es/bitstream/10261/1487/1/OA2rm.pdf>
- Schatz, B. (2007). Digital Evidence: Representation & assurance, Information Security Institute,. Austria, p.3;: faculty of Information Technologies, Queensland University of Technologies,.
- SECRETARIA GENERAL DE LA PRESIDENCIA DE LA REPUBLICA. (2019). REGLA TÉCNICA NACIONAL PARA LA ORGANIZACIÓN Y. QUITO: SECRETARIA GENERAL DE LA PRESIDENCIA DE LA REPUBLICA.
- SECRETARIA NACIONAL DE LA ADMINISTRACION PUBLICA. (2015). NORMA DE GESTION DOCUMENTAL PARA ENTIDADES. DE ADMINISTRACION PUBLICA.

SECRETARIA NACIONAL DE LA ADMINISTRACION PUBLICA. Quito: Registro Oficial Suplemento 445 de 25-feb.-2015. Recuperado el 16 de 08 de 2019, de SECRETARIA NACIONAL DE LA ADMINISTRACION PUBLICA

- SECRETARIA NACIONAL DE LA ADMINISTRACION PUBLICA. (2015). NORMA TECNICA DE GESTION DOCUMENTAL Y ARCHIVO. QUITO: SECRETARIA NACIONAL DE LA ADMINISTRACION PUBLICA.
- Serra, J. (2001). Gestión de los documentos digitales: estrategias para. En El profesional de la información, 4 - 18. Obtenido de http://eprints.rclis.org/bitstream/10760/11449/1/Gesti%C3%B3n_de_los_d
- Shadish W., C. T. (2002). Experimental and Quasi-Experimental Designs for Generalized Causal Inference. . Boston, New York: Houghton Mifflin Company.
- Shustek, L. (2006). What should we collect to preserve the history of software? IEEE Annals of the History of Computing, 28(4), 112, 110-111. doi:10.1109/MAHC.2006.78
- Sierman, B. (2007). Report on Comparison of Planets with. Obtenido de https://www.planets-project.eu/docs/reports/Planets_PP7-D1_ReportOnComparisonOfPlanetsWithOais.pdf
- Spence, J. (2006). Preserving the cultural heritage: An investigation into the feasibility of the OAIS model for application in small organisations. Aslib Proceedings, 58(6)

513-524. doi:10.1108/00012530610713597

- Stawowczyk Long, A. (2009). LONG-TERM PRESERVATION OF WEB ARCHIVES – EXPERIMENTING WITH EMULATION AND MIGRATION METHODOLOGIES. Australia: Digital Preservation Standards.
- Strodl, S., Petrov, P., & Rauber, A. (2011). Research on Digital Preservation within projects co-funded by. Austria.
- Swanson, C. R. (2006). Criminal Investigation, 9th ed. New York: McGraw-Hill. .
- Térmens, M. (2009). Investigación y desarrollo en preservación digital: un balance internacional = Research and development in digital preservation: an international review. En El profesional de la información, 4-18. Recuperado el 15 de enero de 2014, de <http://eprints.rclis.org/bitstream/10760/16218/1/Investigacionpreservacion-EPI.pdf>
- Tessella. (2013). Digital Preservation Maturity Model - White Paper.
- Thaller, M., Heydegger, V., Schnasse, J., S., B., & Chudobkaite, E. (2008). Significant characteristics to abstract content: Long term preservation of information. Research and Advanced Technology for Digital Libraries, 41-49. doi:10.1007/978-3-540-87599-4_5
- The International Federation of Library Associations and Institutions. (2012). The Memory of the World in the Digital age: Digitization and Preservation. vacouver. Obtenido de <http://>

www.ifla.org/news/unesco-releases-vancouver-declaration-on-digitization-and-preservation

- The International Research on Permanent Authentic Records in Electronic Systems. (2013). The InterPARES Project. (A. &. School of Library, Editor, & T. U. Columbia, Productor) Recuperado el 5 de 10 de 2014, de <http://www.interpares.org/>
- The InterPARES Project. (2012). Digital Records Pathways: Topics in Digital Preservation. Module 3: Organizational Culture and its Effects on Records Management. USA: InterPARES / ICA. Recuperado el 9 de 10 de 2019, de http://interpares.org/ip3/display_file.cfm?doc=ip3_canada_gs12_module_3_july-2012_DRAFT.pdf
- The Library of Congress. (2008). Premis Data Dictionary for Preservation Metadata. Premis Editorial Committee. Obtenido de <http://www.loc.gov/standards/premis/index.html>
- The LOCKSS Program. (abril de 2004). Lots Of Copies Keep Stuff Safe. Recuperado el 25 de 12 de 2014, de <https://www.lockss.org/>
- Thomson, L. (2011). Admissibility of Electronic Documentation as Evidence in U.S. courts.
- Torres Freixinet, L. (2008). Preservacion Digital, el Reto del Futuro. Actas de las VIII Jornadas de Archivos Aragoneses. Huesca: Gobierno de Aragón, (págs. 75-94). Huesca.
- U.S. Department of Justice. (2004). Forensic Examination of

Digital Evidence:A Guide for Law Enforcement. Washington.

- UNESCO. (2004). Carta sobre la preservación del patrimonio digital. Actas de la Conferencia General. Paris.
- UNESCO. (2012). La Memoria del Mundo en la era digital: digitalización y preservación. Vancouver: UNESCO.
- Vacca, J. R. (2005). Computer Forensics: Computer Crime Scene Investigation, Volume 1, . Cengage Learning.
- Van Der Hoeven, J. (2007). Dioscuri: emulator for digital preservation. D-Lib Magazine 13 (11/12). doi:DOI:10.1045
- Van der Hoeven, J. L. (2007). Emulation for digital preservation in practice: The results. The International Journal of Digital Curation, 2(2), 123-132. Obtenido de https://www.kb.nl/hrd/dd/dd_projecten/Emulation_research_KB_NA_2005.pdf
- Van der Hoeven, J., & van Wijngaarden, H. (2005). Modular emulation as a long-term preservation strategy for digital objects. 5th International Web Archiving Workshop (IWA05). Viena, Austria. Obtenido de <http://iwaw.europarchive.org/05/papers/iwaw05-hoeven.pdf>
- Van der Merwe, A. a. (2009). Planning an effective digital preservation from a research organization. Obtenido de <http://www.ais.up.ac.za/digi/docs/avdmerwe-paper.pdf>
- Walker, C. A., & McCurdy, M. R. (2002). The dangers of destroying documents in the normal course of business. Australian Digital Forensics Conference . Australia.

- Westlaw . (2006). American Law Reports.
- Wilson, A. J. (2004). Digital Preservation and Academic Library Consortia: A Case Study of the Triangle Research Libraries Network Consortial Licenses. Chapel Hill, North Carolina.
- Woods, K. B. (2008). Creating Virtual CD-Rom Collections. En T. B. Board (Ed.), The Fifth International Conference on Preservation of Digital Objects (págs. 62-69). London: iPRES 2008. Obtenido de <http://www.bl.uk/ipres2008/ipres2008-proceedings.pdf>
- Woodyard, D. (2002). The OAIS experience at the British Library. ERPANET OAIS Training Seminar. Recuperado el 18 de agosto de 2015, de Erpanet: <http://www.erpanet.org>>
- Xuejia Lai, D. G. (2010). Forensics in Telecommunications, Information and Multimedia: Third International ICST . E-Forensics 2010. Shanghai, China: Springer.
- Zabolitzky, J. (2002). Preserving software: Why and how. Iterations: An Interdisciplinary Journal of Software History, 1(13), 1-8.
- Zierau, E. K., & Kulovits, H. (2010). Evaluation of Bit Preservation Strategies. The Seventh International Conference on Preservation of Digital Objects. iPRES 2010. Recuperado el 18 de Agosto de 2015, de <http://www.ifs.tuwien.ac.at/dp/ipres2010/papers/zierau-31.pdf>

ISBN: 978-9942-823-46-5



9 789942 823465