



ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

“ELABORACIÓN Y EVALUACIÓN DE UN MODELO QUE MEJORE LA PRESERVACIÓN A LARGO PLAZO DE DOCUMENTOS DIGITALES EN INSTITUTOS DE EDUCACION SUPERIOR”

VERONICA JUDITH PAUCAR LEÓN

Trabajo de Titulación modalidad: Proyectos de Investigación y Desarrollo, presentado ante el Instituto de Posgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de:

MAGÍSTER EN SEGURIDAD TELEMÁTICA

RIOBAMBA - ECUADOR

Agosto - 2021

©2021, Verónica Judith Paucar León

Se autoriza la reproducción total o parcial, con fines académicos, por cualquier medio o procedimiento, incluyendo la cita bibliográfica del documento, siempre y cuando se reconozca el Derecho de Autor.



ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

CERTIFICACIÓN:

EL TRIBUNAL DEL TRABAJO DE TITULACIÓN CERTIFICA QUE:

El **Trabajo de Titulación Modalidad Proyectos de Investigación y Desarrollo**, denominado: “Elaboración y Evaluación de un modelo que mejore la preservación a largo plazo de documentos digitales en Institutos de Educación Superior”, de responsabilidad de la señorita Verónica Judith Paucar León, ha sido minuciosamente revisado y se autoriza su presentación.

Tribunal:

Ing. Luis Hidalgo Almeida; Ph.D.

PRESIDENTE DEL TRIBUNAL

Ing. Fernando Tiverio Molina Granja, Ph.D.

DIRECTOR

Ing. Oswaldo Geovanny Martínez Guashima, M.Sc.

MIEMBRO DEL TRIBUNAL

Ing. Juan Carlos Díaz Ordoñez. Mag.

MIEMBRO DEL TRIBUNAL

Firmado digitalmente por LUIS EDUARDO HIDALGO ALMEIDA
Nombre de reconocimiento (DN): c=EC, o=BANCO CENTRAL DEL ECUADOR, ou=ENTIDAD DE CERTIFICACION DE INFORMACION-ECIBCE, l=QUITO, serialNumber=0000445780, cn=LUIS EDUARDO HIDALGO ALMEIDA
Fecha: 2021.08.25 15:56:28 -05'00'

LUIS EDUARDO
HIDALGO
ALMEIDA

FIRMA



Firmado digitalmente por:
**FERNANDO
TIVERIO MOLINA
GRANJA**

FIRMA

Firmado digitalmente por OSWALDO GEOVANNY MARTINEZ GUASHIMA
Nombre de reconocimiento (DN): c=EC, o=BANCO CENTRAL DEL ECUADOR, ou=ENTIDAD DE CERTIFICACION DE INFORMACION-ECIBCE, l=QUITO, serialNumber=0000445780, cn=OSWALDO GEOVANNY MARTINEZ GUASHIMA
Fecha: 2021.08.25 15:56:28 -05'00'

OSWALDO
GEOVANNY
MARTINEZ
GUASHIMA

FIRMA




Firmado digitalmente por:
**JUAN CARLOS
DIAZ ORDONEZ**

FIRMA

Riobamba, agosto 2021

DERECHOS INTELECTUALES

Yo, Verónica Judith Paucar León, declaro que soy responsable de las ideas, doctrinas y resultados expuestos en el **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo**, y que el patrimonio intelectual generado por la misma pertenece exclusivamente a la Escuela Superior Politécnica de Chimborazo.



VERÓNICA JUDITH PAUCAR LEÓN

No. Cédula: 060338435-5

DECLARACIÓN DE AUTENTICIDAD

Yo, Verónica Judith Paucar León, declaro que el presente **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo**, es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otras fuentes están debidamente citados y referenciados.

Como autor, asumo la responsabilidad legal y académica de los contenidos de este Trabajo de Titulación de Maestría.

Riobamba, agosto 2021



VERÓNICA JUDITH PAUCAR LEÓN

No. Cédula: 060338435-5

DEDICATORIA

El presente trabajo dedico a Dios, por ser mi guía y amparo en todo momento, por darme la sabiduría, conocimiento y la oportunidad de presentar y culminar este proyecto importante en mi vida.

A mis hijos y esposo por todo el apoyo incondicional brindado durante todo el tiempo, para luchar y no abandonar mis metas.

A mi madre que, con sus lecciones, ejemplos y valores, forjo en mí, una mujer luchadora y perseverante.

A todas las personas especiales que me ayudaron con cariño, entrega para el desarrollo y culminación de mi investigación.

Verónica Paucar

AGRADECIMIENTO

Agradezco a Dios por permitir terminar esta etapa de mi vida, a las personas que, con su apoyo, ánimo y compañía han ayudado en la ejecución del presente trabajo. Un agradecimiento especial al Ing. Fernando Molina Director de tesis que con su aporte de conocimientos y experiencia ha permitido la finalización de este proyecto. A mi familia por su apoyo y sacrificio incondicional, gracias por formar parte de mí vida.

Un reconocimiento sincero a la Escuela Superior Politécnica de Chimborazo por darme la oportunidad de obtener mi especialización y a mis docentes por los conocimientos y experiencia impartidas en las aulas.

Verónica Paucar

TABLA DE CONTENIDO

RESUMEN.....xvii

ABSTRACT..... xviii

CAPÍTULO I

1.	INTRODUCCIÓN	1
1.1.	Problema de Investigación.	1
1.1.1.	<i>Planteamiento del problema</i>	1
1.2.	Formulación del problema	4
1.2.1.	<i>Sistematización del problema</i>	4
1.3.	Justificación de la investigación	4
1.4.	Objetivos de la investigación	7
1.4.1.	<i>Objetivo General</i>	7
1.4.2.	<i>Objetivos Específicos</i>	7
1.5.	Hipótesis	7

CAPÍTULO II

2.	MARCO TEÓRICO	8
2.1.	Antecedentes del problema.....	8
2.2.	Bases teóricas	12
2.2.1.	<i>Origen de la Preservación Digital</i>	12
2.2.2.	<i>Preservación Digital a Largo Plazo de Documentos Digitales</i>	13
2.2.3.	<i>Conceptos Preservación Digital</i>	13
2.2.4.	<i>Tipos de Preservación Digital</i>	14
2.3.	Estrategias de Preservación Digital	14
2.4.	Principios de Preservación a Largo Plazo.....	16
2.5.	Técnicas de Preservación Digital	18
2.6.	Modelos de Preservación Digital.....	27

2.6.1.	<i>Modelo de Referencia OAIS</i>	27
2.6.2.	<i>Modelo PREDECI</i>	29
2.6.3.	<i>Modelo PREMIS</i>	30
2.6.4.	<i>Modelo DAMM</i>	31
2.7.	Principales Características de los Modelos de Preservación Digital	34
2.7.1.	<i>PREMIS (Caplan, 2009)</i>	34
2.7.2.	<i>OAIS (The Consultative Committee for Space Data Systems, 2002)</i>	34
2.7.3.	<i>PREDECI</i>	34
2.7.4.	<i>DAMM (Preservica, 2013)</i>	35
2.8.	Estudio de estructura, estrategias y dimensiones de los modelos de Preservación Digital	35
2.8.1.	<i>Entidades esenciales con las que trabajan los modelos de Preservación Digital</i>	35
2.8.2.	<i>Análisis de las directrices de la Unesco 2003 de los modelos de Preservación Digital</i>	36
2.8.3.	<i>Observación de las estrategias según (Dante, 2012) de modelos de Preservación Digital</i>	40
2.8.4.	<i>Análisis de Dimensiones de la Seguridad de la Información de los modelos de Pre. Digital</i>	41
2.8.5.	<i>Evaluación del estudio de los modelos de preservación digital</i>	42
2.9.	Marco Legal	43
2.9.1.	<i>Secretaría Nacional de la Administración Pública</i>	43
2.9.2.	<i>Ley del Sistema Nacional de Registro de Datos Públicos</i>	43
2.9.3.	<i>Norma de Gestión Documental Para Entidades de Administración Pública</i>	44
2.9.4.	<i>Norma Técnica de Gestión Documental y Archivo</i>	45
2.9.5.	<i>Regla Técnica Nacional para la Organización y Mantenimiento de los Archivos Públicos</i>	48
2.10.	Repositorios Digitales	50
2.10.1.	<i>Conceptos de Repositorios Digitales</i>	50
2.10.2.	<i>Características de Repositorios Digitales</i>	51
2.11.	Auditoría y Certificación de Repositorios de Preservación	52

2.11.1.	<i>Trusted Repositories Audit & Certification (TRAC)</i>	53
2.11.2.	<i>Digital Repository Audit Method Based On Risk Assessment (DRAMBORA)</i>	54
2.11.3.	<i>Catalogue of Criteria for Trusted Digital Repositories (Néstor)</i>	55

CAPÍTULO III

3.	METODOLOGIA DE LA INVESTIGACIÓN	56
3.1.	Tipo de investigación	56
3.2.	Diseño de la Investigación	56
3.3.	Método y Técnicas de Investigación	56
3.3.1.	<i>Métodos</i>	56
3.3.2.	<i>Técnicas</i>	57
3.4.	<i>Enfoque de la investigación</i>	58
3.5.	<i>Alcance de la Investigación</i>	58
3.6.	<i>Fuentes de Información</i>	58
3.7.	<i>Instrumentos de Recolección de datos</i>	59
3.7.1.	Dimensiones del Catálogo Néstor	59
3.7.2.	Comparación de Requisitos para obtener entornos digitales	60
3.7.3.	Análisis del Cumplimiento de la Preservación del Repositorio existente del IST JV	61
3.7.4.	<i>Estado de madurez de los procesos de preservación del Instituto Superior Tecnológico</i>	64
3.8.	Elaboración del modelo de preservación digital a largo plazo PDDLPIESTJV	65
3.8.1.	<i>Introducción</i>	65
3.8.2.	<i>Presentación del Instituto Superior Tecnológico Juan de Velasco</i>	66
3.8.3.	<i>Aproximación al entorno de preservación de documentos de la Institución J. V</i>	66
3.8.4.	<i>Presentación de la propuesta del modelo de Preservación Digital</i>	68
3.8.5.	<i>Elaboración del Modelo PDDLPIESTJV</i>	68
3.8.6.	<i>Actores del modelo PDDLPIESTJV</i>	70

3.8.7.	<i>Aporte y simplificación de la Entidad Ingesta</i>	71
3.8.8.	<i>Aporte y simplificación de la Entidad Funcional Almacenamiento</i>	73
3.8.9.	<i>Simplificación de la Entidad Gestión de Datos</i>	75
3.8.10.	<i>Simplificación de la Entidad Administración</i>	77
3.8.11.	<i>Entidad Funcional Planificación de la Preservación</i>	79
3.8.12.	<i>Entidad Funcional Acceso</i>	81
3.9.	<i>Procedimientos Generales</i>	84
3.10.	<i>Hipótesis</i>	85
3.10.1.	<i>Identificación de Variables</i>	85
3.10.2.	<i>Operacionalización Conceptual de Variables</i>	85
3.10.3.	<i>Operacionalización Metodológica de Variables</i>	86

CAPÍTULO IV

4.	RESULTADOS Y DISCUSIÓN	87
4.1.	<i>Presentación de Resultados</i>	87
4.2.	<i>Procesamiento y Análisis</i>	87
4.3.	<i>Valoración de la Variable Independiente</i>	88
4.3.1.	Variable Independiente: Modelo de preservación digital a largo plazo	88
4.3.2.	Indicador: Nivel de cumplimiento del Modelo elaborado de Preservación Digital a Largo Plazo como un modelo confiable	88
4.4.	<i>Valoración de la Variable Dependiente</i>	93
4.4.1.	<i>Variable Dependiente: Mejorar Preservación de Documentos Digitales a Largo Plazo</i>	93
4.4.2.	<i>Indicador: Evaluación de repositorios seguros propuesta por Néstor para expertos para repositorios seguros</i>	93
4.4.3.	<i>Metodología del Indicador de la variable Dependiente</i>	93
4.5.	<i>Comprobación Estadística de la Hipótesis</i>	94
4.5.1.	<i>Estadística descriptiva</i>	95
4.5.2.	<i>Estadística Inferencial</i>	99

4.6. Interpretación y Análisis.....	103
CONCLUSIONES.....	104
RECOMENDACIONES.....	105
BIBLIOGRAFÍA	
ANEXOS	

ÍNDICE DE TABLAS

Tabla 1-2. Metadatos de Preservación.....	21
Tabla 2-2. Prácticas de Preservación Digital de Documentos a Largo Plazo	23
Tabla 3-2. Formatos de Firma PAdES para Documentos en PDF	25
Tabla 4-2. Formatos de Firmas XAdES para Documentos XML	25
Tabla 5-2: Formatos de Firmas Documentos con sintaxis de mensajes criptográficos.	26
Tabla 6-2. Entidades de los Modelos de Preservación Digital.	35
Tabla 7-2. Cumplimiento de Técnicas de Preservación Digital según UNESCO	39
Tabla 8-2. Técnicas de Preservación Digital según Dante Ortiz de los modelos	40
Tabla 9-2. Dimensiones de Seguridad de la Información de los Modelos de Preservación Digital.....	41
Tabla 10-2. Porcentaje de cumplimiento de efectividad de los modelos	42
Tabla 1-3. Promedio y comparación de cumplimiento de los esquemas.....	60
Tabla 2-3. Lista de cumplimiento de criterios para un repositorio de confianza según Néstor. .	61
Tabla 3-3. Operacionalización de variables.....	85
Tabla 4-3. Operacionalización de variables.....	86
Tabla 1-4. Lista de cumplimiento de criterios para un repositorio de confianza según Néstor.	88
Tabla 2-4. Porcentaje de Cumplimiento Modelo PDDLPIESTJV.....	92
Tabla 3-4. Resumen de casos	95
Tabla 4-4. Estadísticas descriptivas.....	95
Tabla 5-4. Análisis ANOVA.....	99

ÍNDICE DE FIGURAS

Figura 1-2. Principios de la preservación digital a largo plazo	16
Figura 2-2. De documento a documento de archivo	18
Figura 3-2. Versiones como documentos de archivo.....	19
Figura 4-2. Reducción en el uso de formatos propietarios	19
Figura 5-2. Relación del trámite con el archivamiento	20
Figura 6-2. Relación del trámite con el archivamiento	21
Figura 7-2. Mantenimiento al acceso de documentos digitales	26
Figura 8-2. Entidades Funcionales de OAIS	28
Figura 9-2. Entidades Funcionales de PREDECI	30
Figura 10-2. PREMIS como un subconjunto de todos los metadatos de preservación	31
Figura 11-2. DAMM como un subconjunto de todos los metadatos de preservación	32
Figura 1-3. Cuadro estado de madurez de una organización según COBIT	65
Figura 2-3. Generador de AIP y validación de usuarios	72
Figura 3-3. Entidad Funcional Ingesta	73
Figura 4-3. Entidad Funcional Almacenamiento	75
Figura 5-3. Entidad Funcional Gestión de Datos.....	76
Figura 6-3. Entidad Funcional Administración	78
Figura 7-3. Entidad Funcional Plan de Preservación.....	80
Figura 8-3. Entidad Funcional Acceso	82
Figura 9-3. Entidades Funcionales PDDL-IESTJV	83
Figura 1-4: Tabla Area bajo la Curva de una Distribución F	102

ÍNDICE DE GRÁFICOS

Gráfico 1-2. Porcentajes de efectividad de los modelos de preservación digital	42
Gráfico 1-3. Porcentajes de heramientas de evaluación de repositorios seguros	60
Gráfico 1-4. Nivel de cumplimiento de Criterios del Modelo PDDLPIESTJV	92
Gráfico 2-4. Comportamiento Importancia Promedio	98
Gráfico 3-4. Boxplot de Importancia según Experto	98

ÍNDICE DE ANEXOS

ANEXO A. Encuesta Inicial Gestión de Documento Digital

ANEXO B. Encuesta Inicial Lineamientos Gestión de Documento Digital

ANEXO C. Encuesta Inicial de Procesos de Preservación del Repositorio

ANEXO D. Encuesta de Validación del Modelo a Expertos

RESUMEN

El presente trabajo investigativo tiene como objetivo la elaboración y evaluación de un modelo de preservación a largo plazo de documentos digitales en institutos de educación superior. Se analizó los modelos de preservación digital: Sistema de información de archivo abierto (OAIS), Modelo de preservación de evidencia digital (PREDECI), Metadatos de Preservación: Estrategias de Implementación (PREMIS), Modelo de madurez de preservación digital (DAMM) con el fin de obtener el mejor esquema, evaluando las estrategias, políticas, técnicas, estándares y entornos con las que fueron creados. OAIS resulta con un grado de efectividad del 92% como base para la creación del nuevo modelo, cumpliendo con principios de integridad, autenticidad, fiabilidad, disponibilidad y funcionalidad de la información, evitando pérdida o destrucción de patrimonio intelectual. Se estudia leyes de preservación digital que sustente la elaboración del modelo propuesto, adoptando mejores prácticas desde el inicio de la creación de los documentos digitales. Se efectuó una estimación del estado actual del repositorio institucional aplicando técnicas y criterios de Néstor para repositorios seguros, consiguiendo la certificación del escenario al que se enfrenta la creación del nuevo modelo. El modelo de Preservación Digital de Documentos a Largo Plazo para el Instituto de Educación Superior Tecnológico Juan de Velasco PDDLPI-ESTJV mejora el aseguramiento del acervo intelectual y científico, gestionando y asegurando el documento digital en cada una de sus entidades, garantizando la preservación digital en el tiempo, finalmente se hace una evaluación del modelo con una encuesta de 107 criterios probatorios propuesta por Néstor para certificar repositorios seguros para expertos concluyendo que el modelo PDDLPI-ESTJV mejora en un 95% la preservación a largo plazo de documentos digitales.

PALABRAS CLAVES: <SISTEMA DE INFORMACIÓN DE ARCHIVO ABIERTO (OAIS)>, <MODELO DE PRESERVACIÓN DE EVIDENCIA DIGITAL (PREDECI)>, <METADATOS DE PRESERVACIÓN: ESTRATEGIAS DE IMPLEMENTACIÓN (PREMIS)>, <MODELO DE MADUREZ DE PRESERVACIÓN DIGITAL (DAMM)>, <CATÁLOGO DE CRITERIOS PARA REPOSITARIOS DIGITALES DE CONFIANZA (NESTOR)>, <INSTITUTO DE EDUCACIÓN SUPERIOR TECNOLÓGICA (IEST)>.

LUIS
ALBERTO
CAMINOS
VARGAS

Firmado digitalmente por LUIS
ALBERTO CAMINOS VARGAS
Nombre de reconocimiento
(DN): c=EC, l=RIORAMBA,
serialNumber=0602766974,
cn=LUIS ALBERTO CAMINOS
VARGAS
Fecha: 2021.08.16 11:00:50
-05'00'



0088-DBRAI-UPT-IPEC-2021

ABSTRACT

The objective of this research work is to develop and evaluate a model for the long-term preservation of digital documents in higher education institutes. The digital preservation models were analyzed: Open File Information System (OAIS), Digital Evidence Preservation Model (AMIS), Preservation Metadata: Implementation Strategies (PREMIS), Digital Preservation Maturity Model (DAMM) in order to obtain the best scheme, evaluating the strategies, policies, techniques, standards and environments with which they were created. OAIS results with a degree of effectiveness of 92% as the basis for the creation of the new model, complying with principles of integrity, authenticity, reliability, availability and functionality of information, avoiding loss or destruction of intellectual property. Digital preservation laws are being studied to support the development of the proposed model, adopting best practices from the beginning of the creation of digital documents. An estimate of the current state of the institutional repository was made by applying Néstor techniques and criteria for secure repositories, obtaining certification of the scenario facing the creation of the new model. The long-term Digital Preservation of Documents model for the Juan de Velasco Institute of Technological Higher Education PDDLPI-IESTJV improves the assurance of the intellectual and scientific acquis, managing and securing the digital document in each of its entities, guaranteeing the digital preservation over time. Finally, an evaluation of the model is carried out with a survey of 107 evidence criteria proposed by Néstor to certify safe repositories for experts, concluding that the PDDLPI-IESTJV model improves the long-term preservation of digital documents by 95%.

KEY WORDS: <OPEN FILE INFORMATION SYSTEM (OAIS)>, <DIGITAL EVIDENCE PRESERVATION MODEL (AMIS)>, <PRESERVATION METADATA: IMPLEMENTATION STRATEGIES (PREMIS)>, <DIGITAL PRESERVATION MATURITY MODEL (DAMM)>, <CRITERIA CATALOG FOR TRUSTED DIGITAL REPOSITORIES (NESTOR)>, <TECNOLOGIC HIGHER EDUCATION INSTITUTE (IEST)>.

CAPÍTULO I

1. INTRODUCCIÓN

En esta parte se detalla un enfoque general de la problemática, justificación, objetivos e hipótesis de esta investigación. Se incluye la importancia de la preservación digital a largo plazo de los archivos digitales.

1.1. Problema de Investigación.

1.1.1. Planteamiento del problema

El mundo digitalizado en el que se está viviendo debido al impacto de las tecnologías que han revolucionado, la escritura, la impresión, el habla, el sonido, la imagen, el acceso y el uso de los datos. Así la teoría del acceso, el modelo dinámico, la complejidad, la convergencia, la tecnología y representación se reflejan en los cambios de la gestión de los recursos que hoy son representados y recuperados en un ambiente digital informacional, tipos de documentos, normas, tecnologías, objetos y software. (Álvarez-Wong, 2017)

Debido a estas circunstancias, “El patrimonio documental enfrenta severas amenazas: el saqueo y la dispersión, el comercio ilícito, la destrucción, así como la frágil particularidad de su soporte, la obsolescencia del almacenamiento y la falta de financiamiento. Según los antecedentes de creación del Programa, esta situación está provocando que gran parte del patrimonio documental haya desaparecido para siempre y otra parte importante esté en peligro.” (UNESCO, 2003)

La información digital se ha convertido en una parte indispensable de nuestro patrimonio cultural y científico. Los hallazgos científicos, documentos históricos y logros culturales son cada vez más presentados en forma electrónica, y en muchos casos exclusivamente así. Sin embargo, a pesar de los irrefutables beneficios ofrecidos por el contenido digital, hay una serie de desventajas asociadas. Los usuarios deben invertir una gran cantidad de esfuerzo técnico para acceder a dicha

información. Tecnología subyacente que continúa experimentando un desarrollo a un ritmo excepcionalmente rápido y la vertiginosa obsolescencia de tecnologías de acceso combinadas con deterioro físico a veces imperceptible de los medios de almacenamiento representan una grave amenaza para la preservación del contenido de la información, tanto contemporáneamente y a largo plazo.

Thurston menciona los obstáculos enfocándose en los datos e información digital de los gobiernos y administraciones públicas, señala cinco obstáculos o retos en torno a la preservación digital:

- ✓ La preservación digital no es considerada como prioridad de desarrollo, por ello no es prioritario para las naciones, ni cuenta con grandes fuentes de financiamiento.
- ✓ Igualmente, la digitalización y los procesos de automatización, son vistos pensando sólo en el presente y no con enfoque a futuro.
- ✓ Falta de concientización por parte de los planificadores y los interesados sobre los problemas de acceso a futuro, pues creen que la tecnología resolverá todo.
- ✓ Existencia de un vacío en el marco legal e institucional, en muchos países la legislación no es clara, es inadecuada y/o desactualizada, tampoco existen políticas nacionales ni han introducido y/o aplicado normas internacionales.
- ✓ Falta de capacidad práctica para el manejo y preservación de recursos digitales, dado que existen pocos profesionales con experiencia suficiente en la gestión y preservación de estos recursos.
- ✓ Las iniciativas de digitalización son susceptibles a fallar debido a la falta de preparación adecuada y adopción de estándares. (Anne, Thurston, 2012)

A nivel mundial y principalmente en países desarrollados, organizaciones y sectores especializados en la gestión de conocimiento e información han integrado ya desde hace algunas décadas la conciencia operativa y cultura activa sobre la importancia de establecer protocolos, actividades y colaboraciones formales orientadas a la preservación de sus memorias y patrimonio digital. Institutos, gobiernos y organizaciones mundiales como la NASA, UNESCO, Massachusetts Institute of Technology (MIT), Harvard, Library of Congress, IBM, Stanford University, National Library of Australia o Koninklijke Bibliotheek, han desarrollado investigación, sistemas y modelos de trabajo orientados a mantener el acceso permanente y a largo

plazo del patrimonio documental de contenidos nacidos digitalmente y materiales digitalizados.
(Leija Román, 2017)

Ecuador como muchos países no posee políticas, normativas, estrategias específicas que regulen la preservación a largo plazo de la documentación digital, existen leyes como la Ley del Sistema Nacional de Archivo, la Norma de Gestión Documental para Entidades de Administración Pública y estatutos propios de las empresas e instituciones que no posee una normativa específica o un modelo que garantice la Preservación a Largo Plazo de Documentos Digitales. El artículo 4 de la Ley del Sistema de Registro de Datos Públicos, señala: "Las instituciones del sector público y privado y las personas naturales que actualmente o en el futuro administren bases o registros de datos públicos, son responsables de la integridad, protección y control de los registros y bases de datos a su cargo. Dichas instituciones responderán por la veracidad, autenticidad, custodia y debida conservación de los registros. La responsabilidad sobre la veracidad y autenticidad de los datos registrados, es exclusiva de la o el declarante cuando esta o este provee toda la información".
(Asamblea Nacional del Ecuador, 2014)

Para el caso de Instituciones Educativas de Educación Superior las cuales se rigen por el Consejo de Educación Superior en su Título III Tratamiento de la Documentación Capítulo I De La Transferencia de a Documentación, en su Artículo 23 De la Preservación y Salvaguarda de los Documentos estipula en una parte que "La documentación de carácter histórica se digitalizará como medida de preservación, poniendo a disposición en el software especializado la información para estudios e investigación a fin de minimizar la manipulación de los documentos originales, los cuáles serán prestados para consulta solo en casos necesarios para el estudio del documento o para verificar la autenticidad del material, así como los sujetos a estudios paleográficos. De igual forma que lo indicado anteriormente, sobre el tema en las leyes mencionadas el contenido está muy general y abierto a definiciones, sin mecanismos, ni metodologías específicas de cómo tratar la preservación de documentos y datos digitales.

Por esta razón implementar un modelo de preservación a largo plazo de datos digitales que permita mantener, proteger y resguardar de forma anticipada y permanente con gestiones específicas asegurar la continuación y acceso del contenido de documentos digitales a lo largo del tiempo y las tecnologías independientes de su soporte, formato o sistema y que en caso de deterioro o daño por diferentes causas se pueda restaurarlos. Por lo que este trabajo se concentra en el análisis de modelos de preservación digital para garantizar la autenticidad y trazabilidad a largo plazo de los documentos digitales.

1.2. Formulación del problema

¿Es posible mejorar la preservación a largo plazo de documentos digitales de los IST mediante la elaboración y evaluación de un modelo de preservación de documentos digitales previo al análisis de modelos de Seguridad Digital de Datos?

1.2.1. Sistematización del problema

¿En qué consiste y que objetivos persigue la preservación digital en el ámbito de documentos digitales como método emergente a la pérdida de patrimonios culturales e intelectuales a nivel mundial?

¿Cuáles son las acciones, modelos, estrategias o políticas vigentes para la gestión de archivos de documentos digitales, preservación a largo plazo en Ecuador, y para las instituciones de educación superior del país?

¿Qué tipos de modelos cumple con los requisitos y recomendaciones de buenas prácticas en preservación digital a largo plazo y son aplicadas internacionalmente y cuáles son las principales semejanzas, diferencias, beneficios?

¿Cuál es el nivel de preservación digital que existe en la gestión documental de repositorios de instituto tecnológico superior públicos?

¿La elaboración y evaluación de un modelo de preservación digital mejorará las necesidades de almacenamiento seguro y percedero con el fin de mejorar la accesibilidad y trazabilidad a largo plazo de los documentos digitales?

1.3. Justificación de la investigación

“El objetivo de la seguridad de la información es proteger la información de una empresa como el bien máspreciado” (Shameli-Sendi, 2016). La mayoría de las veces la información de una organización es medida imaginariamente, sin tener conciencia del impacto para la empresa en el caso de pérdida, destrucción o de ser vulnerada.

Frankfurt am Main dice, la mayor parte de los documentos creados hoy en día “nacieron” con formato digital, o son convertidos a formato digital mediante alguna transformación tecnológica. Los documentos electrónicos presentan varias diferencias fundamentales con los documentos tradicionales, de ahí que necesiten un tratamiento especial para preservar su integridad como documentos a lo largo del tiempo. Estas características singulares de los documentos electrónicos exigen acciones singulares de preservación. Las organizaciones deben ser conscientes de que las acciones de preservación de documentos electrónicos se inician preferiblemente en el momento de la creación de los documentos. En otras palabras, cuanto antes comience el proceso que da lugar a las actividades de preservación, mayor será la seguridad de que los documentos conservarán los requisitos de fiabilidad, integridad, autenticidad y utilidad. (Nestor, 2006)

Para la humanidad la pérdida de la información digital tendría consecuencias desastrosas, no solo por lo que significa para el que hacer diario de la vida en sociedad, sino también por las consecuencias que provocaría en la continuidad del conocimiento, a la memoria y a la identidad del ser humano, los grupos sociales, los países y las áreas geográficas en que convivimos. (Álvarez-Wong, 2017)

Para Aquino uno de los mayores problemas es que se piensa más en el corto plazo que en el largo plazo, al mismo tiempo, el consumismo imperante en el mercado ha aumentado la obsolescencia de programas y equipos tecnológicos que son necesarios para la visualización de los documentos digitales. En este sentido, uno de los retos más álgidos para el futuro de la preservación de recursos digitales será el contar y tener operativos la cantidad necesaria de software y hardware que hagan posible la lectura de archivos digitales. Cabe resaltar que además de los factores tecnológicos en la preservación digital están implicados una serie de factores legales y documentales. (Aquino, 2016)

Juan Voutssas menciona que “la preservación de documentos de archivo se define como: el conjunto de principios, políticas, reglas y estrategias que rigen la estabilización física y tecnológica, así como la protección del contenido intelectual de documentos de archivo adquiridos, con objeto de lograr en ellos una secuencia de existencia a largo plazo continua, perdurable, estable, duradera, ininterrumpida, inquebrantada, sin un final previsto. Para documentos de archivo digitales se agrega a la definición en el caso de preservación documental digital debe establecerse específicamente cómo esos documentos serán conservados durante y a través de las diferentes generaciones de la tecnología a través del tiempo, con independencia de donde residan, su soporte y de sus formatos. (Voutssas, 2010)

La UNESCO menciona: en la Carta para la preservación del patrimonio digital en el artículo 3 de la misma se reconoce el peligro de pérdida a que están sometidos estos materiales y se afirma: «El patrimonio digital del mundo corre el peligro de perderse para la posteridad. Contribuyen a ello, entre otros factores, la rápida obsolescencia de los equipos y programas informáticos que le dan vida, las incertidumbres existentes en torno a los recursos, la responsabilidad y los métodos para su mantenimiento y conservación y la falta de legislación que ampare estos procesos». (UNESCO, 2003)

La adopción de un modelo de red de preservación digital es una alternativa para las organizaciones que quieren coleccionar, almacenar, preservar y ofrecer acceso a su acervo en copias digitales autorizadas. También es imprescindible la concordancia de esas redes con las normas internacionales ya probadas y que promueven el archivamiento digital de la producción científica a largo plazo. (Arrellano, 2013) Molina y Rodríguez dicen: “Cada modelo de preservación digital funciona de manera diferente; estos modelos se aplican a entornos específicos. Algunos modelos se limitan a ciertos tipos de objetos digitales, algunos se centran en soluciones específicas, mientras que otros describen las interacciones funcionales a un alto nivel y tienden a describir soluciones absolutas” (Molina Fernando y Rodriguez Glen , 2017). Señala M. Termens que: “en lugar de optar por el diseño de un software determinado se optó por la creación de un modelo teórico de carácter general que asegurara la preservación y el acceso a la información” (Termens, 2009).

Por esta razón, en el documento elaborado para la UNESCO por la Biblioteca Nacional de Australia, que contiene directrices generales y técnicas para la preservación del creciente patrimonio digital mundial y el acceso permanente al mismo. Tiene por finalidad servir de manual de referencia sobre el Proyecto de Carta para la Preservación del Patrimonio digital, que se han convertido en el inicio y unificación para que muchos países adpten estrategias y guía para proyectos de preservación de documentos a largo plazo.

La implementación de un Modelo de Preservación Digital a Largo Plazo que mejore el aseguramiento del acervo intelectual que manejan los Institutos Tecnológicos Superiores y que se constituya en una pauta para el qué, cómo y durante cuánto tiempo se resguardaran los documentos digitales, y que permita llegar a cumplir los principios de la preservación digital como la integridad, autenticidad, fiabilidad, funcionalidad de la información, evitando perdida o destrucción de patrimonio intelectual.

1.4. Objetivos de la investigación

1.4.1. Objetivo General

Elaborar y evaluar un modelo que mejore la preservación a largo plazo de documentos digitales en Institutos de Educación Superior

1.4.2. Objetivos Específicos

- Estudiar los modelos de preservación digital documental para asegurar los datos a largo plazo como PREDECI, OAIS, PREMIS, DAMM.
- Analizar las leyes, reglamentos o estatutos vigentes relacionadas con preservación de documentos digitales en Ecuador y a nivel internacional.
- Examinar las necesidades existentes de preservación digital documental del entorno de estudio, para la creación del nuevo modelo.
- Proponer un modelo conceptual de preservación de datos, para la preservación digital de documentos para Institutos Superiores Tecnológicos.
- Evaluar la implementación del modelo propuesto de preservación digital documental

1.5. Hipótesis

La implementación de un Modelo de Preservación de Documentos Digitales mejorará la preservación a largo plazo de documentos digitales.

CAPÍTULO II

2. MARCO TEÓRICO

En este apartado se extrae y resume conceptos y definiciones de diversos autores sobre la preservación digital a largo plazo, así como leyes y reglamentos acerca de preservación y los modelos de estudio OAIS, PREMIS, PREDECI y DAMM.

2.1. Antecedentes del problema

Como referencia para el desarrollo del proyecto se recurre a los estudios y artículos científicos realizados sobre temas afines a la preservación de documentos más relevantes que respaldan la investigación y constituyan métodos de análisis. Entre estos trabajos se tienen los siguientes:

En el artículo científico realizado por (Molina Fernando y Rodriguez Glen , 2017) con el tema “The preservation of digital evidence and its admissibility in the court”, analiza los modelos comunes de preservación digital que existen, los elementos, el grado de cumplimiento de las pautas generales, el uso de técnicas y el cumplimiento de requisitos específicos, así como evaluar la necesidad de una solución al problema.

La conclusión que aportó este estudio fueron:

Las cuestiones ignoradas por los modelos actuales de preservación incluyen el museo de herramientas, terminología, control de calidad de la ingesta, evidencia de entorno de metadatos de ingesta parcial para preservar y garantizar la integridad del original, evaluación de riesgos, almacenamiento distribuido, preservación del tiempo, certificaciones de la estrategia, legalidad de la evidencia, respecto por los derechos fundamentales, la confiabilidad y efectividad de la evidencia, en relación a las reglas de protección de datos y secreto de las comunicaciones, referente a el derecho a la libertad de expresión, confidencialidad, preservación de roles, gestión de roles, control de evidencia física, transmisión, trazabilidad, y continuidad de preservación. Es necesario demostrar que ningún modelo cumple con todos los parámetros, requisitos, principios y estándares mínimos establecidos para preservar la evidencia digital en las instituciones de investigación criminal.

Por otro lado, el artículo científico realizado por (Álvarez-Wong, 2017) con el tema “The digital repositories for conservation. An approach to the digital long-term preservation”, pretende contribuir a la formación de criterios relacionados con la preservación digital a largo plazo, al conocimiento de los repositorios digitales, así como sugerir un conjunto de medidas generales que permita trazar una acertada estrategia para la preservación de la información digital.

Aportando con las siguientes conclusiones:

Un punto crítico para información digital se encuentra la obsolescencia tecnológica, la fragilidad tecnológica, la rápida actualización de las tecnologías, la caducidad de software y formatos, la dependencia tecnológica y la pérdida de funcionalidades.

No hay una solución práctica aplicable universalmente al problema de la obsolescencia tecnológica de los materiales digitales y es poco probable que se encuentre una solución única que ofrezca un medio de acceso económico a todos los materiales, para todos los fines y en todo momento.

El uso intensivo de la nube para almacenar los documentos digitales en Internet aumenta el problema de la preservación digital porque hay que garantizar que se controlen los metadatos de integridad, la cadena de custodia, retención y disposición, transferencia y recuperación, control intelectual, así como la autenticidad, la fiabilidad y confiabilidad de los documentos en línea.

La concientización de la necesidad de establecer políticas de preservación en el medio digital que definan su alcance en correspondencia con los objetivos de las instituciones, establezcan los responsables de aplicarlas para que sean utilizadas como instrumento de gestión en la salvaguarda y garanticen la política de la organización, las responsabilidades asignadas, los calendarios de conservación y de eliminación, y los manuales de procedimientos.

En la tesis de investigación realizada por (De Giusti, M. R., 2014) con el tema “Una metodología de evaluación de repositorios digitales para asegurar la preservación en el tiempo y el acceso al contenido” de la Universidad Nacional de la Plata: propone “una metodología de evaluación para repositorios institucionales se relevaron los modelos que a lo largo del tiempo han servido para representar un repositorio digital”. Donde busca mejorar la calidad de los repositorios, así como la estandarización, ayudar a la interoperabilidad y obtener una mayor visibilidad de las

producciones que una institución educativa guarda en un repositorio, así como asegurar la preservación de los contenidos del repositorio, de modo que siempre sea posible acceder a ellos y que éstos resulten legibles tanto para usuarios humanos como máquina.

De igual manera, este trabajo investigativo aporta con las siguientes conclusiones más relevantes:

Se determinó el cumplimiento del repositorio en relación a los elementos constitutivos del paquete de información del modelo OAIS de la norma ISO 14721, que es el modelo a seguir para demostrar las capacidades del repositorio y sus falencias. Cada una de las partes del modelo abstracto del paquete de información (información de contenido y su representación; información descriptiva de la preservación; información descriptiva) fue contrastada siguiendo el método propuesto en este trabajo.

Se realizó el perfilamiento de todos los objetos del repositorio, determinando su riesgo de preservación en función de los formatos existentes y estipulando así mismo acciones que ya han sido iniciadas para mejorar el estado de los ítems (acciones de conversión, migraciones, presentación de estándares y elección de formatos para exposición y preservación de los ítems).

En relación a la información descriptiva de la preservación, además de trasladar el modelo abstracto de la PDI a la realidad de los metadatos en el repositorio, que dan cuenta de los cinco elementos (integridad, fijeza, procedencia, contexto y derechos), se desarrolló un validador y se establecieron las reglas con las que cotejar el cumplimiento con la PDI.

En el informe realizado por (UNESCO, 2003) con el tema “Directrices para la Preservación del Patrimonio Digital” de la Biblioteca Nacional de Australia para la UNESCO: que contiene directrices generales y técnicas para la preservación del creciente patrimonio digital mundial y el acceso permanente al mismo y tiene por finalidad servir de manual de referencia sobre el Proyecto de Carta para la Preservación del Patrimonio digital.

El aporte del siguiente proyecto es:

Estrategias para preservar los objetos digitales.

- Colaborar con los productores (creadores y distribuidores) para aplicar normas que prolonguen la vida efectiva de los medios de acceso y reduzcan la variedad de problemas desconocidos que deben ser tratados.
- Reconocer que no es realista tratar de preservar todo y que hay que seleccionar el material que debe ser preservado.
- Guardar el material en un lugar seguro.
- Controlar el material utilizando metadatos estructurados y otros documentos que faciliten el acceso y ayuden durante todo el proceso de preservación.
- Proteger la integridad y la identidad de los datos.
- Elegir los medios apropiados para proporcionar acceso pese a los cambios tecnológicos.
- Administrar los programas de preservación para que alcancen sus objetivos de manera económica, oportuna, global, dinámica y responsable.

En el artículo realizado por (Giménez, 2014) con el tema “Criterios ISO para la Preservación Digital de los Documentos de Archivo” de la Universidad Politécnica de Valencia, España: donde tiene como objetivo identificar qué diferencias o semejanzas existen entre la actividad de preservación o conservación de los documentos físicos y digitales, para, por un lado, contextualizar las acciones y los elementos de la preservación digital y, por otro, analizar las principales propuestas que realizan diferentes normas ISO para que las organizaciones implementen un programa de preservación digital que garantice la usabilidad de los documentos a lo largo del tiempo.

Entre las conclusiones con las que aporta este artículo se tiene:

Las normas ISO proponen soluciones y acciones que se deben realizar para garantizar que los documentos digitales se conserven a lo largo del tiempo, en tanto las organizaciones consideren que son esenciales como evidencia de su patrimonio o actividades y deseen garantizar su autenticidad, integridad y usabilidad en todo ese tiempo.

Cualquier organización productora de documentos digitales debe diseñar una estrategia para asegurar su conservación y disponibilidad, en función de afrontar los riesgos de la obsolescencia tecnológica. Es imprescindible que dichos documentos estén organizados, clasificados, descritos e indizados, para poder ser identificados y recuperados de la forma más pertinente en el momento en que se desee. Para asegurar la protección de los documentos electrónicos y su autenticidad, se recomienda que estos no sean dependientes del software que los creó y, además, que sean convertidos al formato .pdf/a, con la incorporación de metadatos. Mediante los metadatos insertados en los documentos digitales se asegura su identificación, por lo cual se debe incorporar información

relacionada con la fecha y hora de creación, su creador, el calendario de conservación, su clasificación y relación con otros documentos, etc. Estos metadatos también se pueden almacenar en un repositorio y deberían poder extraerse de los formatos propietarios mediante el lenguaje de marcas xml.

En cuanto al almacenamiento de los documentos digitales, se debe asegurar un soporte estable contra la obsolescencia tecnológica que, a su vez, permita las migraciones a nuevos soportes, con la completa garantía de que se protege la información, sin pérdidas ni alteraciones del contenido. El proceso de migración debe realizarse con una metodología acorde con unos controles de calidad.

Si se desean enviar documentos electrónicos de un sistema de almacenamiento a otro o en un sistema de gestión documental, la información debe ser encapsulada mediante un paquete de información de archivo, como indica la norma OAIS, cuyos principales componentes son el contenido del documento y sus metadatos, lo que permitirá su preservación a largo plazo.

2.2. Bases teóricas

2.2.1. Origen de la Preservación Digital

Su origen viene del latín Praeservare, donde el prefijo **Prae-** significa antes de o delante de y el verbo **Servare** que significa guardar o salvar. La Real Academia Española define la palabra preservación como: “Proteger, resguardar anticipadamente a una persona, animal o cosa de algún daño o peligro”. Por tanto, la preservación aborda su referencia integral como la actividad de salvaguardar de manera anticipada y presente a algo con mira al futuro. (Antonia Salvador Benítez, Antonio Ángel Ruíz Rodríguez, 2005)

La UNESCO a través de la carta sobre la preservación del patrimonio digital potencia gradualmente esta agenda de desarrollo digital como referente e impulsa las necesidades tanto de acceso, vigilancia, acción y continuidad; como de estrategias, políticas, protección, promoción, funciones y alianzas articuladas desde los distintos gobiernos y naciones para la preservación del patrimonio digital como compromiso internacional de participación. (Publications UNESCO, 2003)

Juan Voutssás menciona que “la preservación digital comprende acciones específicas cuyo fin es asegurar la permanencia y acceso del contenido de documentos digitales a lo largo del tiempo”. (Térmens, 2009).

2.2.2. Preservación Digital a Largo Plazo de Documentos Digitales

La necesidad de conservar documentos digitales de importancia para las diferentes instituciones o empresas con el fin de poder utilizarlos en el futuro actualmente plantea varias soluciones. Frecuentemente para que se mantenga seguro y sin afectaciones se opta por no usar lo que se conserva, solo si fuera necesario para que se mantenga seguro y como nuevo el mayor tiempo posible. Una táctica encontrada es que puede preservar la información digital si constantemente se revisa su estado y se le da el mantenimiento necesario tanto físicamente como internamente, así también se debe tener en cuenta cómo usar lo preservado, con el debido cuidado teniendo siempre presente que alguien más lo usara y por tanto dejarlo como se lo encuentra. También se realiza una copia idéntica de las entidades con la información para usar una y guardar la otra en otro sitio como estrategia. Todo un conjunto de tareas con el fin de implementar programas, estrategias, procesos y procedimientos destinados asegurar la preservación a largo plazo de documentos digitales manteniendo propiedades de autenticidad, integridad, confidencialidad, inalterabilidad, fiabilidad, interpretación, comprensión y disponibilidad a través del tiempo.

La preservación a largo plazo se usa en documentos electrónicos y digitales sin importar el tipo de formato, por lo que es indispensable gestionar métodos de preservación a largo plazo que incluyen tareas para asegurar su conservación, su acceso y disponibilidad. También se preocupa por el sostenimiento del documento original, además examina la innovación de los nuevos soportes físicos donde se almacena y permite tener la legibilidad y autenticidad del documento al momento de accederlo muchos años después según las necesidades de las empresas. (Térmens, 2009)

2.2.3. Conceptos Preservación Digital

- Son los principios, políticas, estrategias y acciones concretas que tienen como fin asegurar la permanencia física y tecnológica de la información, la estabilidad y el acceso a los datos de los documentos digitales y resguardar el contenido intelectual de los mismos por el tiempo que se considere necesario. (SINCHE, 2017)
- Es una parte esencial de la creación y el mantenimiento de la colección digital, cuyo objetivo es ampliar su periodo de vida útil y protegerla de posibles deterioros, pérdida

física y obsolescencia de los soportes. (Antonia Salvador Benítez, Antonio Ángel Ruíz Rodríguez, 2005)

- La preservación es la actividad del aseguramiento y protección de la información, el mantenimiento activo y preventivo, la replicación, y la consciencia de procurar la integridad de las cosas de cara a los usuarios futuros. (Leija Román, 2017)

2.2.4. Tipos de Preservación Digital

- **Preservación de duración larga:** Conjunto de acciones y estándares aplicados a los documentos digitales durante su gestión para garantizar su preservación en el tiempo, independientemente de su medio y forma de registro o almacenamiento. La preservación a largo plazo aplica al documento electrónico de archivo con su medio correspondiente en cualquier etapa de su ciclo vital. (Beagrie, N., & Jones, M., 2008)
- **Preservación de duración media:** Acceso continuo a los materiales digitales aún después de los cambios tecnológicos realizados en un periodo definido de tiempo, pero no indefinidamente. (Beagrie, N., & Jones, M., 2008)
- **Preservación de duración corta:** Acceso a los materiales digitales ya sea por un periodo de tiempo definido o que su uso sea calculado en un periodo de tiempo menor a los cambios tecnológicos. (Beagrie, N., & Jones, M., 2008)

2.3. Estrategias de Preservación Digital

Según (Hong, 2012) identificó siete enfoques diferentes para preservación y sostenibilidad del software:

- **PRESERVACIÓN TÉCNOLOGÍA (Technical Preservation).** - Su acción principal es preservar el software y hardware sin cambiar su estado original. Se debe tener en cuenta:
 - ✓ La evolución tecnológica constata tanto de SW y HW que brindan grandes mejoras.
 - ✓ La preservación y conservación de los equipos tiene un costo elevado que resulta difícil asumir por las empresas, y que por el deterioro físico de los equipos habrá un tiempo que sea imposible su conservación y mantenimiento.
 - ✓ En diversos países se gestiona implementar museos de infraestructura funcional por cada tipo de SW y HW existente.

- **EMULACIÓN (Emulation).** - Esta estrategia se utiliza en centro de datos para emular el escenario original para que el software se mantenga en la misma etapa. Se debe considerar:
 - ✓ No se realiza un seguimiento continuo del tipo de formato ya que el archivo original es el que se utiliza sobre todo en medios digitales ininteligibles.
 - ✓ Es una estrategia costosa al tener que actualizar cada vez que hay nuevos sistemas por lo que no es muy utilizada.
- **MIGRACIÓN (Migración).** – Se basa en actualizar los programas para evitar la obsolescencia permitiendo una mayor funcionalidad, realizando copias periódicas de archivos digitales a soportes estables y seguros. Se utiliza la migración cuando:
 - ✓ Se va a cambiar el soporte físico por seguridad.
 - ✓ Para actualizar servicios de un software a nuevas versiones.
 - ✓ Cuando se desea visualizar archivos en su formato original usando otra herramienta.
 - ✓ Para convertir a formatos más estándares al entorno actual sin afectar la integridad de la información.
- **CULTIVO (Cultivation).** - Conservar los programas activos para modelos de desarrollo actuales y abiertos. Se considera para:
 - ✓ Salvaguardar información que ayudara a generar nueva información, dando la posibilidad al público de acceder a su código.
- **HIBERNACIÓN (Hibernation).** - Preserva el conocimiento de cómo recrear debidamente la funcionalidad del software. Se realiza esta técnica:
 - ✓ Para resguardar el contenido de un archivo, pero también el conocimiento de cómo recrear exactamente la funcionalidad de software a un momento anterior.
- **DESAPROBACIÓN (Deprecation).** - Aislar el software sin salir de la opción de reanimación / recreación, es usado cuando:
 - ✓ No importa la herramienta con la que fue creada la información que se va a preservar.
 - ✓ Con esta técnica se indica si alguna función específica del software no continuará en el futuro.
- **DILACIÓN (Procrastination).** - Es una estrategia en la que se decide no hacer nada, es decir, es cuando la información se va a preservar de forma natural.

También (Antonia Salvador Benítez, Antonio Ángel Ruíz Rodríguez, 2005) menciona otras estrategias de preservación:

- **COPIAS DE SEGURIDAD O DE RESPALDO (Backus).** - Las copias de seguridad o respaldos es la forma más común de preservar la información. Consiste en:
 - ✓ Grabar la información a preservar de un pc en algún tipo de soporte físico con el fin de recuperarla en caso de pérdida.
- **ENCAPSULAMIENTO (Encapsulation).** - Esta estrategia guarda datos sobre la interpretación de archivo o documento para que un sistema futuro pueda descifrar. Este radica en:
 - ✓ Preservar el recurso digital y la información necesaria para interpretarlo y convertirlo.
 - ✓ Utiliza estructuras que se relacionan con todos los componentes de la información a preservar, es decir; el objeto digital, los metadatos, su identificador y descripciones del software.
- **RENOVACIÓN DEL SOPORTE FÍSICO DE ALMACENAMIENTO (Actualizar).** – La actualización o renovación del soporte físico permite salvaguardar la información preservada por mucho más tiempo. Este tipo de preservación permite:
 - ✓ Pasar la información digital a un soporte nuevo o actual evitando el deterioro del soporte físico.
 - ✓ No cambia el formato de archivos al realizar la transferencia de la información digital.
- **MANTENIMIENTO.** - Es una estrategia continua para garantizar el buen estado de los recursos digitales. Esta técnica permite:
 - ✓ Almacenar en medios seguros y confiable los datos.
 - ✓ Que el almacenamiento y el manejo de los archivos sea según las recomendaciones del mercado de tal forma asegurar su expectativa de vida.
 - ✓ Realizar verificaciones y copias de seguridad de forma periódica y sistemática.
- **ARQUEOLOGÍA DIGITAL.** - Son métodos y procedimientos para salvar contenidos dañados de programas o medios antiguos o afectados por cualquier anomalía.

2.4. Principios de Preservación a Largo Plazo



Figura 1-2. Principios de la preservación digital a largo plazo

Fuente: (ESTADO, 2016)

- ***PRINCIPIO DE PRESERVACIÓN DE PLANEACIÓN***

Los objetos digitales se hallan en documentos de textos, bases de datos, imágenes fijas, programas de computador, videos y animaciones, registros sonoros, software, sitios web y más. Para archivar los documentos electrónicos se requieren de una gestión planificada, desde su generación hasta su disposición final garantizando la accesibilidad futura. Estas evidencias documentales deben recopilarse por largos periodos de tiempo, permaneciendo auténticos, íntegros, utilizables y comprensibles para quienes los necesiten. Sin una planeación correcta de la creación de los documentos electrónicos de archivo, no se alcanza Preservación Digital a Largo Plazo.

La Planeación deberá definir cómo se crean los documentos electrónicos de archivo y qué procedimiento debe aplicarse para aquellos que llegan a la Entidad, a través de los canales de recepción formalmente definidos para la interacción con los usuarios. Debe contener un conjunto de variables que deben formar parte del modelo de Preservación Digital a Largo Plazo. Con procesos archivísticos definidos, para identificar y caracterizar los tipos de documentos y los correspondientes expedientes en donde se integran, y aplicar las respectivas estrategias para garantizar su preservación longeva. (ESTADO, 2016)

- ***PRINCIPIO DE IDENTIFICACIÓN***

Existen documentos digitales que no necesitan ser preservados (archivados). El Principio de Identificación se encarga de filtrar las evidencias que indican que un documento electrónico es de archivo y sobre solo éstos la Entidad aplicará reglas técnicas, tecnológicas y procedimentales para su preservación digital. Los documentos objeto de preservación digital, serán los identificados como: Tipos Documentales definidos por los instrumentos archivísticos (TRD), cuya naturaleza sea electrónica en el momento de su archivamiento. El Principio de Identificación requiere un análisis de originalidad previsto jurídicamente por las instituciones, para determinar el formato de archivamiento, en las líneas de lo nacido digital o lo que la Entidad convierta a digital.

- ***PRINCIPIO DE ACCESO***

En Preservación Digital es primordial cumplir con el principio de acceso a los documentos. Para acceder a los documentos electrónicos de archivo hay que representar

el contenido informativo de los documentos, como evidencias auténticas e íntegras, durante el periodo de tiempo que la Entidad necesite. Los tiempos de preservación están estimados en los instrumentos archivísticos; mientras que los documentos electrónicos de archivo a los que se aplican estas retenciones, son los que están definidos en el apartado de Identificación.

2.5. Técnicas de Preservación Digital

Reconocimiento de documentos digitales definitivos: En esta etapa se define legítimamente la originalidad de los documentos digitales definitivos. Así se categorizará en la recepción de documentos cual será documento electrónico de archivo de acuerdo a su información inicial pasando por las fases de validación, revisión y movimiento de pendiendo de su naturaleza hasta formar parte de la evidencia de una actividad institucional. El IST “Juan de Velasco” manejan un 75% de documentos digitales. Esta estrategia debe incluir procesos de DIGITALIZACIÓN CERTIFICADA, para darle a la copia digital de un soporte papel, los atributos de originalidad, reduciendo las demandas de almacenamiento y los procesos de organización técnica para los soportes físicos.



Figura 2-2. De documento a documento de archivo

Fuente: (ESTADO, 2016)

Gestionar versiones de los documentos electrónicos de archivo: Los documentos electrónicos son gestionados en diferentes versiones que a través de la trayectoria han pasado por cambios y modificaciones convirtiendo cada versión en evidencia documental digital que debe ser preservada como parte del desarrollo de un trámite, para contextualizar y comprender los documentos de archivo vigentes en las instituciones.

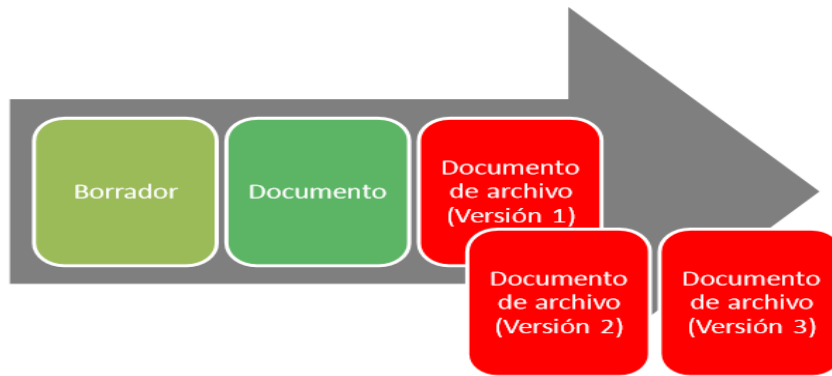


Figura 3-2. Versiones como documentos de archivo

Fuente: (ESTADO, 2016)

Excluir el uso de formatos propietarios: Los documentos de archivo digitales que poseen formatos propietarios de aplicaciones específicas de negocio tendrán que ser transformados a un formato estándar comercial de uso general. Lo establecido en un muestreo documental es la homogeneidad del formato, es decir la extensión más usada es el PDF y PDF/A, en los procesos y actividades de Recepción, Producción y Conversión para los documentos electrónicos de archivo.

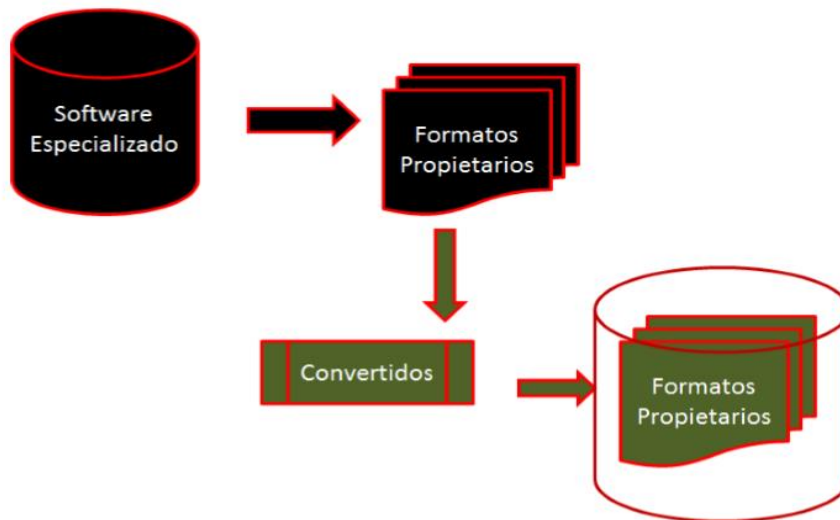


Figura 4-2. Reducción en el uso de formatos propietarios

Fuente: (ESTADO, 2016)

Integrar documentos mediante copias: La preservación a largo plazo de documentos digitales de archivo en su administración debe ser autónoma, logrando esto al existir libertad en el manejo de los objetos digitales al integrar documentos electrónicos de aplicaciones externas al software administrador de las instituciones. Estos documentos deben ser copiados y referenciados físicamente hacia aplicaciones externas a la que no se tenga intervención, en caso de que no exista integración entre el software de gestión documental y aplicaciones de negocio institucionales es aconsejable realizar esta relación lo más breve posible.

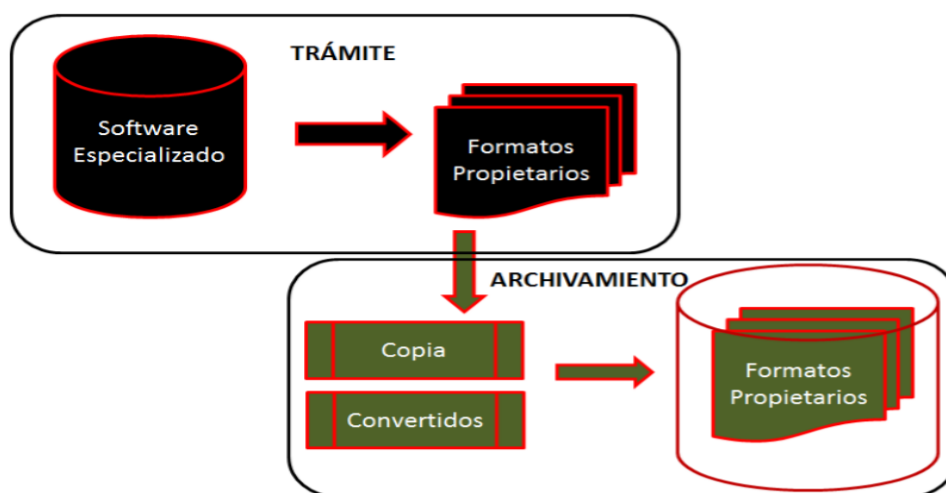


Figura 5-2. Relación del trámite con el archivamiento

Fuente: (ESTADO, 2016)

Respetar el formato original del fichero electrónico recibido: La recepción de documentos digitales es una acción en donde no se tiene la intervención total sobre permanencia y tramitación de los mismo, respetando el formato original garantizando y asegurando los atributos de los documentos electrónicos de archivo. Ejemplo la permanencia de un archivo nacido electrónico en el formato original realizará el circuito de vida en ese formato hasta llegar a la clasificación documental y su respectiva disposición final. En el caso de un documento que se convierte de análogo a digital la originalidad y el valor archivístico reincide en el nuevo documento digital para avalar la repartición, la asignación, el procesamiento y codificación sobre el objeto digital con extensión PDF, JPG o TIFF, según la política de digitalización con que opera en las instituciones.

Normalizar la producción electrónica de documentos: La estrategia dice que los documentos digitales que un Departamento de Gestión Documental genera internamente en una institución debe contar con una política que norme y sistematice la creación, características y atributos de generación que se utilizaran como estándares para la preservación a largo plazo, siendo la producción normalizada del 100% de los documentos, en formato PDF.



Figura 6-2. Relación del trámite con el archivamiento

Fuente: (ESTADO, 2016)

Utilizar metadatos de preservación: Los metadatos facilitan la identificación y descripción de los documentos permitiendo ubicar los datos necesarios para el proceso o registro (manual o automático) de los mismos, en esquemas de almacenamiento de información que sirvan para la preservación de documentos electrónicos de archivo a largo plazo, además se debe tener en cuenta metadatos específicos de técnicas de archivo utilizadas por la institución siguiendo las operaciones de admisión, producción y gestión documental institucional como a continuación se detalla en la tabla 1-2.

Tabla 1-2. Metadatos de Preservación

METADATO	FUNCIÓN
Código	Designación del objeto digital a preservar
Título	Nombre del documento digital
Formato	Identificar el formato de creación del documento electrónico
Software de Creación	Nombre de la aplicación informática utilizada para crear el documento digital
Versión	Versión del software con que fue creado el documento
Tipo de Recurso	Identificación de la categoría de fichero informático a la que pertenece el documento electrónico (Texto, Imagen, Audio, Video).

Estampa de Tiempo	Registro de fecha y hora de acciones sobre el documento digital (creación/captura, modificación, actualización, acceso, anexos, consulta, etc.)
Autor	Emisor responsable del contenido/creación del documento digital
Estado	Metadato de identificación del estado del documento digital: Borrador, Documento o Record
Perfil Autorizado	Metadatos de control de acceso al documento digital
Ubicación de Archivo	Ruta física y/o lógica del repositorio en donde se realiza el almacenamiento del documento digital
Nivel de preservación	Información del tipo de preservación que ha de aplicarse sobre el objeto digital (migración, conversión, emulación, etc.)
Tiempos de aplicación del nivel de preservación	Especificación de fechas para ejecución de migración o conversión de documentos electrónicos de archivo.
Copiado de Respaldo	Asignación de períodos de tiempo para realizar copias de seguridad convencionales, de acuerdo con la política.
Auditoría	Elemento de información para el registro de accesiones sobre el objeto digital, materia de preservación a largo plazo.
Retención	Espacios de tiempo calculados para garantizar sobre los objetos digitales, el tiempo de preservación.
Derechos de Propiedad	Información sobre los derechos de propiedad intelectual relativos al objeto digital que se preserva.
Autenticidad	Definición de elementos de datos para validar autenticidad.
Integridad	Definición de elementos de datos para validar integridad.

Fuente: (ESTADO, 2016)

Realizado por: Verónica Paucar, 2020

Convertir los documentos electrónicos de archivo a formatos perdurables: Esta estrategia se aplica de forma específica para la primera dimensión de las entidades archivísticas, para los tipos de documentos que integran los expedientes. Cuando archivísticamente se cierra el expediente, el departamento encargado realizará una conversión de formato de todos los tipos de documentos integrantes, con una descripción que logre la preservación a largo plazo de documentos digitales de archivo. Las instituciones para la digitalización de documentos de papel a electrónicos

convierten ficheros PDF/A, no todos los formatos de documentos electrónicos pueden ser convertidos a estándares de preservación por lo que en la tabla 2-2 propone ciertas prácticas para la formulación de planes de preservación digital:

Tabla 2-2. Prácticas de Preservación Digital de Documentos a Largo Plazo

Categoría de Contenido	Especificación	Técnicas de Preservación
Documentos Textuales	Características Técnicas	Codificación de caracteres en orden de preferencia: UTF-8 UTF-16 US-Ascii ISO 8859-1
	Formatos	Uso de Formato de marcado basado en XML, con esquema DTD incluido o accesible. Hoja de estilo XSD/XSL y codificación explícita de caracteres. Formato de diseño de páginas: - PDF/UA (compatible ISO 14289-1) - PDF/A (compatible ISO 19005) - PDF (alta calidad disponible. Incluye PDF/X)
	Características Especiales	Imágenes de alta resolución Preservar el mayor número de características como contenido multimedia y elementos interactivos.
	Compleitud	Preservar el documento completo. Todos los componentes del documento deben ser preservados, incluyendo archivos externos asociados y fuentes necesarias para la representación.
	Metadatos	Ver séptima estrategia.
	Aseguramiento Tecnológico	Los documentos deben tener detalles técnicos que ayuden a garantizar la gestión para controlar el acceso ya que también debe preservarse.
Imagen Fija	Representación fidedigna	Calidad igual a la copia maestra de la versión publicada Preservación en el mismo formato que la copia maestra
	Características técnicas	Mayor resolución disponible (no extrapolado o redimensionado) Mayor profundidad de bits disponible Perfil de color embebido en la imagen No compresión Eliminación de capas
	Formatos preferidos	<ul style="list-style-type: none"> • TIFF (*.tif) • JPEG2000 (*.jp2) • PNG (*.png) • JPEG/JFIF (*.jpg) • Digital Negative DNG (*.dng) • BMP (*.bmp) • 7) GIF (*.gif)

	Metadatos	Claves de referencia a cada campo de datos e información técnica de producción (por ejemplo. Metadatos EXIF de cámara digital)
	Medidas tecnológicas	Preservar los atributos de documentos digitalizados que controlen el acceso o impidan el uso por usuarios no autorizados
Conjuntos de información y Bases de Datos	Formatos	Uso de formatos binarios no propietarios. Los formatos en orden de preferencia son: <ul style="list-style-type: none"> • Auto descriptivos (JSON, basados en XML con esquemas conocidos) • Orientados a ambientes WEB • Formatos nativos independientes de la plataforma
	Método de suministro/copia	Disco duro; CDROM, medios DVD ROM, etc.
	Metadatos	La preservación debe incluir todos los metadatos aplicables y las especificaciones técnicas. Debe utilizarse un estándar de metadatos, si es posible. Es necesaria la preservación de la propia base de datos y la versión.
	Medidas Tecnológicas	Conservar atributos de documentos digitalizados que controlen el acceso o impidan el uso para usuarios no autorizados.
	Preservación	Preservar el contenido de las bases de datos para evitar daños y conservar su estado.
	Acceso	Publicar mediante interfaz web <ul style="list-style-type: none"> • Búsqueda completa y sencilla • Observación del contenido preservado

Fuente: (ESTADO, 2016)

Realizado por: Verónica Paucar, 2020

Firmar electrónicamente con vigencia solamente para el trámite del documento: La autenticación del documento se puede logra mediante: La firma electrónica que es un conjunto de métodos y caracteres que se transmite contiguo a un documento que certifica cuál es el autor o emisor del mismo y que no ha sido manipulado o modificado en el intervalo de la comunicación. La estrategia plantea el uso único de firma electrónica su utilidad es igual a la vigencia de los documentos, al finalizar el trámite los datos de la firma pueden ser guardados como metadatos de evidencia, aunque no estén actuales las certificaciones y validaciones en el documento electrónico. Las variantes de firma electrónica antiguas son: PAdES, XAdES, CAdES.

- **PAdES (PDF Advanced Electronic Signature):** Son siglas que identifican la firma electrónica avanzada en formato PDF. Los documentos electrónicos de archivo firmados con PAdES pueden conservarse durante largos períodos, validando la firma del documento desde su aplicación, los datos de la firma de formatos PDF se encuentran

directamente en el documento firmado accediendo que el contenido del archivo PDF sea copiado, almacenado y distribuido como un archivo digital simple, existen variedad de perfiles de firma PAdES:

Tabla 3-2. Formatos de Firma PAdES para Documentos en PDF

FIRMA	DESCRIPCION
PAdES-Basic	Perfil básico. Norma ISO 32000-1
Perfil básico. Norma ISO 32000-1	Firma avanzada basada en CAdES con sello de tiempo incluido.
EPES	Firma avanzada BES, con adición de política de firma.
PAdES-LTV	Es el formato de firma PAdES antiguos. Este perfil permite prorrogar por tiempo indefinido la validez de las firmas en formato PDF. Puede ser utilizado para garantizar la validación muchos años después de la validación de la firma, es decir, garantiza la validación a largo plazo.

Fuente: (ESTADO, 2016)

Realizado por: Verónica Paucar, 2020

- XAdES (Firma electrónica avanzada para documentos XML):** es una técnica para intercambiar información sobre firmas entre diferentes sistemas, con base en el estándar XML. XAdES -XML Advanced Electronic Signature pertenece a una familia de formas avanzadas, porque intentan cubrir diversos escenarios que evolucionan en base a las necesidades existentes con enfoques diferentes con soluciones robustas, seguras y fiables.

Tabla 4-2. Formatos de Firmas XAdES para Documentos XML

FIRMA	DESCRIPCION
XAdES-BES	Forma básica que cumple requisitos legales de firma electrónica avanzada
XAdESEPES	Amplia el concepto BES, añadiendo política de firma como por ejemplo información sobre el certificado y su emisor.
XAdES-T	Es una EPES en que se adiciona una firma de autoridad de tiempo (Time Stamp)
XAdES-C	Es una T con información de los certificados y lista de revocación.
XAdES-X	Es una XAdES-C que añade tiempos (fecha y hora) de los certificados y listas de revocación .
XAdES-XL	Incorpora a la XAdES-X los certificados y fuentes de validación de estos.
XAdES-A	Recomendación para archivamiento porque recoge toda la meta información de todas las extensiones anteriores. El escenario ideal para este formato de firma son documentos cuya validez sea muy elevada: hipotecas, escrituras, títulos universitarios, 15, 20 50 años.

Fuente: (ESTADO, 2016)

Realizado por: Verónica Paucar, 2020

- **CAdES (CMS Advanced Electronic Signatures):** son extensiones de datos firmados con sintaxis de mensajes criptográficos (CMS). El formato CADES tiene 6 diferentes perfiles según el nivel de protección ofrecido. Cada formato mejora y optimiza al anterior, de acuerdo con la siguiente tabla:

Tabla 5-2. Formatos de Firmas Documentos con sintaxis de mensajes criptográficos.

FIRMA	DESCRIPCION
CADES	Forma básica.
CADES-T	Incorporación de sellos de tiempo.
CADES-C	Es un CADES-T que incluye referencia de certificados y listas de revocación.
CADES-X	Añade fecha y hora de los certificados.
CADES-X-L	Incorpora certificados y fuentes de validación para garantizar validez fuera de línea. Es una XAdES-C que añade fecha y hora de los certificados y listas de revocación
CADES-A	Meta información asociada. Perfil de preservación longeva de la firma.

Fuente: (ESTADO, 2016)

Realizado por: Verónica Paucar, 2020

Registrar y mantener el acceso a los documentos digitales de archivo: Los documentos digitales de archivo se deben archivar y a su vez estar accesibles por medio de políticas de seguridad. Existe una inseguridad al aplicar esta técnica, cuando la institución no aplica metadatos de preservación; no realiza operaciones de acceso a largo plazo como migración, emulación, refreshing para los documentos electrónicos de archivo; y no describe condiciones planteadas para preservación a largo plazo de objetos digitales de almacenamiento específicas.



Figura 7-2. Mantenimiento al acceso de documentos digitales

Fuente: (ESTADO, 2016)

2.6. Modelos de Preservación Digital

Los programas de preservación pueden empezar como proyectos piloto, aunque, con el tiempo, se requerirán modelos de gestión duraderos. Un buen modelo es aquel que representa con el suficiente detalle (para los fines específicos) un sistema dado y permite inferir resultados, acciones e incluso paradigmas tras su análisis. Entre los modelos más usados están:

2.6.1. Modelo de Referencia OAIS

El modelo de referencia OAIS (Open Archival Information System) ha sido publicado como una recomendación del CCSDS (Consultative Committee for Space Data Systems) y como norma ISO14721:2003. OAIS enfoca su actividad en la preservación a largo plazo de la información en formato digital, como garantía de que será accesible en el futuro. (Dante, 2012)

En el modelo OAIS y su relación con la Representación de la Información, sirve como modelo funcional de un sistema de archivos. No es un modelo de metadatos en sí mismo, pero define distintos tipos de objetos conceptuales, y algunos de ellos se definen específicamente para cumplir con los propósitos de la preservación y el acceso. Cada tipo de objeto de información se construye a partir de un modelo genérico simple, en el cual el objeto de datos puede ser interpretado usando la información de representación asociada. (De Giusti, M. R., 2014)

Si se acepta que el Modelo de Referencia OAIS es, como establece UNESCO en sus directrices ya citadas, "...para todos aquellos que diseñen, utilicen y evalúen aplicaciones reales. Su valor reside en que explica lo que es necesario a un elevado nivel conceptual, independientemente de los medios seleccionados para lograrlo". (UNESCO, 2003)

- **El archivo OAIS**

El modelo OAIS fue planteado para uso en el área científica del espacio, para conservar digitalmente los datos provenientes de las misiones espaciales. Ha sido adoptado por las bibliotecas de países que han participado en su elaboración e implementación como las Bibliotecas: Congreso de Estados Unidos, Británica, Nacional Alemana. OAIS tiene amplia aplicación para la preservación a largo plazo en cualquier contexto incorpora la vigilancia tecnológica, la conservación digital y procesos que demandan los documentos digitales de todo centro de datos que no deben ser sometidos a cambios, transformaciones o pérdidas. El modelo OAIS, es un modelo de conservación de objetivos digitales que implanta 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. Define actores que interactúan con el archivo, así como los flujos de información, los actores con sus roles que intervienen y son:

- **Productor (Producer).** - El productor es el encargado de enviar objetos digitales para su conservación a largo plazo.
- **Gestión (Management).** - El Gestor se encarga de las políticas de conservación, ingesta y acceso dentro de un archivo OAIS.
- **Consumidor (Consumer).** - El consumidor es el encargado de entender y acceder a la información que se va a acceder.

- **Comunidad Designada**

OAIS define a quien va dirigido el archivo a preservar en los objetos digitales. Una de las principales características del modelo OAIS es la definición de a quién va dirigido el archivo que conserva los materiales digitales a largo plazo, es decir, su público objetivo, lo denomina como Comunidad Designada. Este es una comunidad generadora y receptora de información, tal y como se menciona en la definición del modelo OAIS.

- **Las Entidades Funcionales de un Archivo OAIS**

Una vez revisado 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, empezando con 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.

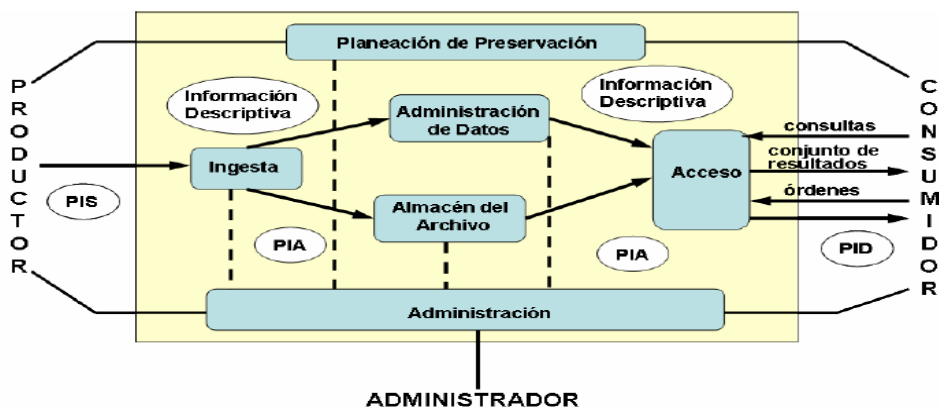


Figura 8-2. Entidades Funcionales de OAIS

Fuente: (The Consultative Committee for Space Data Systems, 2002)

El Modelo OAIS, se desglosa en un conjunto de seis entidades funcionales, que son **Ingestas** (Ingest), **Almacenamiento de Archivos** (Archival Storage), **Gestión de Datos** (Data Management), **Administración** (Administration), **Planificación de la Preservación** (Preservation Planning) y **Acceso** (Access), según como se muestra en la figura 1-2. 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 como 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.

2.6.2. Modelo PREDECI

El modelo PREDECI se basa en el modelo OAIS; Este modelo se divide en un conjunto de seis entidades funcionales, que son Ingesta, Almacenamiento de archivos, Gestión de datos, Administración, Planificación y Acceso a la preservación. Estas entidades funcionales conservan la información de acuerdo con la información definida en el modelo. Este modelo especifica cómo se debe gestionar la información y cómo se transmite la información desde los datos de la entidad funcional de ingesta acceder a la entidad funcional, usa un diccionario de datos basado en PREMIS. Los modelos de preservación digital que utilizan PREMIS como referencia, poseen un enfoque en estrategias para la preservación de metadatos en Archivos Digitales. (Molina Fernando y Rodriguez Glen , 2017)

La Figura 1-2 muestra la arquitectura básica de un SCD, se trata de una topología similar a la de un sistema SCADA. Existen varias unidades de control comunicadas entre sí que realizan las tareas del sistema, de esta forma, en caso de alguna falla dentro del sistema será posible la transmisión de la ejecución de las tareas correspondientes a otro controlador, con esto se logra evitar que una sola falla afecte el proceso completo en una planta. (Molina Fernando y Rodriguez Glen , 2017)

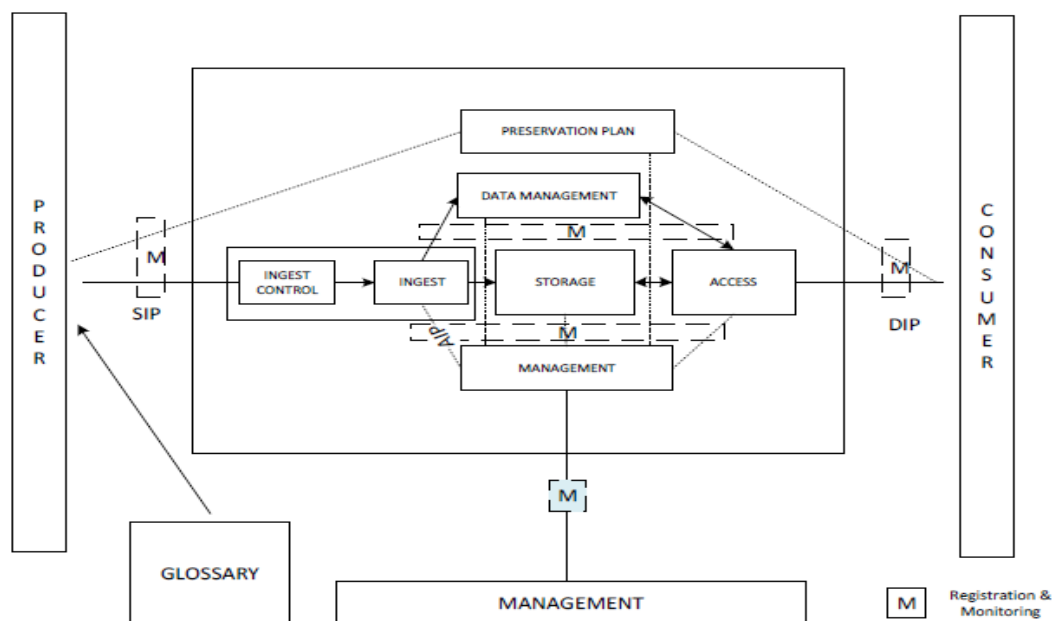


Figura 9-2. Entidades Funcionales de PREDECI

Fuente: (Model For PREDECI,2017)

2.6.3. Modelo PREMIS

PREMIS significa "Metadatos de preservación: Estrategias de implementación", que es el nombre de un grupo de trabajo internacional patrocinado por OCL C y RLG de 2003 a 2005. Ese grupo de trabajo produjo un informe llamado Diccionario de datos de PREMIS para metadatos de preservación que incluye un registro de datos. Este define un conjunto central de unidades semánticas que los repositorios deben conocer para realizar sus funciones de preservación. Generalmente incluirán acciones para garantizar que los objetos digitales puedan leerse desde los medios y que pueden mostrarse, reproducirse o interpretarse de otro modo mediante el software de la aplicación, así como para garantizar que los objetos digitales en el repositorio no se alteren sin darse cuenta, y que los cambios legítimos en los objetos estén documentados. El Diccionario de datos no tiene la intención de definir todos los elementos de metadatos de preservación posibles, solo aquellos que la mayoría de los repositorios necesitarán saber la mayor parte del tiempo.

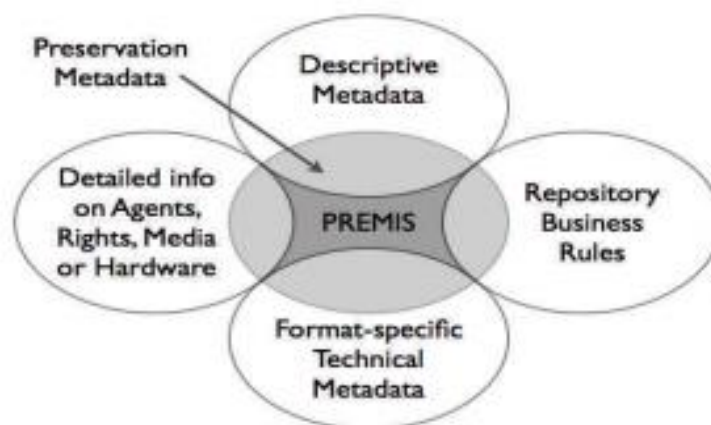


Figura 10-2. PREMIS como un subconjunto de todos los metadatos de preservación

Fuente: <https://www.loc.gov/standards/premis/understanding-premis.pdf>

2.6.4. Modelo DAMM

DAMM (Modelo de madurez de preservación digital) se basa en las características clave de la preservación de la información, como la identificación de formatos de archivo y objetos conceptuales que conforman la información ingerida. El término Modelo de madurez se usa para implicar capas de sofisticación en los procesos, el primero de los cuales debe completarse antes de seguir al siguiente. Este tiene tres secciones principales: (Tessalla, 2013)

- **Almacenamiento duradero:** las capas 1-3 proporcionan niveles crecientes de sofisticación en la seguridad del almacenamiento, cuando se está en un nivel 3 compatible con el sistema puede estar seguro de que su información no se perderá y que no ha sido alterada. (Tessalla, 2013)
- **Gestión de la información:** las capas 4-5 garantizan que los bits sin procesar conservados estén organizados. Tienen una jerarquía descriptiva de metadatos y seguridad, y tienen un conjunto de herramientas poderosas para permitir la carga, administración, búsqueda, navegación y descarga. (Tessalla, 2013)
- **Preservación de la información:** la capa 6 es fundamental para la información que debe conservarse durante más tiempo que la aplicación que la creó. Asegura que los formatos de archivo en los que se mantiene la información sigan siendo relevantes para las aplicaciones disponibles en el momento en que se requiere la información, lo que permite su uso inmediato. (Tessalla, 2013)

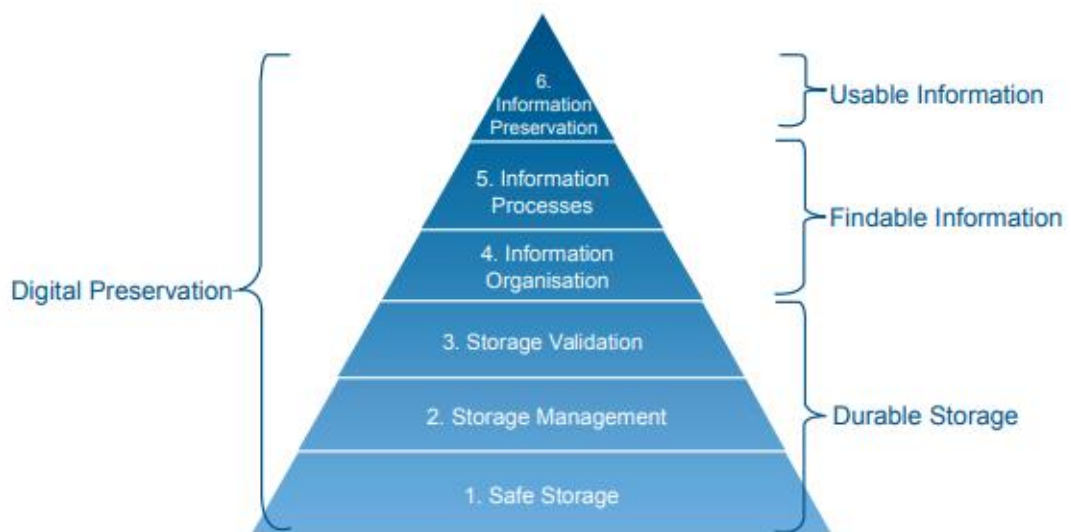


Figura 11-2. DAMM como un subconjunto de todos los metadatos de preservación

Fuente: https://preservica.com/uploads/resources/Preservica-White-Paper-Maturity-Model-2014_NEW.pdf

De acuerdo a las necesidades se debe ubicar el nivel del modelo DAMM, es decir si el almacenamiento es riguroso los niveles 2-3 sería apto. Si hay que custodiar los datos por unos cuantos años se puede acoplar al nivel 4. Si la información a custodiar es grande y no necesita ser tan custodiada encaja en el nivel 5, cuando la información debe ser en contratada para manipularla en el rango de 5-7 años posteriormente de ser creado se coloca en el nivel 6. (Preservica, 2013)

- **Safe Storage (Almacenamiento Seguro).** - El nivel 1 del modelo trata del almacenamiento seguro de forma simple, su característica, es la firmeza a demostrar amenazas frecuentes como el deterioro físico menor en los bits de almacenamiento magnético u óptico.
- **Storage Management (Gestión de Almacenamiento).** – El nivel 2 de DAMM realiza un almacenamiento activo colocando bits en el lugar apropiado, sus características son:
 - Uso de normas que permitan trasladar objetos a otros sitios de almacenamiento tomando en cuenta los beneficios de costo, perpetuación y utilidad.
 - Respaldo de los objetos en más de dos partes.
 - Normas adaptables de movilidad de la información de acuerdo a la situación.
- **Storage Validation (Validación de Almacenamiento).** – La capa 3 del modelo realiza almacenamiento múltiple de objetos, validando la perpetuación a través del acceso y certificación de bits alterados produciendo la regeneración automática de una copia alterna. Características:
 - Diversidad de almacenamiento geográficamente remoto de forma segura.

- Según el almacenamiento validaciones para cada entidad de información.
 - De acuerdo a los intervalos regulares y cada acceso se evidencia la integridad de la información.
 - Si existen errores en la información gracias a las copias alternas se puede auto-regenerar(corregirse).
- **Information Organization (Organización de la información).** - A este nivel 4 la información se organiza en categorías, por la información de colecciones y registros de los objetos de la información. Las características con las que cumple esta capa son:
 - Marca la información con una descripción, leyenda y argumento (metadatos).
 - Cuenta con instrumentos para incorporar información creada al sistema.
 - Posee seguridad por limita el acceso a la información según su permisibilidad.
 - Posibilita la edición y modificación de jerarquías, metadatos y eliminación de implícita de información.
 - Aquí se puede saltar la categoría con el fin de encontrar datos que nos beneficien como metadatos o contexto.
 - Si hay metadatos ligados a registros o a colecciones buscados permite su descarga.
- **Information Processes (Procesos de Información).** - El nivel 5 incrementa técnicas de transacciones eficientes y blandas que ayudan a automatizar acciones de gestión de la información como interfaces de origen y de programadores, difusión de información a los clientes. Sus características son:
 - La sistematización de técnicas de negocios con instrumentos de flujos de trabajo.
 - Posee interfaces para que el programador amplíe el sistema.
 - Permite eliminar contenido y la unificación con los lugares origen.
 - Eliminación a un alto nivel de cosas nocivas para la preservación digital, editando entidades y sus versiones.
- **Information Preservation (Información de Preservación).** – La necesidad de acceder a la información digital almacenada dentro de muchos años al instante se convierte en un desafío para la preservación más cuando el entorno de uso se va transformando, por lo que un sistema de preservación maduro debe poseer las siguientes características:
 - Tipificación de los formatos de archivos y entidades conceptuales
 - Validación mediante la obtención de características de las entidades.
 - Identificación de formatos de archivos en peligro o con necesidades de vigilancia.
 - Valida la migración de pérdida de archivos a un Maestro Digital.
 - Migra con pérdida de formato, pero con transmisión correcta.

- Preservación activa al permitir adicionar nuevas herramientas con fines de preservación.

2.7. Principales Características de los Modelos de Preservación Digital

2.7.1. PREMIS (CAPLAN, 2009)

- Implementación de metadatos en la preservación en Archivos Digitales.
- PREMIS maneja por separado los metadatos, se centraliza únicamente sobre los elementos ligados directamente a la preservación, no existe vínculo con metadatos de acceso, de recuperación de la información, ni con la información sobre derechos.
- Se concentra en el bosquejo de los repositorios tanto en su evaluación como en el intercambio de los paquetes de información guardados entre los repositorios de preservación.

2.7.2. OAIS (THE CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEMS, 2002)

- Modelo de referencia usado para la conservación de archivos digitales a largo plazo.
- Incorpora la vigilancia tecnológica, la conservación digital.
- Posee técnicas necesarias que un centro de datos debe seguir para los documentos digitales no puedan ser alterados, modificados o perdidos.
- Los procesos con los que trabaja son Ingestión, Almacenaje, Gestión de datos, Acceso, Preservación, Servicios comunes.

2.7.3. PREDECI

- Explica cómo se debe administrar la información y cómo se transmite la información a partir de los datos de la entidad funcional de ingestión para acceder a la entidad funcional.
- Incluye la terminología y conceptos para detallar y cotejar arquitecturas, operaciones de sistemas obedeciendo a diferentes estrategias para la preservación a largo plazo.
- Se puede destinar a diferentes archivos digitales con fines de preservación a largo plazo.
- Es responsable de acrecentar la aceptabilidad, disponibilidad, fiabilidad e integridad de documentos digitales a largo plazo.
- Tiene un conjunto de compromisos detallados en las leyes y regulaciones al basarse en OAIS y Nociones de metadatos.

2.7.4. DAMM (PRESERVICA, 2013)

- Implementa capas minuciosas en los procesos, el primero de los cuales debe ser completado antes de pasar a la siguiente.
- Esto es cierto para la Preservación Digital, no tiene sentido tener un sistema de gestión de la información inteligente, si usted no tiene un almacenamiento seguro.
- Identifican los formatos de archivo y objetos conceptuales que componen la información.
- Extrae características de los objetos para la validación del documento futuramente.
- Lleva a cabo la migración de pérdida menor a nuevo documento "Maestro Digital", validando la migración. (Preservica, 2013)

2.8. Estudio de estructura, parámetros, estrategias y dimensiones de los modelos de Preservación Digital

2.8.1. Entidades esenciales con los que trabajan los modelos de Preservación Digital

Tabla 6-2. Entidades de los Modelos de Preservación Digital.

PREMIS	OAIS ISO 14721:2003	PREDECI	DAMM
Entidades intelectuales	Ingesta	Entidad de Ingesta	Nivel 1: Almacenamiento seguro
Objetos	Almacenamiento de Archivos	Función de Almacenamiento	Nivel 2: Administración de almacenamiento
Eventos	Gestión de datos	Función de gestión de datos	Nivel 3: Validación de Almacenamiento
Agentes	Administración	Administración de entidad funcional	Nivel 4: Organización de la Información
Derechos	Planificación de Preservación	Plan de preservación de la entidad	Nivel 5: Procesos de Información
	Acceso	Acceso a funciones.	Nivel 6: Preservación de la Información

Fuente: (Molina Fernando y Rodríguez Glen , 2017)

Realizado por: Verónica Paucar, 2020

Una vez estudiadas las entidades de cada modelo se puede concluir que de los cuatro modelos seleccionados 2 modelos presentan estructuras diferentes y dos semejantes, pero de carácter similar en el tratamiento de preservación de archivo digital.

2.8.2. Análisis de acuerdo a las directrices de la Unesco 2003 de los modelos de Preservación Digital

Las Directrices para la preservación del patrimonio digital se basan en 41 principios que expresan la ciencia de Preservación Digital presentada por la UNESCO en su Carta para la preservación del Patrimonio digital, esto va direccionado a sujetos y empresas que tienen el encargo de programas de preservación digital, según el tipo de usuarios al que se dirige. Estas se concentran en 11 elementos (UNESCO, 2003):

a) Patrimonio:

1. No todos los entes digitales deben ser conservados. El patrimonio digital es solo lo que posee un valor permanente.
2. La prolongación de la existencia y posibilidad de consulta de los objetos dignos de ser conservados es un factor decisivo, pues, si se pierde el acceso a grandes volúmenes de datos, la posibilidad de recuperarlos es ínfima. La continuidad requiere una acción sostenida y directa (denominada preservación digital) y no una especie de “negligencia benigna” pasiva. (UNESCO, 2003)

b) Preservación digital:

1. No existe preservación de objetos digitales si se ha perdido el acceso a ellos, o su autenticidad.
2. La preservación digital debe tomar acciones ante riesgos que amenazan los elementos del objeto digital: material, lógico, conceptual y esencial.

c) Responsabilidad:

1. La preservación digital se logrará si los entes y la gente asumen su responsabilidad y toman acciones o decisiones al respecto.
2. No todos tienen que hacer todo, y no todo tiene que hacerse de inmediato.
3. Aún no existen programas de preservación completos y solventes, pero es necesario actuar poco a poco a no hacer nada para avanzar.
4. Los responsables tienen que estar conscientes de los graves problemas con los que se enfrentara al tomar acciones para alcanzar objetivos sin poner en peligro la preservación.
5. Se debe tomar la responsabilidad seriamente, tomando en cuenta resultados de otros programas de preservación o estudios planteados.

d) Decidir qué conservar:

1. La selección debe ser basada, coherente y responsable.

2. La decisión de conservar un elemento puede ser revisada posteriormente; en cambio, si se decide no preservarlo, la decisión suele ser definitiva. (UNESCO, 2003)

e) Colaborar con los productores:

1. La preservación actualmente debe tomar en cuenta el constante desarrollo de la tecnología digital, características de desarrollo y sus versiones.
2. La mayoría de las veces, los objetos digitales se crean sin propósito de preservarlos a largo plazo.
3. Son actividades de importancia el ayudar a los productores en el momento de implementar normas, conocimientos así la concienciación de la preservación.

f) Derechos:

1. Los programas de preservación deben precisar su derecho legal a reunir, copiar, denominar, modificar, preservar y proporcionar acceso a los objetos digitales de los que son responsables. (UNESCO, 2003)

g) Control:

1. De la transferencia a un lugar seguro de los elementos del patrimonio digital que se va a preservar presumiendo control, protección y gestión.
2. La identificación, descripción de los objetos del patrimonio digital tienen que ser específicos mediante metadatos que permitan encontrarlos, administrarlos y mantenimiento de los recursos.
3. La documentación apropiada de las características de los productos digitales a preservar desde su creación, en vez de hacerlo luego.
4. La interoperabilidad entre programas de preservación se logrará al incorporar técnicas de metadatos normalizados a medida que se implementen.
5. Se debe proteger y preservar los vínculos entre los objetos digitales y sus metadatos.

h) Autenticidad y protección de datos

1. La autenticidad es una cuestión fundamental cuando los objetos digitales se utilizan como pruebas y también puede ser importante para otras clases de patrimonio digital.
2. Debe garantizarse la seguridad del almacenamiento y la gestión de los datos que constituyen los objetos digitales si se desea tener la posibilidad de representar objetos auténticos a los usuarios.
3. La autenticidad es uno de los problemas que los programas de preservación digital deben resolver debido a las constantes transformaciones de los procesos.

4. Con políticas que garanticen la integridad de la información y documentando la identidad de los objetos se logrará una mejor protección de la autenticidad.
5. La protección de los datos se basa en los principios de seguridad y redundancia de los sistemas. En los programas de preservación, la redundancia debe incluir copias de seguridad almacenadas de manera segura, destinadas a conservar los datos a largo plazo, y no un simple ciclo de sobrescrita de nuevos datos sobre los antiguos. (UNESCO, 2003)

i) **Mantenimiento de la accesibilidad** (UNESCO, 2003)

1. El objetivo de mantener la accesibilidad es encontrar métodos económicos de garantizar el acceso cada vez que sea necesario, tanto a corto como a largo plazo.
2. Las normas constituyen la piedra angular de la preservación digital. Sin embargo, muchos programas deben encontrar métodos para preservar el acceso a objetos poco normalizados, en un entorno en el que las normas evolucionan rápidamente.
3. No convendría postergar el proceso de preservación hasta que surja una “norma de preservación digital” única.
4. El acceso a los datos digitales siempre depende de una combinación de equipos y programas informáticos, pero el grado de dependencia de herramientas específicas determina la variedad de las opciones de preservación.
5. Es razonable que los programas opten por estrategias múltiples para preservar el acceso a los datos, especialmente si se trata de colecciones diversas.
6. Las estrategias para preservar la accesibilidad no son autónomas, sino que son respaldadas por otras responsabilidades.
7. Los programas de preservación deben decidir qué niveles de pérdidas son aceptables o no, tanto en lo relativo a elementos y objetos como a necesidades de los usuarios.

j) **Gestión**

8. Abra pérdida de material se espera pacíficamente a que aparezcan soluciones completas y solventes para adoptar medidas responsables
9. Los programas de preservación para una buena gestión, necesitan competencias generales en gestión y conocimientos diversos de la preservación digital para tomar las decisiones correctas cuando sea necesario.
10. La preservación digital integra la evaluación y la gestión de riesgos.
11. Hay que fijar prioridades con el fin de que programas de preservación hagan cara a cantidades de material y problemas que la mayoría de las veces sobrepasan sus capacidades.

12. Los costos de los programas de preservación son difíciles de evaluar porque engloban muchas incertidumbres, como la constante evolución de las técnicas y tecnologías y los plazos de conservación prolongados. Si bien es cierto que los costos por unidad de información son inferiores a los de los objetos no digitales, la cantidad de información en formato digital es tan grande que los costos totales serán probablemente elevados, incluidos los de establecimiento y los recurrentes.
13. Los programas de preservación pueden empezar como proyectos piloto, aunque, con el tiempo, se requerirán modelos de gestión duraderos.
14. El acatamiento de los objetivos de preservación es compromiso de proveedores en ciertas tareas, pero específicamente de los programas de preservación, de sus encargados y los recursos que fijan.

k) Trabajo en equipo

1. El trabajo en grupo es eficaz al elaborar sistemas de preservación por la contribución de conocimientos amplios y ayuda mutua.
2. La cooperación genera costos y medidas, pero a su vez ventajas potenciales.

En la Tabla 7-2, muestra los aspectos de la preservación de las directrices de la UNESCO y evalúa si los modelos de preservación digital analizados cumplen con los mismos, mediante una métrica directa, un método subjetivo y una escala nominal, donde: 3 cumple con la característica, 2 cumple parcialmente, 1 no posee la característica.

Tabla 7-2. Cumplimiento de Técnicas de Preservación Digital según UNESCO

CRITERIOS	PREMIS	OAIS	PREDECI	DAMM
		ISO 14721:2003		
Patrimonio	2	3	2	1
Preservación Digital	2	3	3	3
Responsabilidad	2	3	3	3
Decidir qué conservar	3	3	3	3
Colaborar con los productores	3	1	2	2
Derechos	2	3	2	1
Control	1	3	3	2
Autenticidad y protección de los datos	3	3	3	3
Mantenimiento de la accesibilidad	3	3	3	3
Gestión	3	3	3	3
Trabajo en equipo	2	3	3	2
Porcentaje de Cumplimiento	72%	86%	83%	72%

Fuente: (Molina Fernando y Rodriguez Glen , 2017)

Realizado por: Verónica Paucar, 2020.

De este análisis se observa que la mayoría de los modelos cumplen con las características de la UNESCO 2003, pudiendo deducir que hay diferencias importantes con algunos parámetros ya que cada modelo se crea de acuerdo a ciertas necesidades y entornos, sin que necesariamente fueron creados para cumplir al ciento por ciento con la generalidad de elementos propuestos. De aquí y de acuerdo a la literatura investigada se concluye que el modelo OAIS cumple en un 86% con las características de estudio por lo que es el modelo estándar que se toma como base para la creación del modelo propuesto.

2.8.3. *Observación de las estrategias según (DANTE, 2012) de modelos de Preservación Digital*

En la Tabla 8-2, establece qué estrategias de la preservación según (Dante, 2012) deberían cumplir los modelos de preservación digital analizados, mediante una métrica directa, un método subjetivo y una escala nominal, donde: 3 cumple con la característica, 2 cumple parcialmente, 1 no posee la característica.

Tabla 8-2. Técnicas de Preservación Digital según Dante Ortiz de los modelos

ESTRATEGIAS	PREMIS	OAIS ISO 14721:2003	PREDECI	DAMM
Preservación de la tecnología	1	3	3	1
Migración	3	3	3	3
Emulación	1	2	2	1
Replicación	3	3	3	3
Estandarización	1	3	3	3
Encapsulado	3	3	3	3
Cultivo	2	3	3	2
Hibernación	1	3	2	2
Copias de Seguridad	3	3	3	3
Renovación	3	3	3	2
Arqueología Digital	3	2	2	2
Porcentaje de cumplimiento de técnicas	73%	91%	88%	76%

Realizado por: Verónica Paucar, 2020

Se observa que ningún modelo cumple con la totalidad de las estrategias propuestas por la forma que fueron concebidos desde su creación y contexto y existen puntos que no fueron madurados en su desarrollo, sin embargo 2 modelos poseen mayores características de preservación en su entorno siendo OAIS con un 91% el que librera.

2.8.4. *Análisis de las Dimensiones de la Seguridad de la Información de los modelos de Preservación Digital.*

ISO 17799 define la información como un activo que posee valor para la organización y requiere por tanto de una protección adecuada. El objetivo de la seguridad de la información es proteger adecuadamente este activo para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocio. (Huerta, 2004). Según la norma UNE-ISO/IEC 17799, la seguridad de la información se define como la preservación de:

- a) **Confidencialidad.** - Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.
- b) **Integridad.** - Garantía de la exactitud y completitud de la información y de los métodos de su procesamiento
- c) **Disponibilidad.** - Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados especialmente la información crítica.
- d) **Autenticidad.** - Debe poder verificarse el origen correcto de la información.
- e) **Trazabilidad.** - Permite determinar todas y cada una de las acciones que realiza cada usuario, puede necesitarse conocer quién la ha modificado o accedido.

En la Tabla 9-2, se establece las Dimensiones de la Seguridad de la Información para observar que modelo de preservación digital cumple con estas, mediante una métrica directa, un método subjetivo y una escala nominal, donde: 3 cumple con la característica, 2 cumple parcialmente, 1 no posee la característica.

Tabla 9-2. Dimensiones de Seguridad de la Información de los Modelos de Preservación Digital

DIMENSIONES	PREMIS	OAIS ISO 14721:2003	PREDECI	DAMM
Confidencialidad	3	3	3	3
Integridad	2	3	3	2
Disponibilidad	3	3	3	2
Autenticidad	2	3	3	2
Trazabilidad	1	3	3	3
Promedio de dimensiones de Seguridad	73%	100%	100%	80%

Realizado por: Verónica Paucar, 2020.

De los modelos analizados dos cumplen al 100% con las características de seguridad de la información, en todos sus procesos y gestión de archivos digitales para su preservación poseen características de confiabilidad, autenticidad, integridad, disponibilidad y trazabilidad, por lo que son bases de estudio e implementación en entornos con necesidades similares.

2.8.5. Evaluación del estudio de los modelos de preservación digital.

En la tabla 10-2 se valoran los resultados de los puntos anteriores para determinar qué modelo cumple con un grado de efectividad en cuanto a seguridad de la información y cumplimiento de parámetros de UNESCO y estrategias y técnicas propuestas por Ortiz.

Tabla 10-2. Porcentaje de cumplimiento de efectividad de los modelos

	PREMIS	OAIS	PREDECI	DAMM
Directrices UNESCO	72%	86%	83%	72%
Estrategias y Técnicas de Preservación	73%	91%	88%	76%
Dimensiones de la Seguridad	73%	100%	100%	80%
Promedio de Porcentajes	73%	92%	90%	76%

Realizado por: Verónica Paucar, 2020.

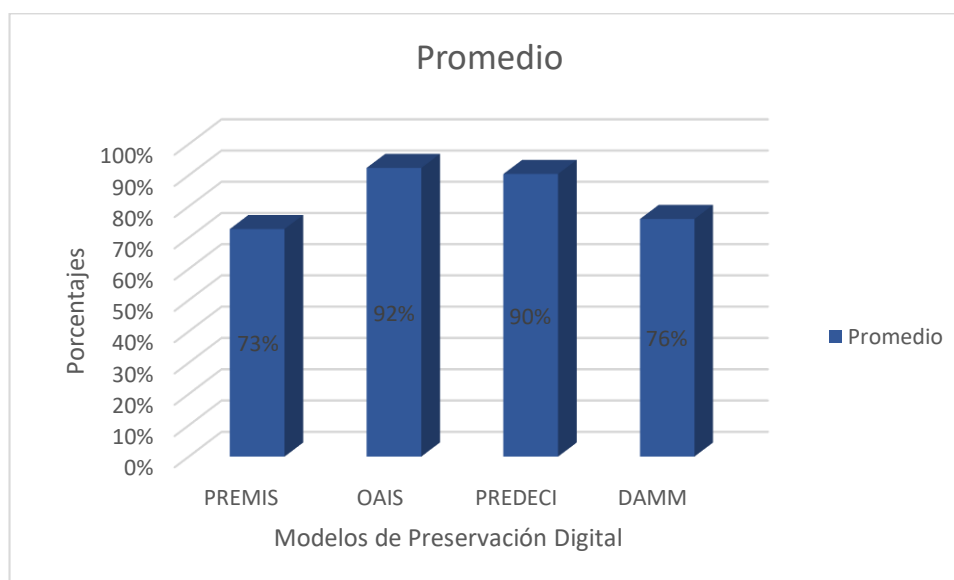


Gráfico 1-2. Porcentajes de efectividad de los modelos de preservación digital

Realizado por: Verónica Paucar, 2020.

Del análisis de los modelos estudiados en la presente investigación como PREMIS, OAIS, PREDECI, DAMM, permite comprobar que OAIS de ISO 14721:2003 cumple con distintas características que aportaran efectivamente en la elaboración del nuevo modelo para mejorar la preservación producción académica de los Institutos Superiores Tecnológicos. De aquí que el modelo OAIS tiene un 92 % de cumplimiento como de muestra en el gráfico 1-2.

2.9. Marco Legal

El marco legal en institutos de educación tecnológica en los últimos años ha tenido varias modificaciones, lo que le ha ocasionado diversas reformas en cuanto a preservación de documentos digitales de producción científica. Se realiza un resumen con algunas leyes, normas específicas que tratan sobre la reglamentación del manejo y preservación de documentos digitales a largo plazo, se realiza un análisis de la Norma de Gestión Documental para Entidades de Administración Pública el Archivo General de la Nación, la Ley del Sistema Nacional de Registro de Datos Público, Norma Técnica de Gestión Documental y Archivo de Ecuador y Regla Técnica Nacional para la Organización y Mantenimiento de los Archivos Públicos.

2.9.1. *Secretaría Nacional de la Administración Pública* (ESPINEL, NORMA TÉCNICA DE GESTIÓN DOCUMENTAL Y ARCHIVO, 2015)

La Secretaria Nacional de la Administración Pública según Acuerdo N°. 1043 menciona:

Que, el artículo 379, numerales 3 y 4, de la Constitución de la República del Ecuador, establece que son parte el patrimonio cultural tangible e intangible relevante para la memoria e identidad de las personas y colectivos, y objeto de salvaguardia del Estado, entre otros: "3. Los documentos, objetos, colecciones, archivos, bibliotecas y museos que tengan valor histórico, artístico, arqueológico, etnográfico o paleontológico. 4. Las creaciones artísticas, científicas y tecnológicas".

2.9.2. *Ley del Sistema Nacional de Registro de Datos Públicos* (ASAMBLEA NACIONAL DEL ECUADOR, 2014)

Se analiza esta ley en lo referente a los siguientes artículos:

Art. 4.- Responsabilidad de la información. - Las instituciones del sector público y privado y las personas naturales que actualmente o en el futuro administren bases o registros de datos

públicos, son responsables de la integridad, protección y control de los registros y bases de datos a su cargo.

Dichas instituciones responderán por la veracidad, autenticidad, custodia y debida conservación de los registros. La responsabilidad sobre la veracidad y autenticidad de los datos registrados, es exclusiva de la o el declarante cuando esta o este provee toda la información.

Las personas afectadas por información falsa o imprecisa, difundida o certificada por registradoras o registradores, tendrán derecho a las indemnizaciones correspondientes, previo el ejercicio de la respectiva acción legal.

La Dirección Nacional de Registro de Datos Públicos establecerá los casos en los que deba rendirse caución.

Art. 25.- Información física y electrónica. - Para efectos de la sistematización e interconexión del registro de datos y sin perjuicio de la obligación de mantener la información en soporte físico como determinan las diferentes normas de registro, los distintos registros deberán transferir la información a formato digitalizado.

La Dirección Nacional de Registro de Datos Públicos definirá el sistema informático para el manejo y administración de registros y bases de datos, el cual regirá en todos los registros del país.

Art. 26.- Seguridad. - Toda base informática de datos debe contar con su respectivo archivo de respaldo, cumplir con los estándares técnicos y plan de contingencia que impidan la caída del sistema, robo de datos, modificación o cualquier otra circunstancia que pueda afectar la información pública.

2.9.3. Norma de Gestión Documental Para Entidades de Administración Pública (ESPINEL, NORMA DE GESTION DOCUMENTAL PARA ENTIDADES DE ADMINISTRACION PUBLICA, 2016)

Según Acuerdo Ministerial 1043 Registro Oficial Suplemento 445 de 25-feb.-2015 con su última modificación: 15-jun.-2016 dice:

Que, el artículo 10 de la Ley Orgánica de Transparencia y Acceso a la Información Pública, establece que: "Es responsabilidad de las entidades públicas, personas jurídicas de derecho público y demás entidades públicas, crear y mantener registros públicos de manera profesional, para que el derecho a la información se pueda ejercer a plenitud, por lo que, en ningún caso se justificará la ausencia de normas técnicas en el manejo y archivo de la información y documentación para impedir u obstaculizar el ejercicio de acceso a la información pública, peor aún su destrucción...";

Que, el Objetivo No. 5 del Plan Nacional para el Buen Vivir 2013-2017, señala la responsabilidad del Estado de garantizar el acceso al patrimonio debe estar orientada hacia el fortalecimiento de redes de investigación, bibliotecas, archivos, museos y sitios patrimoniales a nivel nacional, y que éstos deben operar a través de un subsistema de memoria y patrimonio por medio de instituciones nacionales que garanticen su acceso y circulación. El fin es garantizar la protección, conservación, salvaguarda y difusión de los patrimonios como un bien común.

2.9.4. Norma Técnica de Gestión Documental y Archivo (NORMA TÉCNICA DE GESTIÓN DOCUMENTAL Y ARCHIVO)

Artículo 6. De la política institucional en materia de gestión documental y archivo.

I. Las dependencias emitirán la política institucional en materia de gestión documental y archivo, la que será aprobada por la máxima autoridad institucional y deberá estar alineada con las disposiciones de la presente Norma Técnica y la Metodología que para el efecto emita la SNAP. En ella se establecerá y difundirá el compromiso de organizar, gestionar, conservar y resguardar los documentos de archivo que se generen o reciban, aplicando la metodología de gestión documental y archivo que asegure su autenticidad, fiabilidad, integridad y disponibilidad.

II. Todos los servidores públicos de los sujetos obligados velarán por la integridad y adecuada conservación de los documentos de archivo que genere o reciba la dependencia en cualquier soporte y época, apegándose a los principios generales establecidos en la Declaración Universal sobre los Archivos y el Código de Ética Profesional, emitidos por el Consejo Internacional de Archivos de la UNESCO.

III. El archivo deberá ser condensado en la unidad por el servidor responsable; por consiguiente, se prohíbe expresamente la constitución paralela de expedientes para uso personal.

Del Capítulo II del Sistema Institucional de Gestión Documental y Archivo:

Artículo 10. Descripción, integración y funcionamiento del Sistema Institucional. - Es el conjunto de procesos y procedimientos que interactúan desde que se producen los documentos hasta su destino final, y tiene como objetivo asegurar la autenticidad, fiabilidad, integridad y disponibilidad de los documentos de archivo, cualquiera que sea su soporte y época de producción o recepción, mediante los métodos y procedimientos definidos en la presente Norma Técnica, así como en los instructivos que emita la Dirección Nacional de Archivo de la Administración Pública. Cada dependencia contará con un Sistema Institucional que estará compuesto por:

- I. Los Archivos de Gestión o Activo;
- II. La Dirección de Gestión Documental y Archivo o la que haga sus veces;
- III. El Archivo Central; y,
- IV. Las autoridades y el talento humano calificado suficiente.

Del Capítulo III de Los Procesos Relativos a la Gestión Documental y Archivo:

Artículo 18. De los procesos que deberá realizar el Sistema Institucional. -El Sistema Institucional operará de manera articulada e integral llevando a cabo los siguientes procesos:

- I. Registro de entrada y salida de correspondencia y control de la gestión documental;
- II. Identificación de documentos de archivo;
- III. Integración y ordenación de expedientes;
- IV. Clasificación archivística por procesos;
- V. Descripción documental;
- VI. Valoración documental;
- VII. Transferencias documentales;
- VIII. Preservación de archivos; y,
- IX. Control de la gestión documental y archivo
- X. La SNAP emitirá la metodología para la aplicación de cada uno de los procesos
- XI. que se ejecutarán en el Sistema Institucional.

Artículo 19. De los instrumentos de consulta y control de la gestión documental y archivo. - Para operar los procesos del Sistema Institucional, cada dependencia contará con los siguientes instrumentos:

- I. El Cuadro;

- II. La Tabla;
- III. Los inventarios documentales:
 - a. General por expediente
 - b. De transferencia
 - c. De baja documental
- IV. La Guía de Archivos

Estos son los instrumentos básicos para la gestión, organización, clasificación, conservación y consulta de los diferentes tipos de archivo, por lo que serán de uso obligatorio para todos los servidores públicos participantes en el Sistema Nacional y en los Sistemas Institucionales correspondientes.

Los instrumentos dictaminados y aprobados se remitirán para su conocimiento, validación y registro a la Dirección Nacional de Archivo de la Administración Pública.

Artículo 27. De la preservación de los archivos. - Las dependencias deberán contar con la infraestructura física adecuada para la preservación de los documentos de archivo conforme a lo que establezcan los estándares internacionales y las políticas que emita la SNAP.

Para la adecuada preservación del acervo documental, todos los archivos de las dependencias deberán contar con:

- a) Plan de prevención de riesgos
- b) Programa regular de inspección y mantenimiento
- c) Plan de contingencia.

En los casos en que llegase a haber documentación siniestrada por causas ajenas o imprevisibles, como son los desastres naturales, deberá procederse conforme a la metodología establecida por la SNAP.

Del Capítulo IV De Los Documentos Electrónicos De Archivo:

Artículo 29. Características. - Los documentos electrónicos de archivo forman parte del Sistema Institucional y del Sistema Nacional. Su identificación como documentos de archivo se basa en la misma metodología técnica que se aplica para los documentos impresos. Es decir, emanan del ejercicio de las funciones y atribuciones de la dependencia, son orgánicos, seriados, únicos y estables. Sus requisitos de calidad, como los documentos en papel son: la autenticidad, fiabilidad,

integridad y disponibilidad. De igual forma, los documentos electrónicos de archivo tienen estructura, contenido y contexto, derivado de las atribuciones que les dan origen.

Artículo 30. Gestión. - La organización y gestión de los documentos electrónicos de archivo se llevará a cabo de conformidad con los procedimientos establecidos en la presente Norma Técnica para los documentos de archivo en otros soportes.

Los tiempos de conservación en los Archivos de Gestión o Activo, Central e Intermedio se contarán a partir del momento en que los documentos sean registrados como asunto concluido en el Sistema Informático Integral de Gestión Documental y Archivo y su destino final se determinará mediante la valoración documental de conformidad con lo establecido en la presente Norma Técnica y en la Tabla.

Al suspender la operación de un sistema informático, se verificará que los documentos electrónicos de archivo que contenga, así como su información, se hayan transferido al Sistema Informático Integral de Gestión Documental y Archivo que al efecto implemente la Secretaría Nacional de la Administración Pública, se deberá programar su transferencia a dicho sistema, de acuerdo a un plan coordinado con la Unidad de Tecnologías de la Información y Comunicación.

Artículo 32. Conservación a largo plazo de los documentos electrónicos de archivo. - Cada dependencia elaborará un plan de acción coordinado entre los archivos, las unidades productoras, y la Unidad de Tecnologías de la Información y Comunicación, teniendo como propósito el cumplimiento de los requisitos de autenticidad, fiabilidad, integridad y disponibilidad.

2.9.5. Regla Técnica Nacional para la Organización y Mantenimiento de los Archivos Públicos (SECRETARIO GENERAL DE LA PRESIDENCIA DE LA REPUBLICA , 2019)

Según ACUERDO No. SGPR-2019- 0107 firmado por José Iván Augusto Briones, Secretario General de la Presidencia de la Republica, en ejercicio de las facultades y atribuciones que confieren el artículo 154, numeral 1 de la Constitución de la República del Ecuador, en concordancia con lo que dispone el artículo 2, numeral 1, literal e) del Decreto Ejecutivo No. 5 de 24 de mayo de 2017. Acuerda: Expedir la Regla Técnica Nacional para la Organización y Mantenimiento de los Archivos Públicos en donde mencionan:

Del Capítulo I:

Artículo 1.- Objeto. - El objeto de la presente Regla Técnica es normar la organización y mantenimiento de los archivos públicos, en cada una de las fases del ciclo vital del documento, a fin de asegurar en el corto, mediano y largo plazo, el cumplimiento de los requisitos de autenticidad, fiabilidad, integridad y disponibilidad de los documentos de archivo.

Artículo 2.- Ámbito de aplicación. - La Regla Técnica Nacional para la Organización y Mantenimiento de los Archivos Públicos, será de uso y aplicación obligatoria en todos los organismos, entidades e instituciones del sector público y privado en los que el Estado tenga participación.

Artículo 5.- Principios generales. - Uno de los principios generales que rigen la función archivística., del cual es de interés:

- Responsabilidad: Los servidores públicos son responsables de la organización, conservación, uso y manejo de los documentos. Los particulares son responsables ante las autoridades por el uso de dichos documentos.

Artículo 7.- Política institucional en materia de gestión documental y archivo. -

1. Las entidades públicas emitirán la política institucional en materia de gestión documental y archivo, la cual será aprobada por la máxima autoridad institucional y deberá estar alineada con las disposiciones de la presente Regla Técnica relacionada con la organización, gestión, conservación y custodia de los documentos de archivo.
2. Todos los servidores públicos de los sujetos obligados velarán por la integridad y adecuada conservación de los documentos de archivo que genere o reciba la dependencia, en cualquier soporte y época, apegándose a los principios generales establecidos en la Declaración Universal sobre los Archivos y el Código de Ética Profesional, emitidos por el Consejo Internacional de Archivos de la UNESCO.
3. Se prohíbe expresamente la constitución paralela de expedientes para uso personal.

Artículo 12.- El Sistema Nacional de Gestión Documental y Archivo. - Es el conjunto de dependencias y procesos de gestión documental y archivo articulados entre sí, que tienen como finalidad coordinar las estrategias necesarias para la correcta operación de los procesos y procedimientos a nivel nacional, así como la preservación del patrimonio documental del Estado.

Del Capítulo III: De La Preservación Documental

Artículo 54.- Preservación de archivos. - Para la adecuada preservación del acervo documental, todos los archivos de las entidades públicas de acuerdo a la capacidad presupuestaria anual asignada deberán contar con las siguientes condiciones:

- a. Adecuación de espacios y dotación de mobiliario.
- b. Limpieza y desinfección de repositorios y documentos.
- c. Almacenamiento.
- d. Monitoreo y control de las condiciones ambientales.
- e. Prevención y gestión de riesgos.

Artículo 57.- Almacenamiento. - Dice; existen soportes documentales especiales o diferentes al papel y en estos casos los rangos de temperatura y humedad relativa variarán: como es el caso del Formato electrónico (disquetes, CD-ROM, casetes de video, etc.) la temperatura debe estar en el rango 18-20 °C con una humedad de 30-40%.

2.10. Repositorios Digitales

La preservación digital día a día avanza a nivel de tecnología y estructura con la aplicación de modelos individualizados de acuerdo a la necesidad de cada empresa. Estos deben contemplar recomendaciones y acciones para iniciar un esquema planificado de preservación. Dentro de las actividades esenciales para asegurar los datos digitales están las formas de respaldo en los repositorios que almacenan materiales digitales. El respaldo o backup digital no completa el uso de técnicas, políticas, estrategias que le den conocimientos suficientes para asegurar la integridad de los objetos digitales a largo plazo por lo se tiene menos posibilidad de duración a nivel digital. Para que un programa de preservación sea a largo plazo se debe considerar anticipadamente el tipo de empresa. (Tessalla, 2013) narra como ejemplo que en el caso específico de instituciones educativas o bibliotecas, estas deberán dotarse de un buen repositorio digital que integre todos los procedimientos anexos para su correcta operación como lo son el almacenamiento ordenado de información digital: archivo digital, repositorio digital, etc.; el respaldo de información: backups físicos, copias redundantes o distribución de copias, etc. y la gestión documental: base de datos, metadatos descriptivos, etc., Evaluación de Repositorios Digitales

2.10.1. Conceptos de Repositorios Digitales

Los repositorios son parte fundamental en las estrategias de diseño y adaptación del modelo OAIS o software de preservación digital, ya que funcionan como entes activos en la colaboración técnica

y organizacional de modelos y planes de trabajo adaptados a la gestión digital sostenible de instituciones. En un sentido práctico y funcional el repositorio digital es un sistema informático integral que almacena objetos digitales completos (documentos, audio, videos, fotografías, bases de datos, etc.) de manera ordenada y accesible. Este puede alojarse vía un servidor web o de un servidor local. Puede ser de acceso abierto o cerrado mediante un software que gestiona la ingesta, clasificación y mantenimiento de objetos digitales. (Leija Román, 2017)

(Leija Román, 2017) Leija menciona, “los repositorios institucionales contienen producción de los miembros de una institución, ya sea una universidad o un centro de investigación. Tienen carácter multidisciplinario, a veces se centran exclusivamente en contenidos científicos (artículos, revistas, tesis, congresos, etc.) pero existen también ejemplos de inclusión de material docente, documentación administrativa, colecciones patrimoniales, etc.”

Repositorios digitales en las universidades e instituciones académicas: Denominados repositorios institucionales, constituyen el espacio digital donde se almacena toda la producción científica que se crea permitiendo aumentar la visibilidad y la difusión de dichos recursos. Un servicio de información científica en ambiente digital e interoperable que está dedicado a la gestión de la producción científica y/o académica de una institución. Se encarga de la agrupación, almacenamiento, organización, preservación, recuperación y sobretodo de la amplia diseminación de la información científica producida en la institución. (Ravelo, 2015)

Un Repositorio es una infraestructura web capaz de brindar un conjunto de servicios a una comunidad, destinados a recopilar, gestionar, difundir y preservar contenidos a través de una colección organizada y accesible que debe estar provista de facilidades que le permiten interoperar con otros repositorios similares. El desarrollo de los servicios en un repositorio no es parejo: gestión y difusión avanzadas, recopilación compleja, preservación: reciente. (Universidad de la Plata)

2.10.2. Características de Repositorios Digitales

Las actividades técnicas sugeridas por diferentes literaturas mencionan varios procedimientos que aseguren el acceso digital a nivel de formatos lógicos en repositorios digitales, es por esto que las soluciones deben ser puntuales en preservación digital a largo plazo a nivel lógico, de bits y de estructura. Las políticas de organización, las reglas de almacenamiento descentralizadas, la vigilancia de integridad y autenticidad digital son los ejes obligatorios para mejorar plenamente la preservación, mantenimiento y acceso a la información digital.

Según (De Giusti, M. R., 2014), las principales características de un Repositorio Institucional son:

- Su naturaleza institucional, entendiendo por institución a una organización educativa y de investigación, cuyo punto de partida fueron las universidades;
- Su carácter científico, acumulativo y perpetuo;
- Su carácter abierto e interoperable con otros sistemas

En la investigación de Hitchcock et al. (2007) y citada por Ferreras (2010), informa que muchos de los repositorios institucionales están más preocupados por el acceso que por la preservación, y solo muy pocos cuentan con políticas de preservación digital a largo plazo, generando retos en la gestión y preservación digital perdurable en el tiempo, en cuanto a cultura preservación digital, políticas, responsabilidades operativas y económicos que son necesarias en cualquier programa de preservación digital. Un modelo definido de Preservación digital es el Coalition (2009), donde propone una serie de acciones necesarias para mejorar las tareas diarias de los repositorios institucionales como:

- a) La preservación del software y hardware original con los que fueron creados los materiales digitales.
- b) Preparar software y hardware para emulación de los entornos anteriores.
- c) Recodificar o refrescar los materiales en nuevos formatos para su interpretación futura y constante.

Las actividades operativas y estructurales de los formatos de documentos digitales según su uso prioritario deben ser definidas y diferenciadas como formatos de consulta y formatos de preservación 2013.

2.11. Auditoría y Certificación de Repositorios de Preservación

Saber que contiene un disco duro o un ordenador de almacenaje digital mediante la observación externa es una tarea imprecisa e imposible. El mundo digital de registros de autenticidad e integridad de objetos digitales se ha planteado una serie de estándares y herramientas que permiten conocer y verificar la manera en la que gestionan la custodia de objetos digitales en repositorios de archivo y sistemas de almacenamiento desde su interior y a detalle. Desde el año 1996 el grupo de investigación Task Force on Archiving of Digital Information creado por la Commission on Preservation and Access and the Research Libraries Group de los Estados Unidos

con el objetivo de investigar sobre el continuo e indefinido acceso a futuro de los documentos electrónicos almacenados en forma digital, afirman sobre la necesidad de crear un sistema que certifique de manera externa a los repositorios o archivos digitales con actividades de migración, almacenaje y provisión de acceso. De esta manera se ayudaría a crear un clima de confianza sobre las perspectivas de preservación a largo plazo de manera íntegra y segura.

La tarea de auditar la veracidad y fiabilidad con la que los sistemas de repositorios gestionan objetos digitales ha llevado a la creación de diversos sistemas de auditoría que certifican a repositorios digitales, los cuales se pueden clasificar en tres niveles que van de la certificación básica, a la certificación extendida y la certificación formal. La certificación básica integra una serie de parámetros y metodología de listas de verificación (checklist) sobre los cuales la propia organización evalúa el estado de integridad y confianza en la que los sistemas de archivo integran y custodian archivos. Algunos ejemplos de modelos para certificación básica se los puede encontrar en la metodología inglesa Digital Repository Audit Method Based on Risk Assessment (DRAMBORA) creada por el Digital Curation.

La certificación extendida y formal hace referencia a auditorías bajo normas ISO y DINI respectivamente que mantienen un nivel de certificación extendida cuando las actividades de monitoreo y auditoría son realizadas por la misma organización, y cuando estas son realizadas por auditores externos se considera una certificación formal. Ejemplo el sistema de certificación Trustworthy Repositories Audit & Certification (TRAC) que mediante una serie de criterios y listas de revisión estructuradas que funcionan como una herramienta de auditoría en áreas de políticas y administración, manejo de objetos digitales y tecnología en la gestión de repositorios digitales. Así mismo esta herramienta sirve para evaluar el grado de fiabilidad, compromiso y disposición de la institución ante la preservación segura a largo plazo. En el mismo nivel esta el sistema de certificación NESTOR 1 y NESTOR 2 este actualizado bajo la norma DINI 31644:2012. El concepto de auditoría para certificación de repositorios digitales hoy en día mantiene una agenda de interés internacional en el área de archivos digitales y bibliotecas.

2.11.1. Trusted Repositories Audit & Certification (TRAC)

TRAC: Trusted Repositories Audit & Certification, es una técnica de auditoría de repositorios digitales que permiten la preservación digital a largo plazo. Publicada en el 2007, muestra un conjunto de buenas prácticas sobre las exigencias que un repositorio digital debe cumplir para que sea fiable en la conservación de documentos digitales. TRAC suministra instrumentos de evaluación y certificación a los repositorios digitales, diseña procesos para la certificación,

determina las exigencias mínimas de documentos para la auditoría, estipula los métodos adecuados para la seguridad y conservabilidad de repositorios que son capaces de guardar, migrar y acceder a colecciones digitales de forma fiable. Tiene la influencia de The Center for Research Libraries (CRL) Auditing and Certification of Digital Archives Project y por el Catálogo of Criteria for Trusted Digital Repositories dado por el grupo de trabajo Néstor Network of Expertise in Long-Term Storage and Digital Resources. (Donaldson, 2020)

Catálogo of Criteria for Trusted Digital Repositories define una lista de comprobación. Se subdivide en 84 indicadores: 16 de Infraestructura de la Organización, 44 de Gestión de Objetos Digitales y 16 de Tecnologías, Infraestructura Técnica y Seguridad y se comprueban y analizan por documentación o evidencia que posee un repositorio obteniendo como resultado la certificación del repositorio.

Dobratz, 2007 menciona que no existe una relación directa entre OAIS y TRAC, aunque este relacionados entre sí. (Bote y Termens, 2011) afirma que para impedir desórdenes TRAC utiliza emplea vocabulario del modelo de referencia Open Archival Information System (OAIS), ISO 14721:2003, en el 2012 TRAC se convirtió en una norma ISO 16363:2012.

2.11.2. Digital Repository Audit Method Based On Risk Assessment (DRAMBORA)

DRAMBORA es una metodología que sirve para apoyar en la administración de repositorios en el análisis de riesgos que la institución, mostrando la probabilidad y el impacto potencial de dichos peligros. Establecida por el Digital Curation Centre (DCC) y Digital Preservation Europe (DPE), así como el sistema holandés Data Seal of Approval y el método español Guía de Evaluación Recolecta, (Bernard, 2007), dice: Evalúa el ciclo de vida de la información permitiendo confrontar información electrónica y crítica de una organización.

DRAMBORA es la consecuencia de un período de auditorías piloto realizadas de repositorios por el DCC en los años 2006 y 2007 son métodos de autoevaluación, alentando a las empresas a tomar conciencia de sus objetivos, misión, tareas y activos antes de definir, valorar y negociar los riesgos existentes en su institución. El tratamiento digital se basa en la gestión del riesgo; el administrador digital

Dentro de DRAMBORA, la curación digital se caracteriza como una actividad de gestión de riesgos; el trabajo del curador digital es optimizar las inseguridades y amenazas que ponen en peligro la autenticidad y la legibilidad de los objetos digitales, convirtiéndose en riesgos

manejables. En una primera etapa el auditor genera un perfil organizacional que describe las reglas relacionando los objetivos, actividades y bienes del repositorio, así los riesgos son identificados de cada uno de los perfiles para ser evaluados en probabilidad e impacto, los auditores de acuerdo al tipo de riesgo emiten respuestas y con la asignación segura de recursos, donde el administrador priorice áreas con mayor dificultad o deficiencias. El proceso en sí es iterativo y, por lo tanto, las recurrencias posteriores evaluarán la eficacia de las implementaciones anteriores de la gestión de riesgos.

2.11.3. Catalogue of Criteria for Trusted Digital Repositories (Néstor)

El grupo de trabajo Working Group Trusted Repositories – Certification elabora Catalogue of Criteria for Trusted Digital Repositories. Néstor, es un proyecto de investigación en preservación y conservación digital. El grupo de trabajo ha creado este catálogo (Néstor, 2008) donde se presentan unos juicios para lograr Repositorios Digitales de Confianza: sustentado en estándares nacionales e internacionales, como DINI (DINI, 2007), el informe RLG-OCLC (RLG, 2002). Este catálogo de criterios identifica y analiza a la organización en requerimientos técnicos seguridad, integridad de la información, marco organizacional, gestión de objetos, emplea la terminología del modelo de referencia OAIS, a pesar de tener un financiamiento alemán posee gran aprobación internacional.

Néstor es un proyecto alemán creado con la misión de asegurar la preservación de los recursos digitales en Alemania y trabajar con otras instituciones a nivel internacional para garantizar el acceso a la memoria digital mundial. Entre sus objetivos concretos está el servir de punto de unión y comunicación a todas las partes que trabajan en Alemania sobre preservación a largo tiempo de los documentos electrónicos. Su catálogo para la creación de repositorios fiables, identifica criterios que facilitan la evaluación de repositorios y se basa en la fiabilidad de los contenidos y del propio repositorio tanto a nivel organizativo como técnico. Su objetivo es asegurar la preservación de los contenidos, almacenados como objetos digitales, a largo plazo. Considera un repositorio como aquella institución que ha asumido la responsabilidad de la preservación y accesibilidad a largo plazo de objetos digitales asegurando que puedan ser utilizados en el futuro por una comunidad de usuarios o grupo específico. Los criterios de evaluación que se plantean se articulan en tres apartados: marco organizativo, gestión de objetos e infraestructura y seguridad.

CAPÍTULO III

3. METODOLOGÍA DE LA INVESTIGACIÓN

En esta sección se describe el tipo de investigación, diseño, métodos, utilizadas para la elaboración del modelo de preservación de documentos digitales a largo plazo para institutos superiores tecnológicos, se determina los escenarios de estudio, las herramientas y procedimientos que se emplearon en este proyecto de tesis.

3.1. Tipo de investigación

Esta tesis se compone de una investigación descriptiva y aplicada, se fundamenta en conocimientos existentes, por procedimientos metodológicos de estudios previos utilizados en la preservación digital de documentos que ayuden a formular pautas de preservación a largo plazo y mejorar la seguridad de los documentos digitales y es cualitativa por que se estudia la calidad de las actividades de preservación del repositorio de la entidad de educación superior tecnológica.

3.2. Diseño de la Investigación

La investigación es del tipo cuasi-experimental ya que se analiza modelos existentes, leyes, normativas, políticas de buenas prácticas que servirán de apoyo para la implementación del modelo descriptivo, se escoge el modelo OAIS como base del modelo de Preservación Digital de Documentos a Largo Plazo. De tipo Cualitativa en los escenarios de recolección de datos, se evalúan con los 14 criterios de Néstor para repositorios seguros a largo plazo para certificar el nuevo modelo, en el primero se analiza el entorno, necesidades y falencias de preservación y en el otro escenario se evalúa la propuesta.

3.3. Método y Técnicas de Investigación

3.3.1. Métodos

Se utiliza el método científico, mediante el mismo en las diferentes fases se revisa información en libros, revistas, artículos científicos e Internet, lo que permite detectar los problemas actuales de preservación digital de documentos a largo plazo y obtener un conocimiento válido desde el punto de vista científico, utilizando herramientas fiables, el procedimiento a seguir es:

- Planteamiento del problema
- Formulación de la hipótesis
- Levantamiento de la información (Registros, Internet, bibliografía científica, investigaciones realizadas a nivel nacional e internacional)
- Elaboración del modelo de Preservación de Documentos a Largo Plazo.
- Análisis e interpretación de resultados
- Comprobación de la hipótesis

Método deductivo una vez analizado los problemas que existen en la Preservación Digital de Documentos y estudiado los modelos de preservación PREMIS, PREDECI, OAIS y DAMM se encuentra un modelo que cubra con las falencias existentes en la preservación en entornos educativos, definiendo OAIS como un modelo base y ajustable para el diseño de un nuevo modelo que mejore la preservación de documentos digitales a largo plazo.

Método analítico porque se evalúa los procesos existentes de documentos digitales en base a los criterios de repositorios seguros de Néstor, mismo que permitirá determinar las necesidades, vulnerabilidades y riesgos que se debe tener en cuenta para la creación del nuevo modelo de preservación de documentos digitales a largo plazo.

3.3.2. *Técnicas*

Se basa en revisión de fuentes de información bibliográficas primarias como pruebas y observación de resultados y secundarias como leyes, artículos científicos, tesis, conferencias, revistas, etc. Las técnicas usadas en el presente trabajo de investigación son:

- **Búsqueda de información:** se obtuvieron datos necesarios de fuentes primarias y secundarias para la selección del modelo base que cumpla con los estándares de preservación a largo plazo modelo OAIS.
- **Evaluación:** se obtienen los escenarios de trabajo, es decir con lo que se cuenta antes de la elaboración del nuevo modelo, con el fin de que se adapte al entorno educativo, y la valoración del modelo creado con Néstor.
- **Observación:** se establecen los resultados de la evaluación realizada antes y después del repositorio.
- **Análisis:** permite determinar los mejores estándares, técnicas y mejores prácticas de preservación a largo plazo de los modelos y establecer los resultados de la investigación.

3.4. Enfoque de la investigación

La investigación presenta un enfoque cuantitativo debido a que responde preguntas de investigación sobre Preservación Digital de Documentos y sus retos actuales, que ayudara a establecer un modelo de preservación a Largo Plazo.

3.5. Alcance de la Investigación

La investigación abarca el entorno del Instituto Tecnológico Superior “Juan de Velasco” que oferta servicios de educación cuya visión es formar profesionales de calidad, con un alto nivel humanístico, académico, técnico y tecnológico que sean competitivos, prácticos y científicos.

La finalidad del análisis de los modelos de preservación digital de documentos es cubrir la necesidad desde la perspectiva funcional, de organización y niveles de estado de prácticas de preservación digital para apoyar la definición de un modelo con elementos funcionales, conceptuales y de buenas prácticas que sirvan de argumentos clave para integrar una propuesta de estrategia de preservación a largo plazo. Cabe reiterar que este análisis pretende definir a nivel conceptual y funcional los conceptos y funciones técnicas generales de los sistemas de preservación digital documentos. El alcance de análisis técnico se limitará a un nivel elemental (no a nivel técnico avanzado de programación y códigos) ya que el interés primordial es que los resultados sirvan de modo pragmático y conceptual para entender los niveles funcionales y operativos de los sistemas de preservación digital documental en sus posibilidades y requerimientos de seguridad de la información y necesidades de buenas prácticas.

3.6. Fuentes de Información

Las fuentes de información que se usaron en este proyecto de investigación son:

Primarias

- Evaluación de preservación digital en base a criterios certificados internacionalmente.
- Análisis de los resultados.

Secundarias

- Artículos Científicos
- Tesis doctorales sobre el tema
- Libros de Preservación

- Reglamentos, leyes, estándares nacionales e internacionales.
- Publicaciones de páginas con contenido seguro que argumenten el desarrollo y evaluación de repositorios.

3.7. Instrumentos de Recolección de datos

La recolección de datos se realiza con el catálogo de criterios para repositorios seguros Néstor con el cumplimiento de parámetros antes de la elaboración de un Modelo de Preservación Digital de Documentos a Largo Plazo se busca información que será útil para su creación y después de la creación, se usa la encuesta de evaluación de Néstor para expertos para validar el modelo propuesto y valorar los indicadores de las variables.

3.7.1. Dimensiones del Catálogo Néstor

Para que un repositorio preserve a largo plazo sus objetos digitales, Néstor incluye criterios firmes que permitan la conservación por ciclos largos. Cada criterio se asigna en secciones de organización marco, objeto de gestión e infraestructura y seguridad, asegurando que el diseño tenga relación con parámetros del modelo de referencia OAIS. Posee conceptos de confiabilidad establecidos internacionalmente y ejemplos de buenas prácticas de reglamentaciones, procesos financieros y recurso humano.

El catálogo de criterios de Néstor para establecer la confiabilidad dice que tiene que aplicar principios. Los principios básicos de aplicación del catálogo de criterios para determinar la confiabilidad son:

- **Adecuación:** Hay que adaptarse a los requerimientos, objetivos y actividades del repositorio para que exista una preservación a largo plazo.
- **Cuantificación:** Los indicadores permitirán medir el nivel de confiabilidad de la preservación a largo plazo en los repositorios.
- **Documentación:** Es imprescindible evidenciar los procesos, objetivos, determinaciones e implementaciones del RD a largo plazo para en determinado lapso de tiempo verificar el avance interno o externo de la organización.
- **Transparencia:** Para medir la calidad del repositorio digital a largo plazo es necesario publicar la documentación de interés de los usuarios y socios, estableciendo confianza a través de la evaluación.

3.7.2. Comparación de Requisitos para obtener entornos digitales

Para este estudio se selecciona los esquemas NÉSTOR, TRAC y DRAMBORA, analizadas anteriormente con la finalidad de seleccionar el método que desempeñe las mejores condiciones para un repositorio de confianza basado en los parámetros según (UNESCO, 2003) y (De Giusti, M. R., 2014). Donde el valor 2 se asigna al parámetro de cumple y el valor 1 al parámetro que no cumple para establecer un valor medible.

Tabla 1-3. Promedio y comparación de cumplimiento de los esquemas

CRITERIOS DE CONFIANZA	TRAC	NESTOR	DRAMBORA
Dedicación y compromiso con los objetos digitales.	2	2	2
Organización	2	2	2
Legalidad	2	2	2
Eficiencia y eficacia en las políticas.	2	2	1
Infraestructura técnica adecuada	1	2	1
Adquisición	2	2	2
Integridad de preservación.	2	2	2
Autenticidad de conservación.	2	2	2
Usabilidad de preservación.	2	2	1
Gestión de Metadatos y Existencia de una pista de auditoria.	2	2	2
Difusión	2	2	2
Planificación y actuación.	2	2	2
Promedio de Cumplimiento	1,91	2	1,75

Realizado por: Verónica Paucar, 2020.

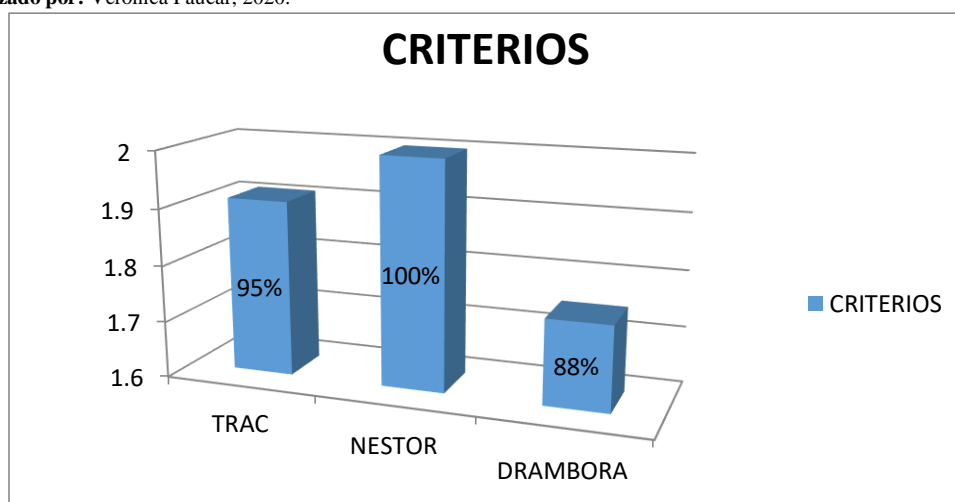


Gráfico 1-3. Porcentajes de heramientas de evaluación de repositorios seguros

Realizado por: Verónica Paucar, 2020.

Interpretación: Para este análisis se ha tomado en cuenta los criterios (De Giusti, M. R., 2014) donde se verifica que Néstor cumple con el 100% de cumplimiento destacándose con respecto a los otros estándares en criterios de infraestructura, usabilidad de preservación y calidad de políticas.

3.7.3. *Análisis del Cumplimiento de la Preservación del Repositorio existente del IST Juan de Velasco*

Para la evaluación del proceso de preservación del repositorio IST Juan de Velasco se aplica un checklist con los criterios de Néstor para repositorios digitales de confianza, con la finalidad de establecer la situación inicial en gestión de marco organizacional, administración de objetos e infraestructura y seguridad de los archivos digitales de su repositorio.

Tabla 2-3. Lista de cumplimiento de criterios para un repositorio de confianza según Néstor.

A.	MARCO ORGANIZACIONAL	Verificación	
1	El repositorio digital ha definido sus objetivos.	X	No cumple
	El repositorio digital ha desarrollado criterios para la selección de sus objetos digitales.		
	El repositorio digital asume la responsabilidad de la conservación a largo plazo de la información representada por los objetos digitales		
	El repositorio digital ha definido su (s) comunidad (es) designada (s)		
2	El repositorio digital otorga a su comunidad designada el uso correcto información representada por los objetos digitales	X	No Cumple
	El repositorio digital garantiza que su comunidad designada pueda acceder a los objetos digitales.		
	El repositorio digital garantiza que la comunidad designada pueda interpretar los objetos digitales.		
3	Se evidencia normas legales.	X	No Cumple
	Contratos legales entre los productores de información y el repositorio digital.		
	Al llevar a cabo sus tareas de archivo, el repositorio digital actúa sobre la base de las normas legales.		
	Con respecto al uso, el repositorio digital actúa sobre la base de los requisitos legales.		

4	La forma organizativa es adecuada para el repositorio digital.		No Cumple
	Se asegura la financiación adecuada del repositorio digital.	X	
	Se dispone de suficiente personal calificado.	X	
	Existen estructuras organizativas apropiadas para el repositorio digital.	X	
	El repositorio digital se involucra en la planificación a largo plazo.	X	
	La continuación de las tareas de conservación está garantizada incluso más allá de la existencia del repositorio digital.	X	
5	Se lleva a cabo una gestión de calidad adecuada		No Cumple
	Se han definido todos los procesos y responsabilidades.	X	
	Se han definido todos los procesos y responsabilidades.	X	
	El repositorio digital documenta todos sus elementos en base a un proceso definido.	X	
	El repositorio digital reacciona ante cambios sustanciales.	X	
B	GESTIÓN DE OBJETOS		
6	El repositorio digital garantiza la integridad de los objetos digitales durante todas las etapas de procesamiento.		No Cumple
	Ingesta: el repositorio digital garantiza la integridad de los objetos digitales.	X	
	Almacenamiento de archivos: el repositorio digital garantiza la integridad de los objetos digitales.	X	
	Acceso: el repositorio digital garantiza la integridad de los objetos digitales.	X	
7	El repositorio digital garantiza la autenticidad de los objetos digitales durante todas las etapas del procesamiento.		No Cumple
	Ingesta: el repositorio digital garantiza la autenticidad de los objetos digitales.	X	
	Almacenamiento de archivos: el repositorio digital garantiza la autenticidad de los objetos digitales. objetos italianos.	X	
	Acceso: el repositorio digital garantiza la autenticidad de los objetos digitales.	X	

8	El repositorio digital tiene un plan estratégico para sus medidas técnicas de preservación.	X	No Cumple
9	El repositorio digital acepta objetos digitales de los productores en base a criterios definidos.		No Cumple
	El repositorio digital especifica sus objetos de transferencia (paquetes de información de envío, SIP).	X	
	El repositorio digital identifica qué características de los objetos digitales son importantes para la preservación de la información.	X	
	El repositorio digital tiene control técnico de los objetos digitales para llevar a cabo medidas de conservación a largo plazo.	X	
10	El almacenamiento de archivos de los objetos digitales se realiza según especificaciones definidas.		No Cumple
	El repositorio digital define sus objetos de archivo (paquetes de información de archivos, AIP).	X	
	El repositorio digital se encarga de transformar los objetos de transferencia (SIP) en objetos de archivo (AIP).	X	
	El repositorio digital garantiza el almacenamiento y la legibilidad de los AIP.	X	
	El repositorio digital implementa estrategias para la preservación a largo plazo de los AIP.	X	
11	El repositorio digital permite el uso de los objetos digitales en base a criterios definidos.		No Cumple
	El repositorio digital define sus objetos de uso (Paquetes de información de difusión, DIP).	X	
	El repositorio digital define sus objetos de uso (Paquetes de información de difusión, DIP).	X	
	El repositorio digital asegura la transformación de AIPs en DIPs.	X	
12	El sistema de gestión de datos es capaz de proporcionar las funciones de repositorio digital necesarias		No Cumple
	El repositorio digital identifica de forma única y permanente sus objetos y sus relaciones .	X	
	El repositorio digital adquiere metadatos adecuados para la descripción e identificación formal y basada en el contenido de los objetos digitales.	X	
	El repositorio digital adquiere metadatos adecuados para la descripción estructural de los objetos digitales.	X	
	El repositorio digital adquiere metadatos adecuados para registrar los cambios realizados por el repositorio digital en los objetos digitales.	X	

	El repositorio digital adquiere metadatos adecuados para la descripción técnica de los objetos digitales.	X	
	El repositorio digital adquiere metadatos adecuados para registrar los derechos y condiciones de uso correspondientes.	X	
	Los metadatos asignados a los objetos digitales están garantizados en todo momento.	X	
C	INFRAESTRUCTURA Y SEGURIDAD		
13	La infraestructura de TI es la correcta.		No cumple
	La infraestructura de TI incorpora las demandas de la administración de la gestión de objetos.	X	
	La infraestructura de TI implementa seguridad del sistema de seguridad de TI.	X	
14	La infraestructura protege el repositorio digital y sus objetos digitales.	X	

Realizado por: Verónica Paucar, 2020.

Realizado el análisis de la situación del repositorio de almacenamiento digital del IST Juan de Velasco mediante los criterios de Néstor, se verifica que no cumple con ninguno de los criterios analizados de repositorios de confianza que garanticen la preservación digital a largo plazo por lo que es indispensable la elaboración de un modelo que permita la preservación de los acervos científicos para su posterior aplicación y certificación.

3.7.4. Estado de madurez de los procesos de preservación del Instituto Superior Tecnológico

Siendo una necesidad fundamental de la institución, comprender el estado de sus procesos y sistemas a nivel de administración de sus acervos científicos y en a la evaluación obtenida en el punto anterior se tiene una visión imparcial del desempeño del instituto en donde se encuentran sus procesos de preservación y que mejoras requiere. Se aplica el siguiente marco de referencia de COBIT 5. (ISACA, 2019)

COBIT es un marco de referencia que permite identificar información de la administración de los procesos TI que una organización necesita para alcanzar sus metas, sus necesidades de inversión, así como la gestión y el control de los recursos TIC. El control mediante escalas es fácil y razonable de entender, permitiendo concientizar los problemas y mejorar. Se basa en los criterios de efectividad, eficiencia, confidencialidad, integridad, disponibilidad, desempeño y fiabilidad. Los recursos TIC que se pueden identificar en COBIT son aplicaciones, información, infraestructura y personal (IF GOVERNANCE INSTITUTE, 2019).

COBIT® – Modelo de Madurez	
0) Inexistente.	Total falta de un proceso reconocible. La organización ni siquiera ha reconocido que hay un problema que resolver.
1) Inicial	Hay evidencia de que la organización ha reconocido que los problemas existen y que necesitan ser re sueltos. Sin embargo, no hay procesos estandarizados pero en cambio hay métodos ad hoc que tienden a ser aplicados en forma individual o caso por caso. El método general de la administración es desorganizado.
2) Repetible	Los procesos se han desarrollado hasta el punto en que diferentes personas siguen procedimientos similares emprendiendo la misma tarea. No hay capacitación o comunicación formal de procedimientos estándar y la responsabilidad se deja a la persona. Hay un alto grado de confianza en los conocimientos de las personas y por lo tanto es probable que haya errores.
3) Definida	Los procedimientos han sido estandarizados y documentados, y comunicados a través de capacitación. Sin embargo se ha dejado en manos de la persona el seguimiento de estos procesos, y es improbable que se detecten desviaciones. Los procedimientos mismos no son sofisticados sino que son la formalización de las prácticas existentes.
4) Administrada	Es posible monitorear y medir el cumplimiento de los procedimientos y emprender acción donde los procesos parecen no estar funcionando efectivamente. Los procesos están bajo constante mejoramiento y proveen buena práctica. Se usan la automatización y las herramientas en una forma limitada o fragmentada.
5) Optimizada	Los procesos han sido refinados hasta un nivel de la mejor práctica, basados en los resultados de mejoramiento continuo y diseño de la madurez con otras organizaciones. TI se usa en una forma integrada para automatizar el flujo de trabajo, suministrando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte con rapidez.

Figura 1-3. Cuadro estado de madurez de una organización según COBIT

Fuente: (ISACA, 2019)

Según el marco de referencias COBIT 5 el estado de madurez de los procesos de la institución en estudio está en el nivel 0) Total falta de un proceso reconocible. La organización ni siquiera ha reconocido que hay un problema que resolver.

3.8. Elaboración del modelo de preservación digital de documentos a largo plazo PDDL-UESTJV

3.8.1. Introducción

Aquí se presentará los resultados que se encontraron al utilizar diferentes medios de recolección de la información como: entrevistas realizadas a las personas involucradas en el proceso archivístico y un cuestionario de auditoría basada en Néstor que permite acercarnos al estado de

preservación a largo plazo de la institución, los sujetos con los que se tuvo contacto son el técnico TIC encargado de los procesos y posteriores entrevistas realizadas a los encargados de recepción del archivo físico y digital; y al coordinador de la institución quienes han ayudado en este proyecto teórico de investigación. Los primeros resultados se presentan en forma de caso de estudio y la auditoría en forma de tabla que permite valorar y observar el entorno de preservación.

La investigación propone un modelo teórico de referencia en preservación digital a largo plazo para entidades educativas de prototipo mediana o pequeña, por la cantidad de alumnos matriculados en la institución.

3.8.2. Presentación del Instituto Superior Tecnológico Juan de Velasco

El Instituto Superior Tecnológico Juan de Velasco tiene domicilio en la Provincia de Chimborazo, ciudad de Riobamba Av. Chimborazo 11-56 y Cuba (a una cuadra del parque de la madre). Puede establecer campus, sedes o extensiones bajo el cumplimiento de los requisitos y formalidades establecidas en la Ley Orgánica de Educación Superior y demás normativa vigente, previa aprobación del Consejo de Educación Superior.

- **MISIÓN**

"Somos una institución de educación superior que forma profesionales de tercer nivel tecnológico con conocimientos sólidos, orientados al emprendimiento, capaces de llevar adelante cambios innovadores mediante la investigación, que aporten al plan de desarrollo local, regional y nacional con conciencia ética y solidaria en beneficio de la sociedad".

- **VISIÓN**

"Ser una institución acreditada a nivel superior con una formación integral de calidad, competitivos frente a los cambios de innovación tecnológica-investigativa, con responsabilidad social y un desarrollo sostenible de nuestro país".

3.8.3. Aproximación al entorno de preservación de documentos de la Institución Juan de Velasco

En esta etapa se realiza unas entrevistas a las personas encargadas del acervo académico - científico de la institución. Quien hace el proceso de ingesta del documento digital en la

institución es la persona encargada de secretaría realizando el manejo de los documentos de producción académica final de los estudiantes durante todo el ciclo de vida de los mismos. En el Anexo A se encuentran las preguntas realizadas en la entrevista, de esta exploración se deduce que los procesos de ingesta se realizan de forma manual previo a un oficio de entrega recepción de la investigación académico-científica realizada por los estudiantes, una vez recogida su original y las copias se le asigna en el espacio de archivología de la secretaría. Cuando requieren de un archivo (tesis), se realiza una petición escrita para su prestación, en cuanto al proceso de digitalización se posee una copia en una unidad de CD a la cual no se realiza ninguna estrategia de preservación en el tiempo.

En el caso de entrevista del Coordinador Académico se analiza si poseen en el instituto reglamentos, plan, políticas o estándares que permitan preservar sus documentos digitales de producción académica, supo manifestar que no poseen ningún tipo de reglamento interno que permita la regulación de procesos de preservación. A demás indica que la sociabilización de la Regla Técnica Nacional para la Organización y Mantenimiento de los Archivos Públicos que rigen en el Ecuador, según acuerdo No. SGPR-2019- 0107 del 10 de abril del 2019, que tiene por objetivo cumplir con las dimensiones de la seguridad de la información y la preservación documental, no ha sido difundida entre el personal por lo que se puede deducir que el conocimiento de preservación de documentos digitales a largo plazo es nulo. Anexo B

En la entrevista con la persona encargada de los servidores y plataformas de la institución y una de las aproximaciones más importantes que permite ver la situación en la que se encuentra la instrucción a nivel de preservación a largo plazo de sus archivos digitales, así también de su repositorio físico. Si la institución cuenta con un repositorio digital o biblioteca digital o similar dice que no cuentan con un repositorio digital de las producciones científicas de los estudiantes. Que los formatos de los archivos en los que se almacena la producción académica son PDF, en el caso de la gestión de los archivos de interés la secretaría es la que gestiona de forma manual según los estatutos institucionales, el almacenamiento y localización geográfica, en relación a la pregunta de la integridad, no alteración, gestión de metadatos, formatos de los documentos digitales manifiesta que no existe ese proceso por parte de ningún personal de la institución, así como en infraestructura no poseen un espacio que cumpla con un estándar para el propósito de conservación, en conclusión no hay una buena gestión de la seguridad de la información de los productos intelectuales, afirmaciones en base al Anexo C

El entorno de trabajo analizado y las circunstancias en las que se desempeña y los tipos de datos y procesos, se puede afirmar que la entidad no dispone de un modelo de gestión de la información

digital para la preservación de documentos científicos y demás documentos, se identifica que no existe conocimiento y cuidado sobre el patrimonio de la información que manejan. Existe innegable inquietud sobre la vida útil de los archivos científicos producidos por su entidad por la omisión de leyes y estándares de conservación digital. Esto se afirma en base a las respuestas formuladas por preguntas del Anexo B.

3.8.4. *Presentación de la propuesta del modelo de Preservación Digital*

Después de exponer la investigación y verificar el entorno en base a los casos de estudios entrevistados, se realiza una evaluación con 14 criterios propuestos por Néstor y se obtiene datos sobre sus sistemas y procesos informáticos que permiten realizar un análisis de sus falencias en los procesos.

La presentación del modelo de preservación a la institución educativa fue receptada positivamente de manera general ya que se logró que se tome consciencia de la aplicación de leyes, norma y estrategias que permitan salvaguardar la producción científica generada por sus estudiantes, actualmente esta actividad es responsabilidad del departamento de secretaria de la institución quien la gestiona en todo el ciclo de vida. En el modelo que se propone se define diferentes roles y responsabilidades en la gestión del archivo digital. Se observa que el personal encargado de los archivos no tiene conocimiento técnico por lo que se debe realizar capacitación a los encargados de los documentos digitales y personal del departamento informático, es preciso definir perfiles en base roles. El apoyo por parte de la institución se ha desarrollado de forma desinteresada de forma presencial, telefónica y en línea durante todo su desarrollo.

3.8.5. *Elaboración del Modelo PDDLPIESTJV*

El modelo se denomina PDDLPIESTJV (Preservación Documentos Digitales a Largo Plazo en Instituciones de Educación Superior Tecnológico Juan de Velasco). Con los datos obtenidos en las entrevistas y la evaluación con Néstor sobre las necesidades preservación digital, y previo al análisis de los modelos de preservación a largo plazo, se adopta el entorno y funciones de preservación del modelo OAI, en aspectos de instituciones de educación superior como el tecnológico Juan de Velasco. Se aborda la preservación del entorno de creación de los acervos científicos digitales y la capacidad de aumentar su preservación en el tiempo, así como la administración del archivo digital en repositorios externos confiables con el establecimiento de políticas futuras y convenios que garanticen el objetivo de esta investigación añadiendo una

característica con la que no se cuenta en OAIS. El ambiente en el que se está trabajando es cerrado. La entidad no cuenta con políticas, sistemas ni modelos que preserve su acervo científico.

En la figura 1-2 del Capítulo 2 muestra el archivo OAIS con sus seis entidades: Ingesta (Ingest), Administración (Administración), Planificación de la Preservación (Preservation Planning), Gestión de los Datos (Data Management), Archivo de Almacenamiento (Archival Storage) y Acceso (Access). Descripción de las funciones de OAIS:

- ✓ **Ingesta (Ingesta).** - Se encarga de recibir los paquetes de información y añade los metadatos necesarios para transformar el objeto en fichero archivable y siendo estos metadatos parte del Paquete de Información Archivable (AIP). Aquí se puede rechazar información del Productor si esta no está definida según el modelo de información OAIS. El SIP interviene con los datos que proceden del Productor y el proceso de la ingesta genera un AIP donde la información se prepara para ser archivada. El Productor envía información al archivo en forma de Paquete SIP este es recibido por la función Recepción de la Submisión, después le envía al bloque de Verificación de la Calidad para comprobar que coincida con el modelo de información y validar la entrada.
- ✓ **Archivo de Almacenamiento (Archival Storage).** - Gestiona el acopio de la información, y la recuperación de los mismos. Esta entidad recibe el paquete de información de Archivo(AIP) y la almacena en la base de datos del archivo OAIS. La función Recibir Datos recibe el AIP, enviando una señal de confirmación de almacenamiento al Bloque Ingesta. Al mismo tiempo la entidad Funcional Administración gestiona políticas de acceso a través de las funciones de Gestión de la Jerarquía de Almacenamiento y Substitución de Medios que sirven para cambiar el soporte donde está la información y así esta no se pierda. Las funciones Comprobación de Error y Recuperación frente a Desastres realizan actividades de notificación de error y recuperación de copias del archivo, en caso de haber corrupción de los datos o en el soporte donde estos se hospedan.
- ✓ **Gestión de los Datos (Data Management).** - Proporciona funciones para proteger la Información Descriptiva (Descriptive Information) y los datos administrativos para la gestión de los datos. Es así que se encarga de actualizar la base de datos del Archivo OAIS, así como mejora el acceso a Información Descriptiva. Su función más relevante es ser Administrador de Base de Datos, responsable de mantener la integridad de la información, creando tablas o esquemas que soporten las funciones de Gestión de Datos.

El bloque de recuperación de la actualización de la Base de Datos notifica la actualización de la misma a las entidades funcionales Ingesta y Administración.

- ✓ **Administración (Administration).** - Esta entidad realiza todo el mantenimiento del archivo OAIS. Suministra actividades para crear el fichero completo, ejecuta todas las operaciones de archivo o la migración /actualización de los datos archivados. Aquí están involucrados todos los actores del modelo OAIS, se encarga de la gestión de todos los flujos de políticas de los datos que se va archivar. Manteniendo la integridad y trazabilidad de la configuración durante las fases del ciclo de vida de los documentos. Permite gestionar tanto los procesos de auditoria para verificar la calidad y políticas de archivos, así como verificación de estándares.

- ✓ **Planificación de la Preservación (Preservation Planning).** - Monitoriza los servicios del archivo OAIS, para certificar que la información almacenada en un archivo OAIS es accesible a largo plazo para la Comunidad Designada, así el medio se vuelve obsoleto. También se encarga de realizar recomendaciones de mejora de archivo y permite la monitorización de los nuevos avances en tecnología para aplicar después políticas de preservación y estándares.

- ✓ **Acceso (Access).** - Realiza procesos de recuperación de la información a los consumidores, así como la denegación de acceso. Es la entidad funcional que facilita servicios a los consumidores para que puedan recibir y entender la información que solicitan. Coordina las actividades de acceso de información recuperando y generando un paquete de Información de Diseminación (DIP) para que el consumidor pueda disponer de la Información que requiere. 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.

Los resultados obtenidos mediante el análisis de los casos de estudio sobre la preservación de documentos digitales, el análisis de las leyes de preservación del Ecuador y la evaluación previa con NESTOR, permite la personalización de las entidades funcionales del modelo OAIS como se puede observar en la Figura 9-3.

3.8.6. Actores del modelo PDDL-IESTJV

Los actores que interactúan con el archivo y sus roles son:

- **Productor.** - El productor son todos los estudiantes quienes generan sus archivos digitales de sus tesis una vez aprobados y cumplido con el reglamento de la institución para su conservación a largo plazo.
- **Gestión.** - El Gestor es la persona con conocimiento informático encargada de la administración de las políticas de conservación, ingesta y acceso dentro de un archivo PDDLPIESTJV.
- **Consumidor.** - Los consumidores son todas las personas que conforman la comunidad como estudiantes, docentes, administrativos quienes acceden a la información.

3.8.7. *Aporte y simplificación de la Entidad Ingesta*

Recepción de la Sumisión: Según su descripción en el modelo OAIS, proporciona y facilita la apropiada capacidad de almacenamiento desde el Productor o desde el Administrador.

A esta entidad se adiciona una subfunción de **Comprobación del Envío** de los Datos que se ingresan con los documentos digitales (tesis), esto incluye una autorización correspondiente para su preservación y difusión, que cumpla con la reglamentación necesaria de preservación de la institución que verifique los tipos de usuarios según los roles de las entidades de la comunidad designada sean estos administradores, educadores, creadores y público en general, así como la generación de la primera copia original del objeto digital a preservar verificando errores causados por aplicaciones activas o medios corruptos con errores en la recepción del objeto original.

Función Recepción del Envío: El SIP puede ser entregado por diferentes medios de comunicación que necesita cumplir las normativas legales específicas de acceso, validando que no sea un archivo corrupto, para incorporar al archivo del modelo PDDLPIESTJV, colocando identificadores ingresos, así como derechos de autor, y al existir un error en el proceso de adquisición solicitar el reenvío del paquete al Productor. Los metadatos descriptivos en la función recepción de envío son ingresados por interfaz de usuario mediante web, que proporcionaran datos de usuarios, auditorias, estado, conexiones, observaciones e integridad configurados en la subfunción Comprobación de datos del archivo, teniendo la capacidad de integrar diversos esquemas de metadatos de preservación como PREMIS generando el AIP del archivo digital como objeto de archivo a largo plazo.

En la **función Aseguramiento de la calidad** se concibe con una subfunción de la Función Recepción de la sumisión, el tratamiento del objeto digital es el mismo del modelo OAIS. Esta

acredita que la transferencia de datos SIP sea exitosa mediante Comprobaciones de Redundancia Cíclica (CRC) hacia el proceso de almacenamiento transitorio. En el caso de los productos científicos generados en IST, se probará una vez más que los archivos a ser transferidos o su medio de comunicación, no tengan errores de lectura/escritura, autenticando los formatos de acuerdo a los datos recibidos por el proceso Comprobación del Envío del archivo a través de auditorías, atendiendo a la integridad de los datos, certificando la entrada al coincidir el archivo con el modelo de información validando así la integridad de los datos.

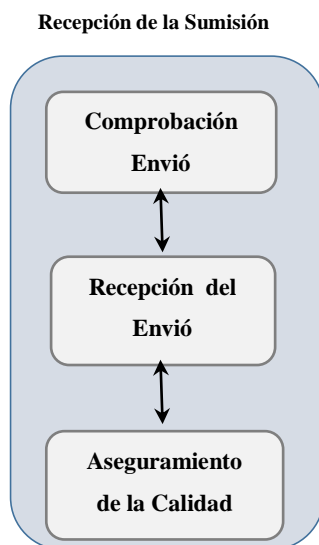


Figura 2-3: Generador de AIP y validación de usuarios

Realizado por: Verónica Paucar, 2020

Generar AIP: esta función convierte el SIP en AIP para preparar la información en base a reglas, políticas y esquemas afines a los archivos digitales, se obtiene un informe de auditoría a la administración cumpliendo este bloque con el estándar de acceso a la interoperabilidad.

Generación de Información Descriptiva: esta función es la que extrae datos descriptivos del AIP, que en este caso serán los archivos de conocimiento científico (tesis), a más de seleccionar información descriptiva de otros bloques que sean de ayuda para administrar la gestión de datos, al realizar la extracción /generación de metadatos facilita la recuperación del objeto digital archivado a largo plazo, también se inspeccionará formatos de los AIP para realizar modificaciones si fueran necesarias en la entidad de Planificación de la Preservación.

Coordinación de las Actualizaciones: Permite gestionar el envío de AIPs de los documentos digitales al Almacenamiento de Archivo y la información descriptiva a Gestión de Datos.

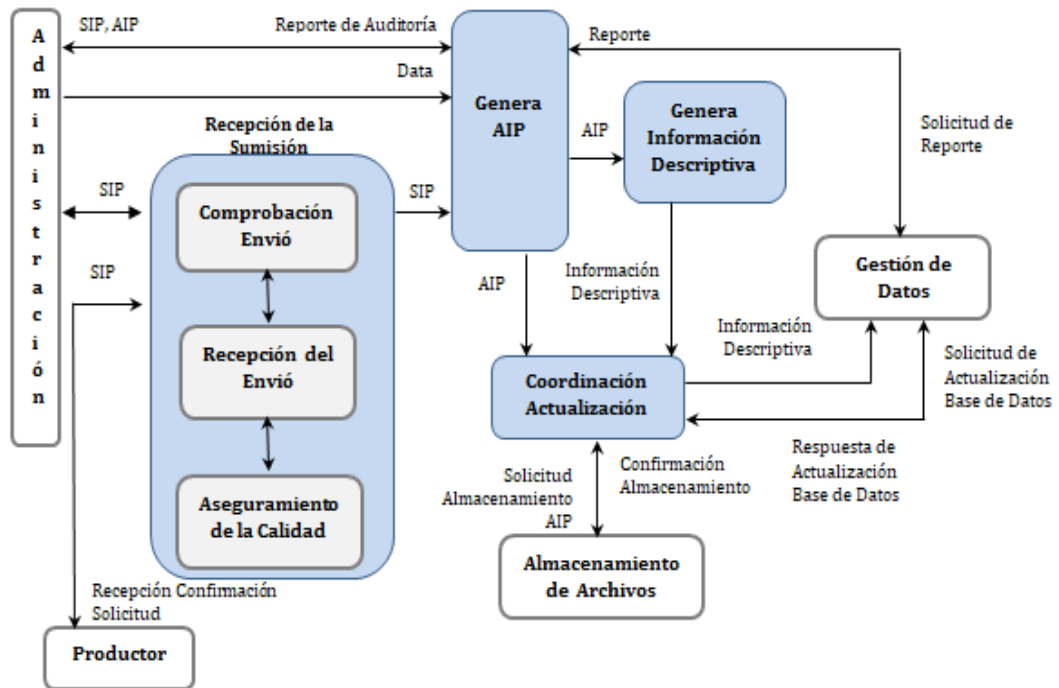


Figura 3-3. Entidad Funcional Ingesta

Realizado por: Verónica Paucar, 2020 (basado en el modelo OAIS)

3.8.8. *Aporte y simplificación de la Entidad Funcional Almacenamiento*

La entidad de Almacenamiento de Archivo es una función primordial concebida dentro del modelo PDDL-PIESTJV es la que se encarga de almacenar la información en el medio físico en uno o más unidades internas que contendrán documentos digitales. Guarda el AIP recibido de la ingesta garantizando la integridad al verificar que los datos al ser transferidos no sean dañados, ni tengan errores, duplicando los objetos digitales y constantemente se remite información del inventario a la administración para gestionar políticas de acceso y ayudar en el manejo de la gestión de jerarquía de almacenamiento, la sustitución de medios y garantizando el acceso a la información en caso de desastres.

Función Recepción de Datos: Recibe una petición para almacenar de forma estable el AIP que viene de la Ingesta, muestra la frecuencia de recuperación de los datos que forman el AIP y pasa a la función de comprobación de errores.

Función Verificación de Errores: Valida que el AIP de la ingesta y sus elementos estén sin ningún tipo de error; así también comprueba que no ocurra daños en las transferencias de datos dentro de los procesos de almacenamiento. El hardware y software emite avisos de probables

errores que son enviados al registro de error para ser revisados por los encargados del almacenamiento y corregirlos para asegurar su disponibilidad.

Función Administración de la Jerarquía de Almacenamiento: Sitúa los AIPs en el medio de almacenamiento apropiado, añadiendo más políticas de seguridad si fuera preciso. Se encarga de la elección del tipo de medio, dispone a los mecanismos realizando la transferencia física de los dispositivos de almacenamiento de los documentos digitales, finalizado la transferencia se confirma el almacenamiento definitivo a la ingesta y su ID de embodegamiento de la información del AIP, en este escenario se puede realizar un almacenamiento virtual u otro tipo de soporte aprobado de acuerdo a su uso o velocidad de acceso. Esta función se complementa con la función comprobación de errores.

Función Substitución de Medios: Esta función es eliminada ya que la función Recuperación Frente a Desastres realiza la misma función.

Función Recuperación Frente a Desastres: Duplica, migra, moviliza refresca los documentos digitales recopilados en el archivo y replica físicamente la copia del archivo digital en diversos medios extraíbles o por su sistema de red de transferencia. Quién pone las reglas de recuperación es la Administración. Se planifica prevención y recuperación ante desastres informáticos con el documento digital como un archivo que contiene datos dañinos, es ilegible, dispositivos dañados o que no se pueden leer parcial o totalmente sin posibilidad de ser rehabilitado, la pérdida total de datos requiere una solicitud de una copia al proveedor para su reemplazo, movilizándolo a un nuevo medio de almacenamiento sin alterar en este proceso el contenido de la información, ni datos de descripción de la preservación (PDI) dando un grado de seguridad en la integridad y disponibilidad.

Función Proveedor de Datos: Realiza copias de AIPS recolectados a la entidad acceso. Mediante una solicitud de AIP. Aquí se identifica al API solicitado, transfiriéndole a un almacenamiento temporal, cuando existe un pedido de transferencia de datos de acceso se encarga de avisar desde su inicio hasta su finalización.

Función Medio de Almacenamiento: Aquí se ejecuta la copia del archivo digital original y de sus elementos que le acompañan de procesos de repositorios aceptados, sobre la reproducción se hacen todas las actividades de acceso, gestión y operaciones de almacenamiento. La función coordinadora recibe la copia original del documento digital aprobado de esta función para gestionar su embodegamiento a un repositorio externo de confianza.

Función Coordinación: Se agrega esta función para coordinar y organizar directamente acciones de replicación del documento digital original procesado localmente en la función en Medio de Almacenamiento de datos con la entidad externa con quien se compartirá transacciones y procesos de replicación del API mediante el equilibrio de técnicas, políticas, acuerdos, alianzas de trabajo colaborativo en replicación de repositorios digitales en la red logrando garantizar su presentación a largo plazo en nuestro caso quien intervendrá según artículo 76 del estatuto del instituto, la unidad de relaciones internacionales e institucionales.

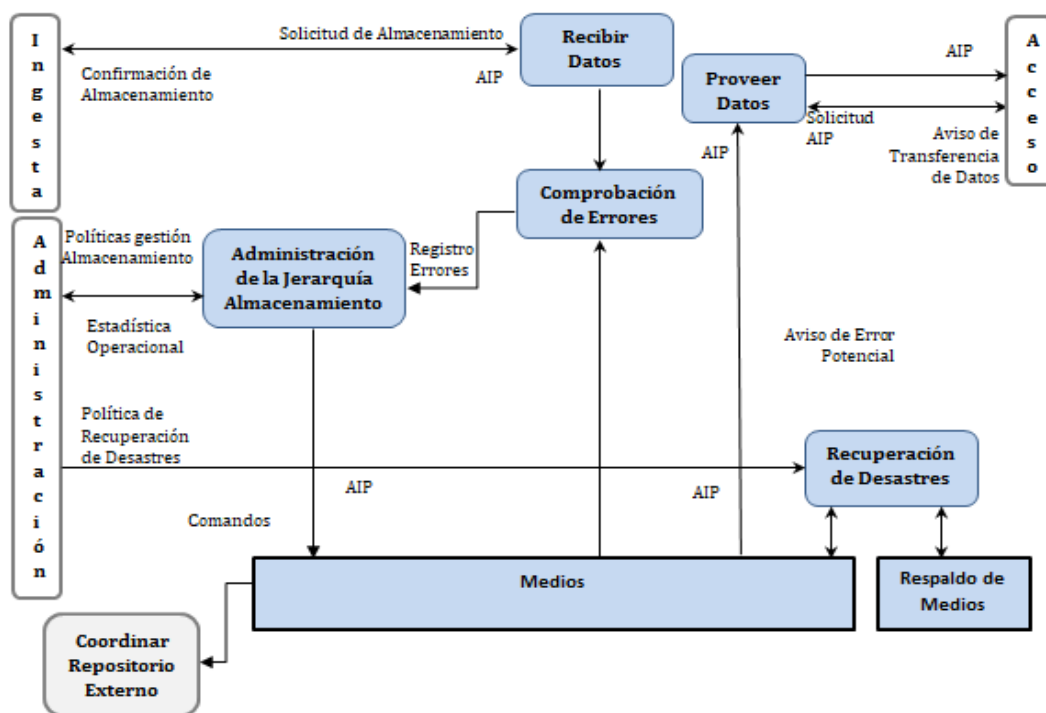


Figura 4-3. Entidad Funcional Almacenamiento

Realizado por: Verónica Paucar, 2020 (basado en el modelo OAIS)

3.8.9. Simplificación de la Entidad Gestión de Datos

La entidad funcional Gestión de Datos tiene como actividad primordial realizar procesos de administración y custodia de la información descriptiva o administrativa de la base de datos que describen los documentos digitales para generar reportes, su funcionamiento está ligado con la entidad de almacenamiento. Actualiza la información que se incorpora y ofrece informes si se modifica o borra algún dato. Genera reportes de los diversos componentes del modelo, la solicitud de reporte puede ser de entidad ingesta, acceso o administración, suministran diversos tipos de informes o la descripción específica del archivo digital, por lo que esta entidad es necesaria en su totalidad.

Función Generar Reporte: Genera informes de los documentos digitales almacenados, estos pueden ser visualizados por su categoría, accesos o suministrar datos descriptivos de acuerdo a la petición realiza por ingesta, acceso y administración.

Función Realizar Consultas: La función acceso realiza una petición de consulta a esta función que accede a la base de datos para mostrar una respuesta para el solicitante.

Función Administrador de Base de Datos: Se encarga de la administración de políticas de actualización de la base de datos; la administración quién envía las reglas para mantener la base de datos integra, responsable de proveer componentes de almacenamiento de información, además de encargarse de la recepción de la actualización del sistema, previo la recepción de información descriptiva y solicitud de actualización con procesos provenientes de la ingesta y la administración.

Función Recepción de Actualización de Base de Datos: Los procesos de esta función se fusionan con la función Administrador de Base de Datos por lo que se elimina del esquema.

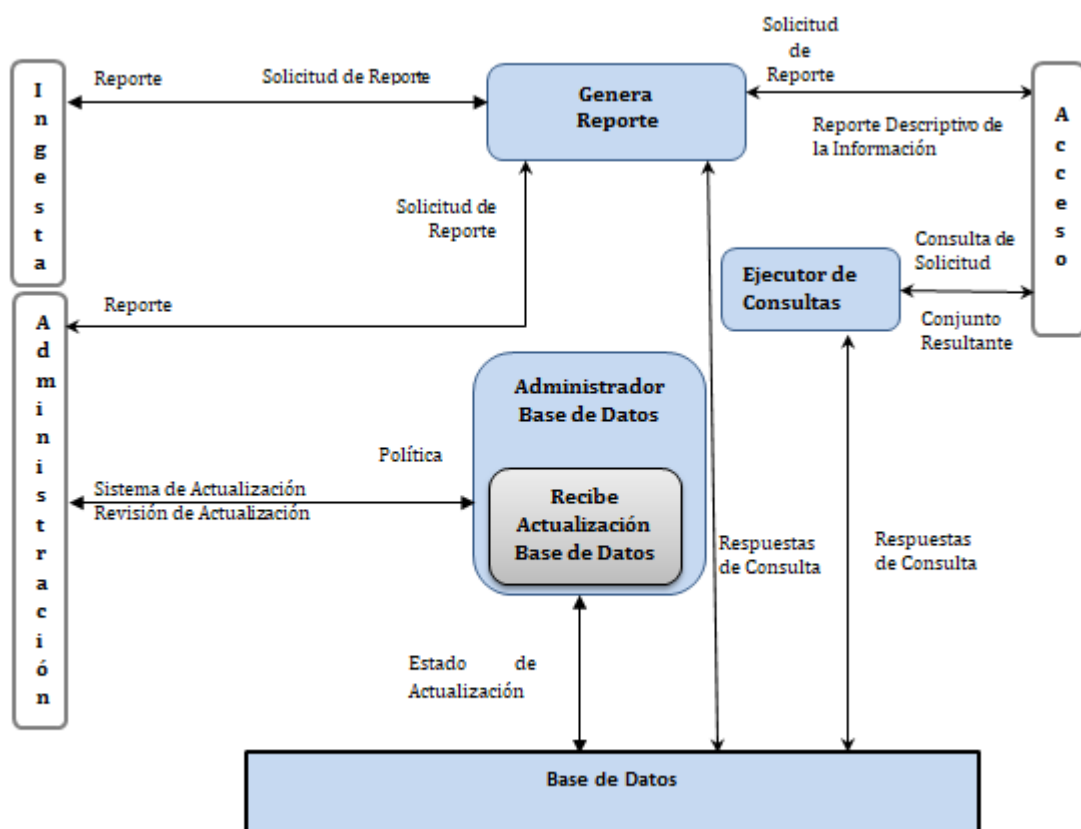


Figura 5-3. Entidad Funcional Gestión de Datos

Realizado por: Verónica Paucar, 2020 (basado en el modelo OAIS)

3.8.10. Simplificación de la Entidad Administración

Esta entidad posee funciones y servicios para ejecutar todo el sostenimiento del documento digital y es el espacio de las interrelaciones internas y externas del modelo PDDLPI-IESTJV, determina convenios con el productor del documento digital añadiendo información, ejecuta operaciones de actualización de los datos, estableciendo reglas de almacenamiento de los documentos en riesgo y responsabilidades de escucha a peticiones de consultas de los documentos digitales. Esta función esta involucra a todos los actores del modelo. Responsable de mantener la integridad y trazabilidad durante el ciclo de vida de los documentos.

Función Control de Acceso Físico: De acuerdo con las estrategias de archivo, aporta con componentes o elementos físicos que restringen o permiten el acceso físico a los documentos digitales

Función Establecer Estándares y Políticas: Como su nombre lo indica es responsable de crear, implantar y proteger patrones, modelos, esquemas, políticas y normas del sistema de archivo. Recibe recomendaciones y propuestas de la entidad de planificación de preservación de nuevos estándares para los documentos digitales y del manejo de informes de riesgos constantes, devolviendo a esta entidad objetivos normas, políticas de migración de estándares aprobados. Minimiza conflictos de hechos inesperados negociando responsabilidades de entrega de documentos digitales, establece políticas de recuperación ante catástrofes, políticas de seguridad del archivo, de acceso físico, de control de error del documento digital, los lineamientos del proceso ingesta y estándares de formato del documento.

Función Presentación de Auditoría: Aquí se recibe comentarios de los paquetes AIP/SIP desde la planificación de preservación, emite observaciones si los registros de AIP/SIP se han aplicado con éxito en la ingesta, comprobará que los envíos de AIP/SIP se efectúen con los acuerdos de envío, comprobando que los paquetes cumplan con las especificaciones del archivo. Verificará que la información del PDI sea correcta, clara y autónoma de la comunidad asignada. La revisión del documento digital se modificará en base a las políticas internas. Realiza reportes de auditoría a ingesta, al productor. En el caso de algún incidente intervendrá la Comisión Académica del IEST quien organice y recobre información para ser auditada verificando su integridad.

Función Negociación de Aceptación: Solicita reportes finales aceptables para tratar y proceder a negociar con el productor la preservación del documento digital, realiza la exposición de un calendario de sesiones de pedidos de información acordadas, estableciendo pautas y recursos

precisos de transferencia y la aceptación de los SIPs al modelo PDDL-IP. La entidad Planificación de Preservación envía plantillas establecidas de AIP/SIP mandando a la función de sumisión de auditoría para que él envío sea aprobado.

Función Actualización de la Información del Archivo: Proporciona los medios necesarios para renovar la información de los documentos digitales del modelo.

Función Servicio al Cliente: Es la que gestiona y conserva cuentas de consumo, creando datos de facturación y recibiendo pago del cliente por recursos usados. Función que se decide suprimir ya que no se realiza facturación por el acceso al acervo de conocimientos científico (documento digital).

Función Activación de la Petición: Ayuda con la realización de la petición de transmisión, difusión o propagación de la información a la entidad acceso.

Función Gestión y Configuración del Sistema: Observa frecuentemente los documentos digitales en lo que se refiere a lo tecnológico, obedece a la función establecimiento de estándares y políticas reforzando la custodia del archivo del modelo o los avances tecnológicos.

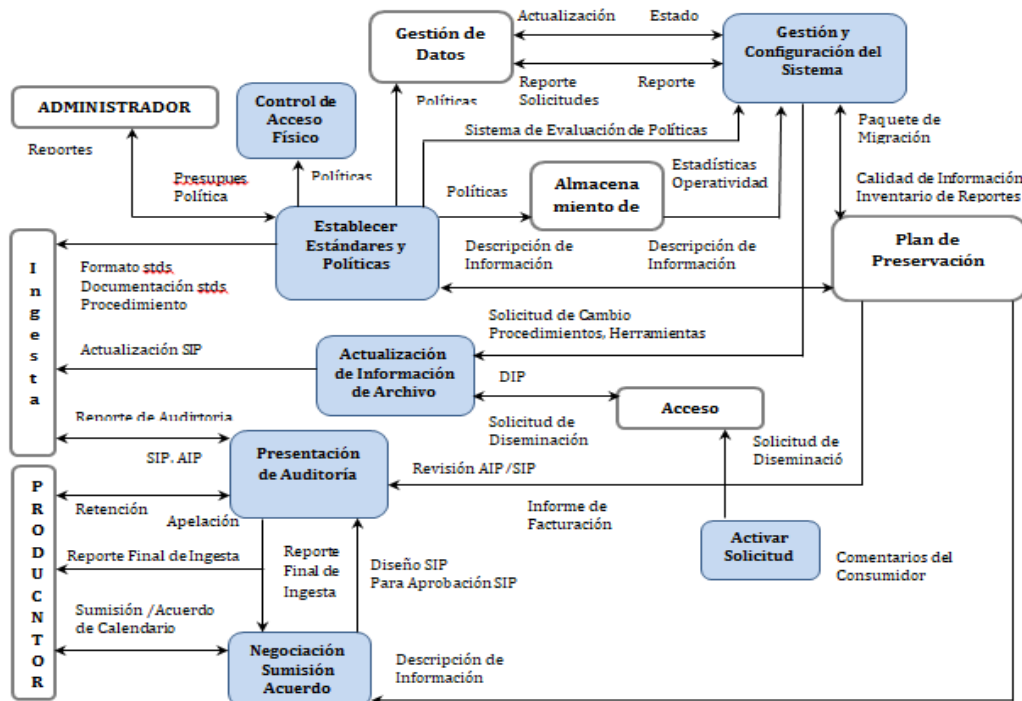


Figura 6-3. Entidad Funcional Administración

Realizado por: Verónica Paucar, 2020 (basado en el modelo OAIS)

3.8.11. Entidad Funcional Planificación de la Preservación

Esta función inspecciona el entorno del modelo, constituye planes de preservación a largo plazo, certifica que la información recopilada esté disponible y comprensible para la comunidad, hace una supervisión a la tecnología de procedencia y sus avances, de las políticas de la información, de los escenarios informáticos, para aplicar nuevas políticas de preservación y estándares de ser necesario.

Desarrollo de Diseño de Empaquetamientos y Planes de Migración: Realiza prototipos de implantación de reglas y políticas de administración mediante el desarrollo de diseños de paquetes de información previo a recomendaciones y sugerencias sobre su aplicación, sugiere SIP/AIP examinados e individualizados, recibe resultados de prototipos, requerimientos de prevención, estándares aprobados, objetivos de migración y envía todos estos asuntos para ser tratados en la función desarrollo de estándares y estrategias de prevención devolviendo esta su asesoramiento.

Monitoreo Diseñado de la Comunidad: Trabaja con los clientes y productores y hace un seguimiento de las necesidades y exigencias de servicio y tecnologías de producto, como avances de plataformas de computación, tipos de dispositivos y medios de comunicación, formatos de la información, software de manejo de paquetes. Las encuestas, observaciones frecuentes, grupos de trabajo comunitarios constantes son fundamentales para el desarrollo de esta función que se encarga de enviar alertas tecnológicas, estándares de datos externos, resultados de prototipos a la función monitoreo y desarrollo de estrategias de prevención en base a solicitudes de prototipos.

Monitoreo de la Tecnología: Como su nombre lo indica monitoriza las tecnologías obsoletas que podrían afectar al documento digital en su medio computarizado, a la vez busca y rastrea nuevas tecnologías, hardware y software, estándares informáticos para renovar el documento digital en el repositorio de software y evitar que este caiga en la obsolescencia, recibe solicitud de prototipos de las funciones, y devuelve alertas de tecnologías, estándares de datos externos, resultados de prototipos y reportes a la función desarrollo de estrategias y estándares de preservación.

Desarrollo de Estrategias y estándares de preservación: Trabaja con los clientes y productores y hace un seguimiento de las necesidades, exigencias de servicio y tecnologías de producto, como avances de plataformas de computación, tipos de dispositivos y medios de comunicación, formatos de la información, software de manejo de paquetes, para recomendar propuestas,

teniendo revisiones AIP/SIP y plantillas de nuevos AIP/SIP, paquetes de migración y consejos de personalización provenientes otras funciones para una mejor la administración del documento digital en la planeación de preservación. Aquí quedará establecido políticas y estándares de preservación del instituto de educación superior que permitan valorar futuros conflictos, proporcionando reportes del peligro encontrado y de aprobar el cambio o reposición del documento digital o esquema del sistema, basado en legislaciones actuales y certificaciones de su proceso de preservación a largo plazo. Para lograr su funcionamiento recoge del monitor de tecnología alertas tecnológicas, estándares de datos externos, resultados de prototipos, recibe reportes, alertas de requerimientos de estándares emergentes de la función monitor de comunidad designada, informes de inventario, rendimiento y comentarios de consumidores desde la administración, y absorbe o recoge asuntos, cuestiones de la función desarrollo de diseño de empaquetado y planes de migración, es decir esta función es el eje de esta entidad.

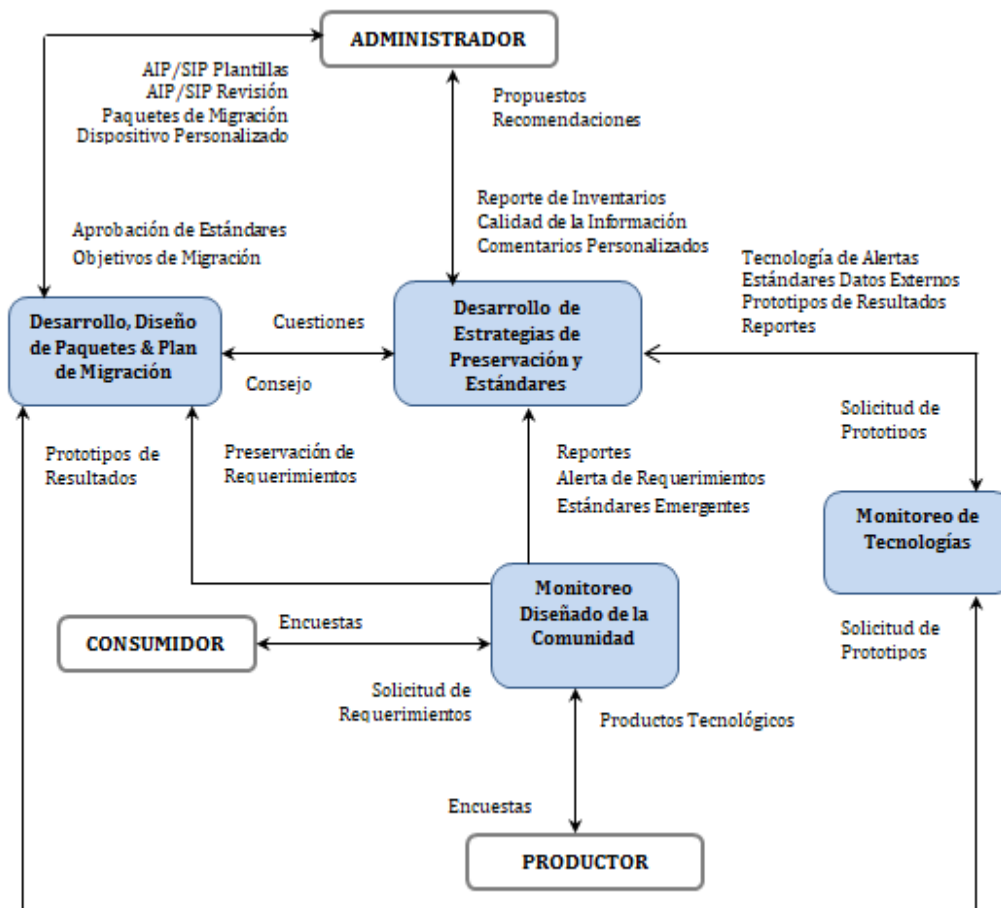


Figura 7-3. Entidad Funcional Plan de Preservación

Realizado por: Verónica Paucar, 2020 (basado en el modelo OAIS)

3.8.12. Entidad Funcional Acceso

Entidad que sistematiza el acceso a la información, lleva el proceso de transmisión de los DIP (Paquetes de Información de Disseminación) a los usuarios, facilita los servicios a los consumidores situando y buscando la información a ser presentada a los usuarios, los datos que recibe el consumidor son una copia exacta del original pero puede ser en un formato diferente.

Función Coordinador de Actividades de Acceso: Proporciona varias interfaces de recuperación de los documentos digitales a través de servicios en línea. Para disponer un DIP (paquete de difusión de la información) para entregar al cliente, este puede solicitar un informe a través de distintas consultas usando formatos apropiados para su entrega. Las peticiones de consulta son procesadas de forma inmediata en gestión de datos. Las solicitudes de órdenes se establecen una sola vez para compartir documentos, o por la activación de pedido de la administración o por la función almacenamiento de archivo.

Función Generar DIP: Admite una petición de propagación, recobra el AIP de la entidad funcional almacenamiento de archivo temporal haciendo un duplicado para ser procesado cuando sea necesario de forma inmediata. Realiza procedimientos estadísticos muestreos en espacios transitorios, realiza transformaciones en varios tipos de archivos de salida, clasifica datos de usuario dando seguridad según perfil usuario, transfiere una demanda de información de gestión de datos con el afán de conseguir información descriptiva, sumersión y asignar en almacenamiento temporal mientras comunica a la función coordinar actividades de acceso que el documento digital está listo para ser enviado en condiciones iguales a su creación.

Función Dar Respuesta: Da respuesta y determina un Id de reproducción de autorización del documento digital en las entregas a los clientes, cuando realiza una entrega en línea recepta la respuesta de la función coordinar actividades de acceso disponiendo transmisión en tiempo real por medio de reglas de comunicación. Una vez que verifica el destinatario establece la transferencia en línea peticionada, esta respuesta es enviada al área de almacenamiento temporal, una vez la respuesta ha sido enviada, se recibe una notificación de recibido.

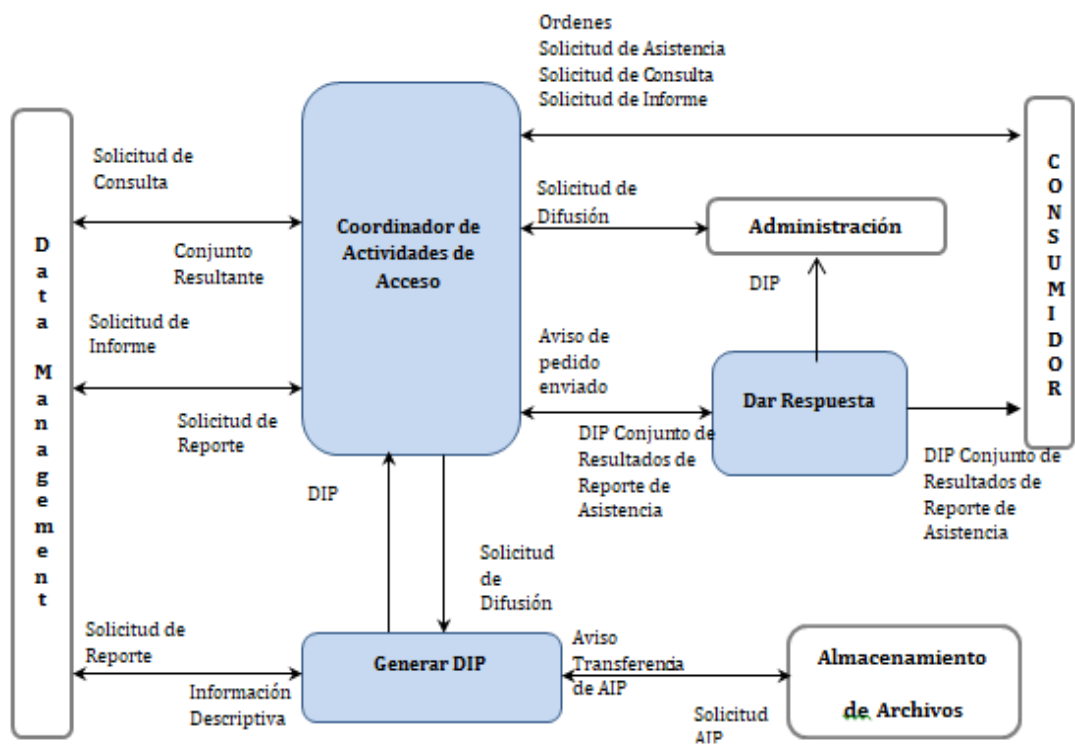


Figura 8-3. Entidad Funcional Acceso

Realizado por: Verónica Paucar, 2020 (basado en el modelo OAIS)

ENTIDADES FUNCIONALES DE PDDL-UESTJV

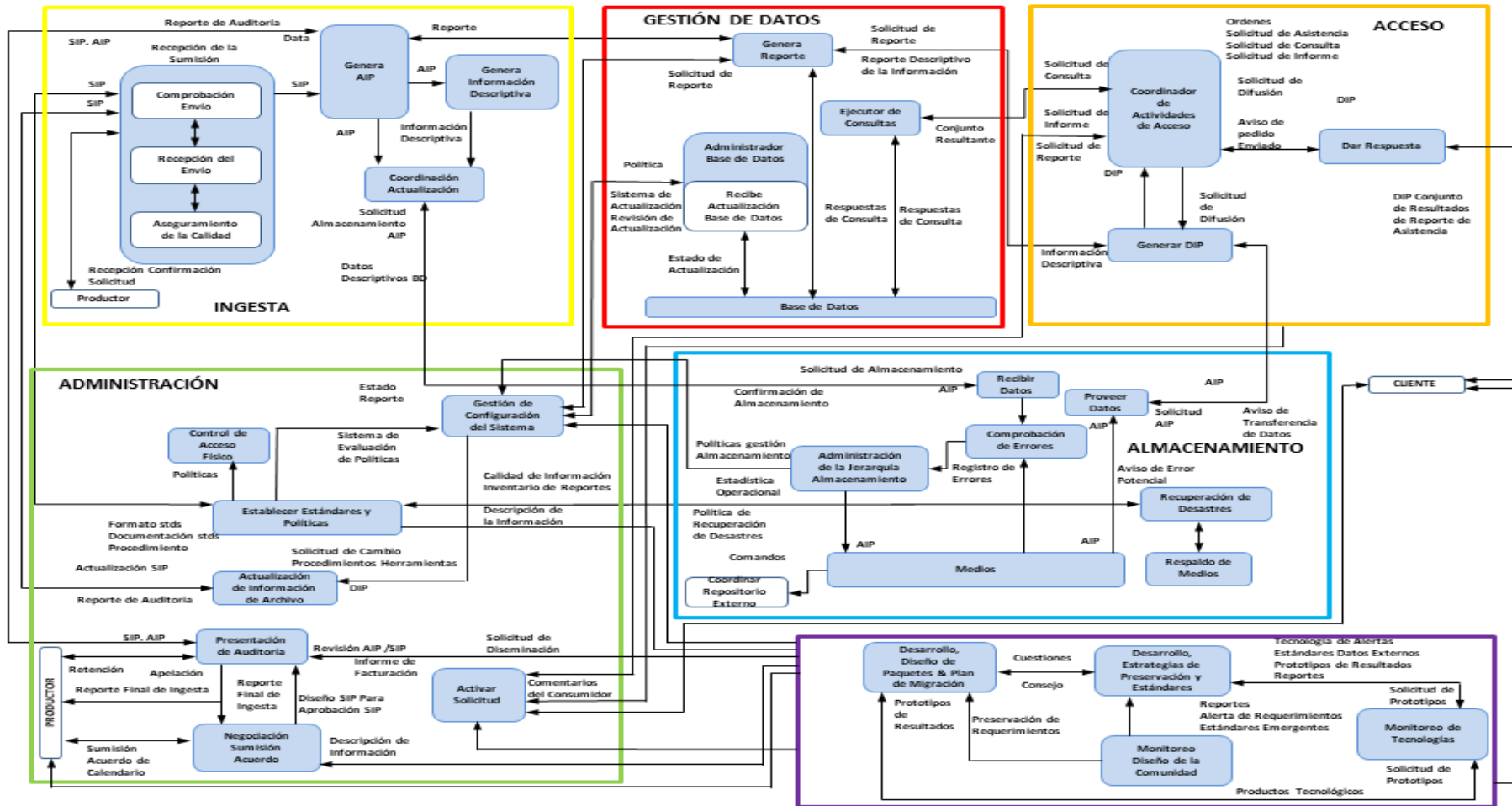


Figura 9-3. Entidades Funcionales PDDL-UESTJV

Realizado por: Verónica Paucar, 2020 (basado en el modelo OAIS)

3.9. Procedimientos Generales

Para cumplir con los objetivos de investigación se indica la secuencia de pasos realizados:

1. Análisis de leyes, reglamentos, normas sobre preservación digital a nivel nacional e internacional.
2. Estudio de los modelos de preservación digital PREDECI, OAIS, DAMM, PREMIS, ámbitos de cada uno características, entidades y especificaciones de cada uno, para seleccionar el modelo que cubra los requerimientos y necesidades del entorno de estudio como se indica en el punto 2.8.5 del capítulo II.
3. Evaluación inicial de la gestión del archivo digital y su entorno de preservación mediante entrevistas y criterios de NÉSTOR para repositorios seguros.
 - a. Realización de entrevistas para determinar el tratamiento del documento digital (ingesta, administración, gestión de datos, almacenamiento, planificación y acceso del documento digital)
 - b. Entrevista para establecer el cumplimiento de políticas, planes, normas y leyes de preservación digital en los documentos digitales, parte administrativa y legal.
 - c. Entrevista para valorar los métodos, estrategias, modelos y nivel de preservación en repositorio.
4. Análisis de los resultados de las entrevistas y evaluación con criterios del catálogo de Néstor para determinar el escenario inicial, determinando las necesidades y requerimientos de la gestión del archivo y repositorio.
5. Elaboración del nuevo modelo de preservación digital a largo plazo de acuerdo a los requerimientos y necesidades analizadas.
 - a. Establecer la comunidad del Modelo.
 - b. Realizar la distribución de los paquetes de información utilizados en la gestión de datos de acuerdo al ciclo de vida digital del documento digital en el modelo.
 - c. Definición de entidades del nuevo modelo.
 - d. Establecer las funciones y procesos necesarias para cada entidad.
 - e. Relacionar las entidades de acuerdo al rol que desempeña dentro del modelo.
 - f. Revisión de las actividades del nuevo modelo de preservación digital a largo plazo.
6. Evaluación del nuevo modelo PDDL-IESTJV. Se aplica nuevamente los criterios de NÉSTOR al modelo creado para verificar si cumple con la característica de repositorio seguro a largo plazo en la gestión del archivo digital con expertos en el tema de seguridad telemática, auditoría de sistemas información.

7. Se realiza la evaluación del modelo con una encuesta de validación de repositorios propuesta por Néstor para expertos, permitiendo valorar y obtener resultados que certifiquen que es un repositorio de preservación a largo plazo, encuesta que se muestra en el Anexo D.
8. Observación y análisis de los resultados de la evaluación del modelo PDDL-IPSTJV, así como del cumplimiento de parámetros que permitan demostrar la mejora de la preservación de documentos digitales a largo plazo de acuerdo al modelo elaborado para entornos de educación superior tecnológica como se muestra en el siguiente capítulo IV.

3.10. Hipótesis

¿La implementación de un Modelo de Preservación de Documentos Digitales mejorará la preservación a largo plazo de documentos digitales?

3.10.1. Identificación de Variables

Variable Independiente: Modelo de Preservación Digital

Variable Dependiente: Mejorar la Preservación de Documentos Digitales a Largo Plazo

3.10.2. Operacionalización Conceptual de Variables

Tabla 3-3. Operacionalización de variables

VARIABLE	TIPO	CONCEPTO
Modelo de Preservación Digital	Variable Independiente	Conjunto de entidades, funciones y procedimientos conceptuales y descriptivas para mejorar la integridad, accesibilidad, disponibilidad y fiabilidad de los documentos digitales usando modelos, estrategias y valoraciones internacionales que permitan almacenar, recuperar, migrar y evaluar mejorando la preservación de estos objetos por largo tiempo.
Mejorar Preservación de Documentos Digitales a Largo Plazo	Variable Dependiente	Disminuir la posibilidad de pérdida de documentos digitales mediante la aplicación de un modelo que mejore el acceso, la integridad y disponibilidad de los mismo a largo plazo.

Realizado por: Verónica Paucar, 2020

3.10.3. Operacionalización metodológica de variables

Tabla 4-3. Operacionalización de variables

VARIABLE	INDICADOR	TÉCNICA	INSTRUMENTO/FUENTE
Modelo de Preservación Digital	Nivel de cumplimiento del Modelo elaborado de Preservación Digital a Largo Plazo como un modelo seguro.	Observación Evaluación Análisis	Criterios de evaluación de repositorios seguros Néstor. Encuesta.
Preservación de Mejorar Documentos Digitales a Largo Plazo	Evaluación de repositorios seguros propuesta por Néstor para expertos para repositorios seguros	Observación y análisis de la evaluación aplicada	Aplicación de encuesta con las Dimensiones de Néstor a expertos en el aseguramiento de la información.

Realizado por: Verónica Paucar, 2020

CAPÍTULO IV

4. RESULTADOS Y DISCUSIÓN

En este apartado se desarrolla la comprobación de las hipótesis y la evaluación del modelo en base al análisis de los escenarios estudiados en otros capítulos.

4.1. Presentación de Resultados

Después de elaborar el modelo de preservación de documentos digitales a largo plazo PDDLPIESTJV se evalúa la importancia de la elaboración del mismo para la preservación de los acervos científicos en un repositorio de almacenamiento de archivos digitales seguros certificados por Working Group, autores de Catalogue of Criteria for Trusted Digital Repositories (2006), que tenga las características de preservación en el tiempo en sus diferentes fases desde el inicio, elaboración y evaluación.

En virtud de estos resultados, se observa las diferencias entre el escenario sin modelo y el escenario con modelo, resultando la inferencia de que el modelo PDDLPIESTJV cumple con un repositorio seguro en base a las necesidades.

4.2. Procesamiento y Análisis

En este proyecto se decide utilizar el software estadístico SPSS de IBM, en su versión: 20.0.0, ya que este programa permite la aplicación de técnicas estadísticas tanto descriptivas (resumen de casos, estadísticas y gráficos descriptivos) como inferenciales (One Way ANOVA), además, este software tiene la capacidad de analizar variables en escala de Likert, lo cual resulta de gran utilidad a la hora de trabajar con instrumentos de evaluación por expertos como Néstor.

Para la comprobación de la hipótesis estadística se utilizó la técnica One Way ANOVA, ya que dicha técnica admite la comparación de la importancia promedio asignada por cada uno de los cuatro expertos, de esta forma fue posible conocer si existen diferencias estadísticamente significativas entre la validación generada por cada experto, o si existe un consenso unánime con respecto a la validación del modelo y su importancia en la preservación de documentos digitales a largo plazo.

4.3. Valoración de la Variable Independiente

4.3.1. Variable Independiente: Modelo de preservación digital a largo plazo

Se procede a evaluar con catálogo de criterios para repositorios digitales confiables, usado en la valoración inicial del estudio mencionado en el punto 3.7.4. del capítulo III, validando el modelo creado para preservar documentos digitales a largo plazo.

4.3.2. Indicador: Nivel de cumplimiento del Modelo elaborado de Preservación Digital a Largo Plazo como un modelo confiable.

Para la evaluación del proceso de preservación del modelo creado PDDL-IPREST se aplica un checklist con el catálogo de criterios para repositorios digitales de confianza, con la finalidad de establecer el cumplimiento del marco organizacional, administración de objetos e infraestructura y seguridad de los archivos digitales en contexto del modelo elaborado.

Tabla 1-4. Lista de cumplimiento de criterios para un repositorio de confianza según Néstor.

A.	MARCO ORGANIZACIONAL	Escenario antes del modelo	Escenario con el modelo
1	El repositorio digital ha definido sus objetivos.		
	El repositorio digital ha desarrollado criterios para la selección de sus objetos digitales.	No Cumple	Cumple
	El repositorio digital asume la responsabilidad de la conservación a largo plazo de la información representada por los objetos digitales	No Cumple	Cumple
	El repositorio digital ha definido su (s) comunidad (es) designada (s)	No Cumple	Cumple
2	El repositorio digital otorga a su comunidad designada el uso correcto información representada por los objetos digitales		
	El repositorio digital garantiza que su comunidad designada pueda acceder a los objetos digitales.	No Cumple	Cumple
	El repositorio digital garantiza que la comunidad designada pueda interpretar los objetos digitales.	No Cumple	Cumple

3	Se evidencia normas legales.		
	Contratos legales entre los productores de información y el repositorio digital.	No Cumple	Cumple
	Al llevar a cabo sus tareas de archivo, el repositorio digital actúa sobre la base de las normas legales.	No Cumple	Cumple
	Con respecto al uso, el repositorio digital actúa sobre la base de los requisitos legales.	No Cumple	Cumple
4	La forma organizativa es adecuada para el repositorio digital.		
	Se asegura la financiación adecuada del repositorio digital.	No Cumple	Cumple
	Se dispone de suficiente personal calificado.	No Cumple	Cumple
	Existen estructuras organizativas apropiadas para el repositorio digital.	No Cumple	Cumple
	El repositorio digital se involucra en la planificación a largo plazo.	No Cumple	
	La continuación de las tareas de conservación está garantizada incluso más allá de la existencia del repositorio digital.	No Cumple	Cumple
5	Se lleva a cabo una gestión de calidad adecuada	No Cumple	Cumple
	Se han definido todos los procesos y responsabilidades.	No Cumple	Cumple
	Se han definido todos los procesos y responsabilidades.	No Cumple	Cumple
	El repositorio digital documenta todos sus elementos en base a un proceso definido.	No Cumple	Cumple
	El repositorio digital reacciona ante cambios sustanciales.	No Cumple	Cumple
B	GESTIÓN DE OBJETOS		
6	El repositorio digital garantiza la integridad de los objetos digitales durante todas las etapas de procesamiento.		

	Ingesta: el repositorio digital garantiza la integridad de los objetos digitales.	No Cumple	Cumple
	Almacenamiento de archivos: el repositorio digital garantiza la integridad de los objetos digitales.	No Cumple	Cumple
	Acceso: el repositorio digital garantiza la integridad de los objetos digitales.	No Cumple	Cumple
7	El repositorio digital garantiza la autenticidad de los objetos digitales durante todas las etapas del procesamiento.		
	Ingesta: el repositorio digital garantiza la autenticidad de los objetos digitales.	No Cumple	Cumple
	Almacenamiento de archivos: el repositorio digital garantiza la autenticidad de los objetos digitales. objetos italianos.	No Cumple	Cumple
	Acceso: el repositorio digital garantiza la autenticidad de los objetos digitales.	No Cumple	Cumple
8	El repositorio digital tiene un plan estratégico para sus medidas técnicas de preservación.		Cumple
9	El repositorio digital acepta objetos digitales de los productores en base a criterios definidos.		
	El repositorio digital especifica sus objetos de transferencia (paquetes de información de envío, SIP).	No Cumple	Cumple
	El repositorio digital identifica qué características de los objetos digitales son importantes para la preservación de la información.	No Cumple	Cumple
	El repositorio digital tiene control técnico de los objetos digitales para llevar a cabo medidas de conservación a largo plazo.	No Cumple	Cumple
10	El almacenamiento de archivos de los objetos digitales se realiza según especificaciones definidas.		
	El repositorio digital define sus objetos de archivo (paquetes de información de archivos, AIP).	No Cumple	Cumple
	El repositorio digital se encarga de transformar los objetos de transferencia (SIP) en objetos de archivo (AIP).	No Cumple	Cumple

	El repositorio digital garantiza el almacenamiento y la legibilidad de los AIP.	No Cumple	Cumple
	El repositorio digital implementa estrategias para la preservación a largo plazo de los AIP.	No Cumple	Cumple
11	El repositorio digital permite el uso de los objetos digitales en base a criterios definidos.		
	El repositorio digital define sus objetos de uso (Paquetes de información de difusión, DIP).	No Cumple	Cumple
	El repositorio digital define sus objetos de uso (Paquetes de información de difusión, DIP).	No Cumple	Cumple
	El repositorio digital asegura la transformación de AIPs en DIPs.	No Cumple	Cumple
12	El sistema de gestión de datos es capaz de proporcionar las funciones de repositorio digital necesarias		
	El repositorio digital identifica de forma única y permanente sus objetos y sus relaciones .	No Cumple	Cumple
	El repositorio digital adquiere metadatos adecuados para la descripción e identificación formal y basada en el contenido de los objetos digitales.	No Cumple	Cumple
	El repositorio digital adquiere metadatos adecuados para la descripción estructural de los objetos digitales.	No Cumple	Cumple
	El repositorio digital adquiere metadatos adecuados para registrar los cambios realizados por el repositorio digital en los objetos digitales.	No Cumple	Cumple
	El repositorio digital adquiere metadatos adecuados para la descripción técnica de los objetos digitales.	No Cumple	Cumple
	El repositorio digital adquiere metadatos adecuados para registrar los derechos y condiciones de uso correspondientes.	No Cumple	Cumple
	Los metadatos asignados a los objetos digitales están garantizados en todo momento.	No Cumple	Cumple
C	Infraestructura y seguridad		
13	La infraestructura de TI es la correcta.		

	La infraestructura de TI incorpora las demandas de la administración de la gestión de objetos.	No Cumple	Cumple
	La infraestructura de TI implementa seguridad del sistema de seguridad de TI.	No Cumple	Cumple
14	La infraestructura protege el repositorio digital y sus objetos digitales.	No Cumple	No Cumple

Fuente: (Nestor, 2006)

Realizado por: Verónica Paucar, 2020

El valor numérico para saber el estádisco es:

- Cumple tiene un valor de 2.
- No cumple tiene un valor de 1.

Análisis para verificar el cumplimiento de los requisitos del Modelo con la Tabla 2-4 se muestra los porcentajes de cumplimiento de requisitos y necesidades según los criterios de NESTOR analizados antes de la elaboración del modelo y después de su elaboración.

Tabla 2-4. Porcentaje de Cumplimiento Modelo PDDL-PIESTJV.

	Escenario Sin Model	Escenario con Model
Percentage de Cumplimiento	0%	96%

Realizado por: Verónica Paucar, 2020.

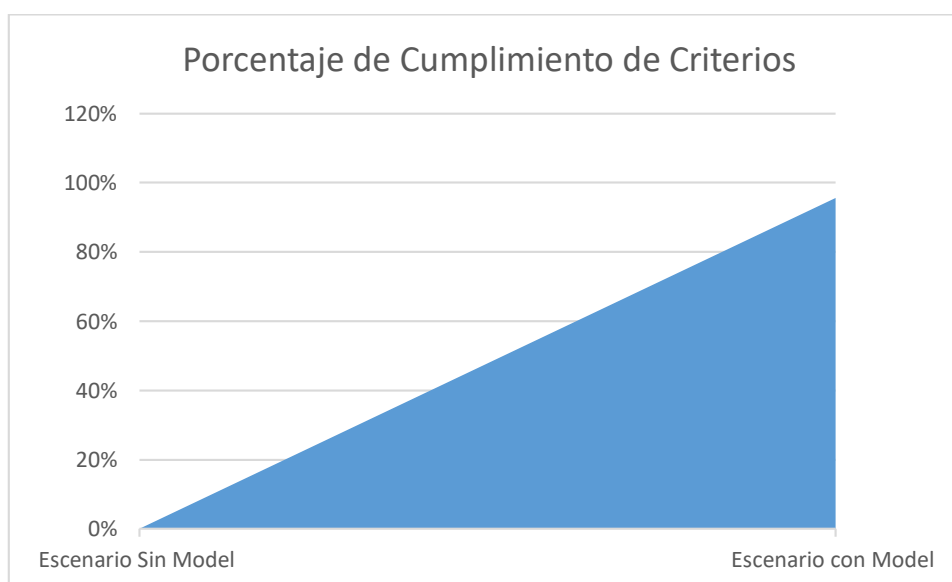


Gráfico 1-4. Nivel de cumplimiento de Criterios del Modelo PDDL-PIESTJV

Realizado por: Verónica Paucar, 2020.

Se realiza el análisis de los checklist, tanto del modelo creado PDDLPIESTJV y el modelo que inicialmente contaba la institución para verificar el cumplimiento de los parámetros de un repositorio seguro, verificando si se logra cubrir las necesidades y requerimientos encontrados inicialmente, los criterios de NÉSTOR muestran el cumplimiento de los parámetros con los que el modelo fue creado. Cada una de sus entidades gestionan el documento digital, sus funciones y procesos aseguran el mismo, desde la ingesta del archivo, añadiendo información descriptiva, realizando respaldos necesarios del archivo digital, gestionando los perfiles de acceso y administración, planificando las políticas, estrategias de preservación a nivel local y de forma externa y así mismo el tipo acceso y disponibilidad del mismo, asegurando nuestro objeto digital en un repositorio de confianza certificado y garantizando la preservación digital a largo plazo en un 96 % del acervo científico versus el estado inicial en el que se le encontró, pasando la institución a un estado de madurez 3 según COBIT 5, como se muestra en la figura 12-2 del capítulo III, ya que se logra estandarizar y documentar los procesos. Con la implementación total del modelo se logrará un estado de madurez mayor.

4.4. Valoración de la Variable Dependiente

4.4.1. Variable Dependiente: Mejorar Preservación de Documentos Digitales a Largo Plazo

4.4.2. Indicador: Evaluación de repositorios seguros propuesta por Néstor para expertos para repositorios seguros

Para valorar si existe una mejora de preservación a largo plazo de los documentos digitales gestionados por el nuevo modelo PDDLPIESTJV, se realiza una encuesta a expertos en procesos de aseguramiento del archivo digital en base un cuestionario de 107 preguntas probatorias relacionadas con repositorios seguros como se indica en el Anexo D, las cuales permitieron validar los procedimientos de preservación del modelo, se utilizó herramientas probabilísticas para valorar los resultados.

4.4.3. Metodología del Indicador de la variable Dependiente

Todo el análisis estadístico, tanto descriptivo como inferencial, se realizó mediante el software estadístico SPSS de IBM, en su versión: 20.0.0.

Como se mencionó en la definición de Néstor, al realizar la encuesta propuesta para su valoración, este instrumento se estructura con base en la escala de Likert para cada uno de los incisos que lo componen. Gracias a que la escala de Likert es de tipo ordinal, ya que sus posibles valores varían entre 1 (insignificante) y 5 (alta), fue posible realizar un análisis estadístico que resuma la información de este tipo de variables y a la vez permita comprobar la hipótesis estadística establecida para la presente investigación.

Con la intención de estudiar la importancia asignada a los diferentes aspectos que debe contener un modelo de preservación digital para preservar archivos digitales por largo tiempo, se realizó un análisis estadístico descriptivo, sectorizando los resultados según las calificaciones planteadas por los cuatro expertos que participaron en la validación del modelo de preservación digital y aseguramiento del documento digital antes mencionado. Dentro de los cuatro expertos constan dos especialistas en Auditoría y dos especialistas en Seguridad Telemática, los cuales se codificaron respectivamente como: aud_1, aud_2, st_1, st_2.

El análisis descriptivo inició con un estudio de casos, de esta forma fue posible obtener información sobre el número de preguntas que fueron respondidas y el porcentaje de información válida dentro de cada evaluación. Posteriormente, se calcularon estadísticas descriptivas como la media, media recortada, mediana, varianza, desviación estándar, valores mínimo y máximo, rango, rango intercuartílico, asimetría y curtosis. Finalmente, se utilizaron técnicas descriptivas gráficas para comparar la importancia asignada por cada uno de los cuatro expertos, dichas técnicas fueron: Gráfico de Barras y Boxplot (Diagrama de caja y bigotes).

4.5. Comprobación Estadística de la Hipótesis

Para comprobar la hipótesis estadística planteada en la presente investigación, se aplicó la técnica estadística inferencial One Way ANOVA (Análisis de varianza de un solo sentido), la cual consiste en comparar la importancia promedio asignada por cada uno de los cuatro expertos, de esta forma es posible conocer si existen diferencias estadísticamente significativas entre la validación generada por cada experto, o si existe un consenso unánime con respecto a la validación del modelo. La hipótesis matemática asociada al ANOVA se define a continuación:

$$H_0: \mu_{aud_1} = \mu_{aud_2} = \mu_{st_1} = \mu_{st_2}$$

$$H_1: \mu_i \neq \mu_j \text{ para al menos un } i \neq j$$

Con base en la expresión matemática de las hipótesis nula y alternativa, se definen las hipótesis estadísticas a ser consideradas en el presente estudio:

H₀: La implementación de un Modelo de Preservación de Documentos Digitales sí mejorará la preservación a largo plazo de documentos digitales.

H₁: La implementación de un Modelo de Preservación de Documentos Digitales no mejorará la preservación a largo plazo de documentos digitales.

4.5.1. Estadística descriptiva

En la Tabla 3-4 se muestra el resumen de casos, donde consta la información sobre el número y porcentaje de: incisos válidos, incisos sin responder (casos perdidos) y total de incisos; con respecto a las evaluaciones presentadas por los cuatro expertos.

Tabla 3-4. Resumen de casos

Experto		Casos					
		Válidos		Perdidos		Total	
		N	%	N	%	N	%
Importancia	<i>aud_1</i>	106	99.1%	1	0.9%	107	100.0%
	<i>aud_2</i>	107	100.0%	0	0.0%	107	100.0%
	<i>st_1</i>	91	85.0%	16	15.0%	107	100.0%
	<i>st_2</i>	106	99.1%	1	0.9%	107	100.0%

Fuente: Herramienta SPSS de IBM, en su versión: 20.0.0.

Realizado por: Verónica Paucar, 2021.

Interpretación:

En el resumen de casos se observó que el porcentaje de preguntas válidas varía entre 85% y 100%, donde el experto con código *st_1* presentó la mayor cantidad de casos perdidos, sumando un total de 16 incisos sin contestar; los demás expertos presentaron un porcentaje de casos perdidos muy bajo, cercano a cero.

En la Tabla 4-4 se muestran estadísticas descriptivas sectorizadas según cada uno de los cuatro expertos, estas medidas descriptivas son: media, media recortada, mediana, varianza, desviación estándar, valores mínimo y máximo, rango, rango intercuartílico, asimetría y curtosis.

Tabla 4-4. Estadísticas descriptivas

Experto		Estadístico	Error estand
	Media	4.45	.067
	95% Intervalo de confianza Media	4.32	
		4.59	
	5% Media recortada	4.50	
	Mediana	5.00	
	Varianza	.479	
aud_1	Desviación estándar	.692	
	Mínimo	3	
	Máximo	5	
	Rango	2	
	Rango intercuartílico	1	
	Asimetría	-.883	.235
	Kurtosis	-.436	.465
	Media	4.08	.067
	95% Intervalo de confianza Media	3.95	
		3.95	
	5% Media recortada	4.09	
Importancia	Mediana	4.00	
	Varianza	.474	
aud_2	Desviación estándar	.688	
	Mínimo	3	
	Máximo	5	
	Rango	2	
	Rango intercuartílico	1	
	Asimetría	-.110	.234
	Kurtosis	-.860	.463
	Media	4.97	.019
	95% Intervalo de confianza Media	4.93	
		4.93	
	5% Media recortada	5.00	
st_1	Mediana	5.00	
	Varianza	.032	
	Desviación estándar	.180	
	Mínimo	4	
	Máximo	5	

	Rango		1	
	Rango intercuartílico		0	
	Asimetría		-5.319	.253
	Kurtosis		26.887	.500
	Media		4.56	.048
	95% Intervalo de confianza Media	4.46	4.46	
		4.46	4.65	
	5% Media recortada		4.56	
	Mediana		5.00	
	Varianza		.249	
st_2	Desviación estándar		.499	
	Mínimo		4	
	Máximo		5	
	Rango		1	
	Rango intercuartílico		1	
	Asimetría		-.231	.235
	Kurtosis		-1.984	.465

Fuente: Herramienta SPSS de IBM, en su versión: 20.0.0.

Realizado por: Verónica Paucar, 2021.

Interpretación:

Al analizar las diferentes medidas descriptivas, se observó que los cuatro expertos establecen una importancia promedio que varía entre 4 y 5, con una mediana de 5 para aquellos expertos con código: aud_1, st_1, st_2 y una mediana de 4 para el experto con código aud_2, siendo estos los valores más altos en la escala de Likert. Además, la escala de importancia otorgada por cada experto se mantuvo en un rango que varía entre 3 y 5, a lo largo de todos los incisos de la validación del modelo de preservación digital.

En el Gráfico 2-4 se presenta un gráfico de barras, el cual permite visualizar la importancia promedio establecida por cada uno de los cuatro expertos.

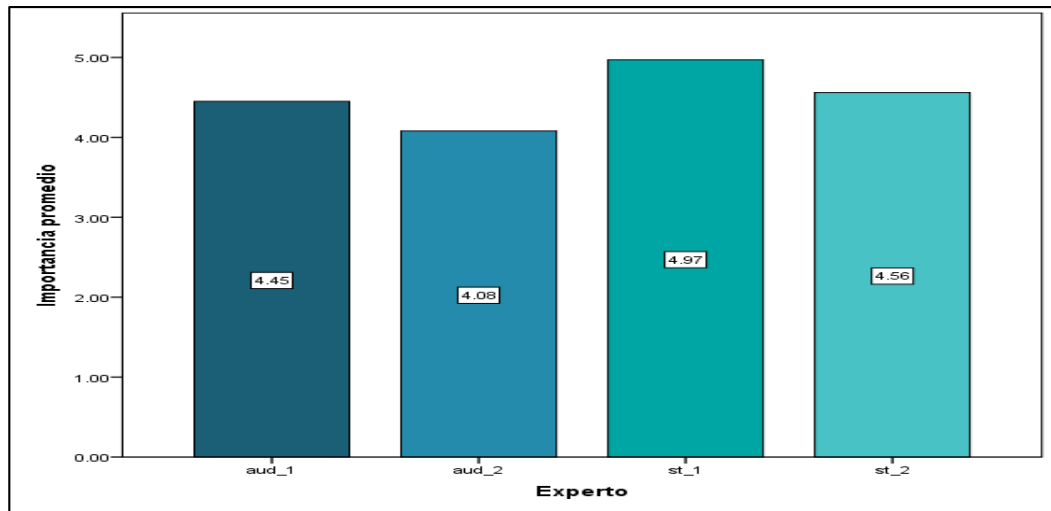


Gráfico 2-4. Comportamiento Importancia Promedio

Realizado por: Verónica Paucar, 2021.

En el Gráfico 3-4 se presenta un boxplot, también conocido como diagrama de caja y bigotes, el cual permite visualizar la realidad presente a lo largo de cada evaluación y además es posible visualizar en qué valores se concentran las calificaciones establecidas por cada experto.

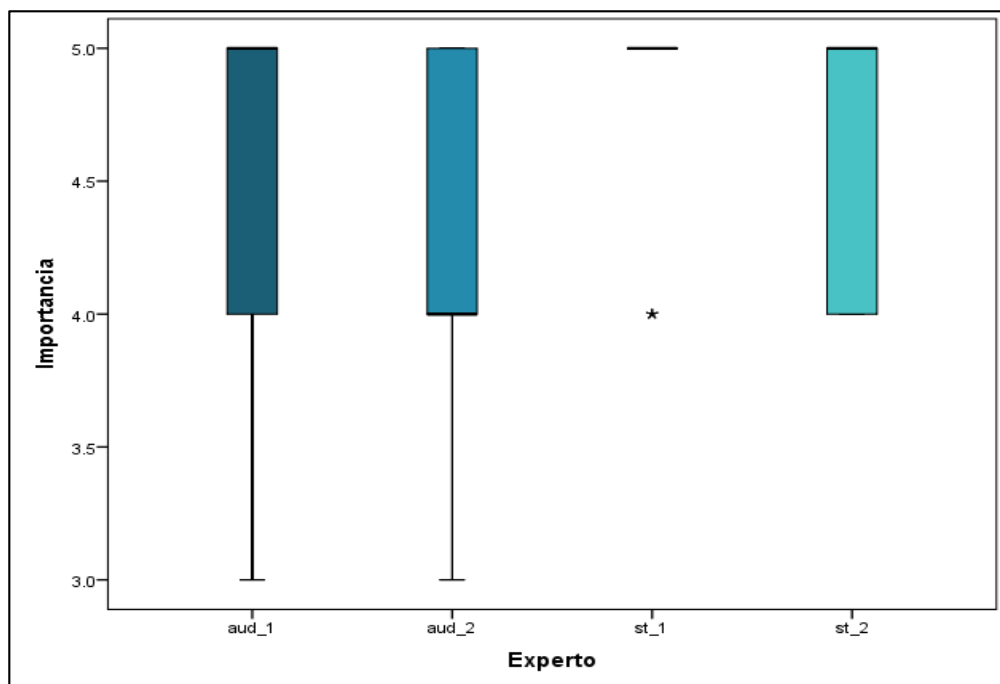


Gráfico 3-4. Boxplot de Importancia según Experto

Realizado por: Verónica Paucar, 2021.

Interpretación de Gráficas: Como se puede observar en el diagrama de barras correspondiente al Gráfico 1-4, la importancia promedio es un tanto mayor para los expertos en Seguridad Telemática, en comparación con los expertos en Auditoría. Además, el boxplot del Gráfico 2-4,

muestra una realidad muy similar para los dos expertos en Auditoría, con valores entre 3 y 5; mientras que los expertos en Seguridad Telemática plantean valores mucho más cercanos a 5.

4.5.2. Estadística Inferencial

Cálculo del ANOVA

La variabilidad de un conjunto de n mediciones es cuantificada por la suma de cuadrados de las desviaciones:

El procedimiento ANOVA divide en partes esta suma de cuadrados de las desviaciones, llamada suma total de cuadrados, cada parte se corresponde con cada una de las variables independientes del experimento. Al dividir cada parte entre una constante apropiada, da como resultado un estimador independiente e insesgado de la varianza poblacional, la varianza del error experimental. Cuando una variable está altamente relacionada con la respuesta, su parte de la suma total de cuadrados (llamada suma de cuadrados de la variable) aumentará. Esta condición puede detectarse si se compara la suma de cuadrados para esa variable con la suma de cuadrados del error, SSE. La prueba estará basada en un estadístico que posee una distribución F y especifica que la hipótesis de que no hay efecto para la variable independiente debe ser rechazada si el valor de F es grande.

Suponga que se desea comparar las medias de dos poblaciones mediante información de dos muestras independientes de tamaños $n_1 = n_2$,

En la Tabla 5-4 se muestran los resultados obtenidos al aplicar la técnica estadística inferencial One Way ANOVA (Análisis de varianza de un solo sentido), la cual consiste en comparar la importancia promedio asignada por cada uno de los cuatro expertos, de esta forma es posible conocer si existen diferencias estadísticamente significativas entre la validación generada por cada experto, o si existe un consenso unánime con respecto a la validación del modelo.

Tabla 5-4. Análisis ANOVA

Importancia					
	Suma de cuadrados	gl	Cuadrado medio	F	p-value
Entre Grupos	38.929	3	12.976	40.661	.000
Dentro Grupos	129.569	406	.319		
Total	168.498	409			

Fuente: Herramienta SPSS de IBM, en su versión: 20.0.0.

Realizado por: Verónica Paucar, 2021.

EXPLICACIÓN DE LA TABLA:

Suma de cuadrados entre los grupos (SCE): La suma de cuadrados entre grupos es una medida estadística que cuantifica la variabilidad presente entre los cuatro grupos de calificaciones, los cuales se forman gracias a la participación de los cuatro expertos. La suma de cuadrados entre grupos se define a continuación:

$$SCE = n_j \sum_{j=1}^4 (\bar{y}_j - \bar{y})^2$$

Donde:

n_j : es el número de preguntas respondidas por cada uno de los cuatro expertos ($j = 1, 2, 3, 4$)

\bar{y}_j : el promedio de calificaciones obtenido por cada uno de los cuatro expertos.

\bar{y} : promedio total de las calificaciones asignadas por los expertos.

En la Tabla 3-4 se muestra una suma de cuadrados entre los grupos de 38.929, este valor representa la variabilidad presente entre los cuatro grupos de calificaciones.

Suma de cuadrados dentro de los grupos (SCI): La suma de cuadrados dentro de los grupos es una medida estadística que cuantifica la variabilidad presente intra-grupos, es decir dentro de los cuatro grupos formados. La suma de cuadrados intra-grupos se define a continuación:

$$SCI = \sum_{j=1}^4 \sum_{i=1}^{n_j} (y_{ij} - \bar{y}_j)^2$$

Donde:

n_j : es el número de preguntas respondidas por cada uno de los cuatro expertos ($j = 1, 2, 3, 4$)

y_{ij} : la i -ésima calificación en el j -ésimo grupo.

\bar{y}_j : el promedio de calificaciones obtenido por cada uno de los cuatro expertos.

En la Tabla 3-4 se muestra una suma de cuadrados dentro de los grupos de 129.569, este valor representa la variabilidad intra-grupos, es decir dentro de los cuatro grupos de calificaciones.

Suma de cuadrados total (SCT): La suma de cuadrados total es una medida estadística que cuantifica la variabilidad de un conjunto de mediciones de tamaño n. La suma de cuadrados total se define como la suma de cuadrados de las desviaciones de la media (promedio):

$$\text{SCT} = \sum_{i=1}^n (y_i - \bar{y})^2$$

Donde:

y_i : cada una de las $n = 410$ calificaciones asignadas, en conjunto, por los cuatro expertos.

\bar{y} : promedio total de las calificaciones asignadas por los expertos ($\bar{y} = 4.515$).

Además, la suma de cuadrados total es igual a la suma de cuadrados entre los grupos más la suma de cuadrados dentro de los grupos, es decir, se cumple que:

$$\text{SCT} = \text{SCE} + \text{SCI}$$

En la Tabla 3-4 se muestra una suma de cuadrados total de 168.498, este valor representa la variabilidad presente a lo largo de todas las calificaciones asignadas, en conjunto, por los cuatro expertos.

Grados de libertad entre los grupos: Los grados de libertad entre grupos se definen como el número de grupos menos uno, en este caso el número de grupos es 4, por lo tanto, los grados de libertad entre grupos tiene un valor de 3.

Grados de libertad dentro de los grupos: Los grados de libertad dentro de los grupos se definen como el número de calificaciones obtenidas menos el número de grupos, en este caso el número de calificaciones de los expertos suman un total de 410 respuestas y el número de grupos es 4, por lo que los grados de libertad dentro de los grupos tiene un valor de 406.

Grados de libertad total: Los grados de libertad total se definen como la suma de los grados de libertad entre los grupos (3) más los grados de libertad dentro de los grupos (406), por lo tanto, los grados de libertad total tienen un valor de 409.

Cuadrado medio entre los grupos (MCE): El cuadrado medio entre grupos se define como la suma de cuadrados entre grupos dividida por los grados de libertad entre los grupos:

$$MCE = \frac{SCE}{3} = \frac{38.929}{3} = 12.976$$

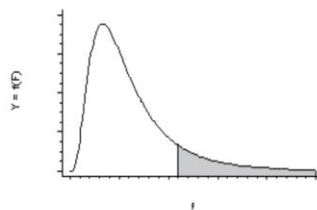
Cuadrado medio dentro de los grupos (MCI): El cuadrado medio dentro de los grupos se define como la suma de cuadrados dentro de los grupos dividida por los grados de libertad dentro de los grupos:

$$MCI = \frac{SCI}{406} = \frac{129.569}{406} = 0.319$$

Estadístico de prueba (f): f es el estadístico de prueba que, como su nombre lo indica, permite probar la hipótesis estadística asociada al ANOVA. Este estadístico sigue una distribución F (Fisher-Snedecor). El estadístico de prueba f se define como la división entre el cuadrado medio entre grupos y el cuadrado medio intra-grupos:

$$f = \frac{MCE}{MCI} = \frac{12.976}{0.319} = 40.661$$

Estadístico teórico (f_{α}): El estadístico teórico f_{α} se define como el cuantil de la distribución F de Fisher-Snedecor que deja una probabilidad (área bajo la curva) igual a alfa. Para la presente investigación, el estadístico teórico se establece con 3 grados de libertad en el numerador, 406 grados de libertad en el denominador y un nivel de significancia alfa igual a 0.05. Dicho estadístico se obtiene mediante una tabla del área bajo la curva de F:



Area bajo la curva de F, por encima de un valor de F y K-1 gl (columnas) y N-K gl (filas). (Elaboración propia)													
N-k	Ns	k-1											
		1	2	3	4	5	6	7	8	9	10	11	12
100	0,01	6,8953	4,8239	3,9837	3,5127	3,2059	2,9877	2,8233	2,6943	2,5898	2,5033	2,4302	2,3676
	0,05	3,9362	3,0873	2,6955	2,4626	2,3053	2,1906	2,1025	2,0323	1,9748	1,9267	1,8857	1,8503
	0,10	2,7564	2,3564	2,1394	2,0019	1,9057	1,8339	1,7778	1,7324	1,6949	1,6632	1,6360	1,6124
200	0,01	6,7633	4,7128	3,8810	3,4143	3,1100	2,8933	2,7298	2,6012	2,4971	2,4106	2,3375	2,2747
	0,05	3,8884	3,0411	2,6498	2,4168	2,2592	2,1441	2,0556	1,9849	1,9269	1,8783	1,8368	1,8008
	0,10	2,7308	2,3293	2,1114	1,9732	1,8763	1,8038	1,7470	1,7011	1,6630	1,6308	1,6031	1,5789
300	0,01	6,7201	4,6766	3,8475	3,3822	3,0787	2,8625	2,6993	2,5709	2,4668	2,3804	2,3073	2,2444
	0,05	3,8726	3,0258	2,6347	2,4017	2,2441	2,1288	2,0402	1,9693	1,9112	1,8623	1,8206	1,7845
	0,10	2,7223	2,3203	2,1021	1,9637	1,8666	1,7938	1,7369	1,6908	1,6525	1,6201	1,5922	1,5679
400	0,01	6,6987	4,6586	3,8309	3,3664	3,0632	2,8472	2,6842	2,5559	2,4518	2,3654	2,2923	2,2294
	0,05	3,8648	3,0183	2,6272	2,3943	2,2366	2,1212	2,0325	1,9616	1,9033	1,8544	1,8126	1,7764
	0,10	2,7181	2,3159	2,0975	1,9590	1,8617	1,7889	1,7318	1,6856	1,6472	1,6147	1,5867	1,5623
500	0,01	6,6858	4,6479	3,8210	3,3569	3,0540	2,8381	2,6751	2,5469	2,4429	2,3565	2,2833	2,2204
	0,05	3,8601	3,0138	2,6227	2,3898	2,2320	2,1167	2,0279	1,9569	1,8986	1,8496	1,8078	1,7716
	0,10	2,7156	2,3132	2,0948	1,9561	1,8588	1,7859	1,7288	1,6825	1,6441	1,6115	1,5835	1,5590
	0,01	6,6773	4,6407	3,8144	3,3506	3,0478	2,8321	2,6691	2,5409	2,4369	2,3505	2,2773	2,2144

Figura 1-4: Tabla Area bajo la Curva de una Distribución F
Fuente: (Viedma C. d., 2009)

De esta forma es posible identificar un estadístico teórico $f_{0,05}$ con un valor aproximado de 2.6272

Nivel de significancia alfa: El nivel de significancia alfa (α) se define como la probabilidad de rechazar la hipótesis nula cuando esta es verdadera (Error de tipo I), en estadística se suele utilizar como estándar un nivel de significancia alfa igual a 0.05, el cual se traduce en un 5% de riesgo al concluir que sí existen diferencias significativas, cuando éstas en realidad no existen.

Valor p: El valor p, también conocido como p-value se define como la probabilidad de que la distribución F de Fisher-Snedecor tome valores menores o iguales al estadístico de prueba:

$$p = P(F \leq f) = 0.000$$

4.6. Interpretación y Análisis

Finalmente, el estudio de la hipótesis estadística mediante la técnica One Way ANOVA, permitió obtener un p-value (valor p) de aproximadamente cero, por lo que al fijar un nivel de significancia estadística alfa igual a 0.05 (5%) no se rechaza la hipótesis nula (H_0), por lo tanto, es posible concluir con una confianza estadística del 95% que la implementación de un Modelo de Preservación de Documentos Digitales sí mejora la preservación a largo plazo de documentos digitales.

CONCLUSIONES

- Se ha estudiado los diferentes modelos propuestos para preservación digital de documentos a largo plazo, analizando cada uno de ellos y se observa que el modelo OAIS cumple con el 92% cumpliendo con un grado de efectividad en seguridad de la información y las mejores estrategias de preservación, sirviendo de base para la elaboración del modelo propuesto en entornos de educación superior tecnológicos y que ayude al aseguramiento y gestión del documento digital.
- Al analizar las leyes, normas, reglas vigentes a nivel nacional sobre preservación digital de documentos, se puede citar que no poseen el alcance necesario para preservar los acervos científicos a pesar de estar obligadas por la legislación. La falta de normativas, políticas ponen en riesgo el patrimonio digital intelectual de las instituciones de educación Superior Tecnológicas.
- La aplicación de Criterios de Néstor permitió medir el nivel de integridad, disponibilidad y accesibilidad de la producción académica-científica de la institución, identificando las necesidades y requerimientos para la elaboración del modelo de preservación a largo plazo, verificando que existe una total falta de un proceso reconocible.
- La elaboración del modelo conceptual de preservación digital a largo plazo de documentos digitales para Institutos Superiores Tecnológicos, mejora en el 96% los procesos de preservación a largo plazo sobre el escenario inicial, teniendo como principal tarea el aseguramiento de los productos científicos digitales por medio de estrategias, técnicas y lineamientos preservación, ya que es el patrimonio y evidencia de la vida académica de la institución y del aporte a la comunidad y al país.
- La evaluación de Néstor para certificar repositorios por expertos, permite establecer la importancia del modelo PDDL-IESTJV, de acuerdo a las calificaciones otorgadas por cada especialista la confianza estadística es del 95 %, permitiendo comprobar que la implementación del modelo propuesto de Preservación de Documentos Digitales si mejora la preservación a largo plazo de documentos digitales.

RECOMENDACIONES

- Al momento de seleccionar un modelo se debe evaluar las necesidades y el entorno al que se va aplicar, que se adaptable, expandible y cumpla con estándares de preservación internacionales que faciliten al momento de decidir cuál es el mejor modelo que cubra las necesidades de la organización.
- Para no incurrir en faltas a ley se debe capacitar y analizar las leyes, reglamentos estatutos inmersos a nivel institucional y de país sobre preservación digital y así planificar un modelo que garantice su legalidad y el aseguramiento de su archivo digital.
- Para analizar las necesidades y requerimientos de los repositorios de preservación a largo plazo existen diferentes metodologías y herramientas que sirven de apoyo en la administración y análisis de riesgos a los que se expone una institución.
- Se recomienda el modelo de preservación de documentos digitales a largo plazo PDDLPIESTJV para institutos superiores tecnológicos, para mejorar los niveles de preservación. Este puede ser actualizado o adaptado de acuerdo a las necesidades de cada institución, es primordial iniciar estos procesos desde la creación del archivo digital.
- Un modelo de preservación tiene que ser evaluado constantemente de acuerdo a normas y criterios internacionales que certifiquen repositorios seguros y la gestión del objeto digital con la finalidad de seguir efectuando reajuste en las funcionalidades del modelo y garantizar la preservación.
- Para posteriores investigaciones que deseen tomar la presente como referente, se pide complementar el modelo como distribuido, con protocolos de aplicación distribuida, monitoreo, replicación.

BIBLIOGRAFÍA

Ali, Z. (2018). *The Science of Blockchain Algorithms*. Mammoth Technologies.

Álvarez-Wong, B. I. (2017). Los repositorios digitales para la conservación. Un acercamiento a la preservación digital a largo plazo. *48(2)*, 15-22. Obtenido de <http://www.redalyc.org/pdf/1814/181454540003.pdf>

Anne, Thurston. (Septiembre de 2012). Digitization and Prevension : Global Opportunites and Cultural Challenges. *International conference on permanent accesse to digital documentary heritage* (págs. 31-47). Vancouver, UBC. Canada: Luciana Duranti and Elizabeth.

Antonia Salvador Benítez, Antonio Ángel Ruíz Rodríguez. (2005). Metadatos para la Preservación de Colecciones Digitales. *Cuadernos de Documentación Multimedia*.

Aquino. (22 de Noviembre de 2016). *Retos de la preservación digital*. Obtenido de Retos de la preservación digital.: <http://www.infotecarios.com/>

Asamblea Nacional del Ecuador. (10 de Marzo de 2014). *Ley del Sistema Nacional de Registro de Datos Públicos*. Obtenido de www.lexis.com.ec: <https://www.telecomunicaciones.gob.ec/wp-content/uploads/2016/04/Ley-Organica-del-Sistema-Nacional-de-Registro-de-Datos-Publicos.pdf>

Beagrie, N., & Jones, M. (diciembre de 2008). *Preservation Management of Digital Materials: The Handbook*. . Obtenido de <http://www.dpconline.org/graphics/>

Caplan, P. (febrero de 2009). Entender PREMIS. *Library of Congress Network Development and MARC Standards Office*. Obtenido de Entender PREMIS.

Dante, A. O. (2012). Preservación Digital: problemáticas, estrategias, metadatos, infraestructura y políticas. *STBD-SI-DGB-UNAM*, 1.

- De Giusti, M. R. (2014). *Una metodología de evaluación de repositorios digitales para asegurar la preservación en el tiempo y el acceso a los contenidos*. Obtenido de <http://sedici.unlp.edu.ar/handle/10915/43157>
- Donaldson, D. R. (2020). Certification Information on Trustworthy Digital Repository Websites: A Content Analysis. *ResearchGate*.
- Espinel, V. A. (2015). *Norma Técnica de Gestión Documental y Archivo*. Ecuador: Secretaria Nacional de la Administración Pública.
- Espinel, V. A. (15 de Junio de 2016). *NORMA DE GESTION DOCUMENTAL PARA ENTIDADES DE ADMINISTRACION PUBLICA*. Obtenido de http://www.puertodemanta.gob.ec/wp-content/uploads/2016/12/6.-NORMA_DE_GESTION_DOCUMENTAL_PARA_ENTIDADES_DE_ADMINISTRACION_PUBLICA.pdf
- ESTADO, U. A. (2016). *PLAN DE PRESERVACION DIGITAL A LARGO PLAZO DEL SISTEMA INTEGRADO DE CONSERVACION DOCUMENTAL*. Colombia. Obtenido de PLAN DE PRESERVACION DIGITAL A LARGO PLAZO.
- Giménez, V. C. (2014). Criterios ISO para la preservación digital de los documentos de archivo. *Universitat Politècnica de València, España*, 135-150.
- Hong, N. P. (2012). Where does it go from here? The place of software in digital repositories. *The 7th International Conference on Open Repositories, Edinburgh, United Kingdom*.
- Huerta, A. V. (2004). *Códigos de buenas prácticas de seguridad UNE-ISO/IEC 17799*. Valencia: Grupo S2.
- IF GOVERNANCE INSTITUTE, C. (15 de Enero de 2019). *ISACA*. Obtenido de ISACA: <http://www.isaca.org/Knowledge-Center/cobit/Documents/cobitT4.1spanish.pdf>
- ISACA. (5 de Noviembre de 2019). *Un Marco de Negocio Para el Gobierno y la Gestión de las TIC en las Empresas*. Obtenido de Un Marco de Negocio Para el Gobierno y la Gestión de las TIC en las empresas: https://issuu.com/opvallar/docs/cobit_5_-_framework_spanish

José Ramón Cruz Mundet & Carmen Díez Carrera. (2016). Sistema de Información de Archivo Abierto (OAIS): luces y sombras de un modelo de referencia. *ScienceDirect*, 221-247.

Leija Román, D. A. (2017). *Preservación digital distribuida y la colaboración interinstitucional*. Barcelona: Facultad de Biblioteconomía y Documentación.

Molina Fernando y Rodríguez Glen . (2017). Model for digital evidence preservation in criminal research institutions - PREDECI. *International Journal of Electronic Security and Digital Forensics*, 150.

Nestor, w. G.-C. (Diciembre de 2006). *Catalogue of Criteria for Trusted Digital Repositories*. Obtenido de Catalogue of Criteria for Trusted Digital Repositories.

NORMA TÉCNICA DE GESTIÓN DOCUMENTAL Y ARCHIVO. (s.f.). Obtenido de http://rauec.gob.ec/images/NORMATIVA/norma_tecnica.pdf

Preservica. (Julio de 2013). *Digital Preservation Maturity Model*. Obtenido de *Tessella*. Obtenido de <http://preservica.com/download/852>

Ravelo, G. (2015). *Propuesta de requisitos para la valoración de riesgos de preservación en repositorios digitales*. Cuba: Universidad de La Habana.

Secretaría General de la República Ecuador, 2. (24 de Noviembre de 2019). *LEY ORGANICA DE EDUCACION SUPERIOR, LOES*. Obtenido de LEY ORGANICA DE EDUCACION SUPERIOR, LOES: <https://procuraduria.utpl.edu.ec/sitios/documentos/NormativasPublicas/Ley%20Org%C3%A1nica%20de%20Educaci%C3%B3n%20Superior%20Codificada.pdf>

SECRETARIO GENERAL DE LA PRESIDENCIA DE LA REPUBLICA . (10 de 04 de 2019). *REGLA TÉCNICA NACIONAL PARA LA ORGANIZACIÓN Y MANTENIMIENTO DE LOS ARCHIVOS PÚBLICOS*. Obtenido de <https://www.aea.ec/wp-content/uploads/2019/05/REGLA-TECNICA-NACIONAL.pdf>

Shameli-Sendi, A. A.-B. (2016). Taxonomy of information security risk assessment (ISRA). *Computers & Security* 57, 14-30.

- SINCHE. (2017). *SISTEMA INTEGRADO DE CONSERVACIÓN*. Obtenido de https://www.sinchi.org.co/files/DOCUMENTOS%20INSTITUCIONALES/Instrumentos%20archivisticos/SISTEMA%20INTEGRADO%20DE%20CONSERVACION_SINCHI.pdf
- Térmens, M. (2009). Perspectivas para la sostenibilidad y la preservación de los repositorios institucionales. *Presentación. 4as Jornadas OS-Repositorios. Barcelona, .*
- Tessalla. (2013). *Digital Preservation Maturity Model - White Paper*. Obtenido de Digital Preservation Maturity Model - White Paper.: https://preservica.com/uploads/resources/Preservica-White-Paper-Maturity-Model-2014_NEW.pdf
- The Consultative Committee for Space Data Systems. (2002). *MODEL FOR AN OPEN ARCHIVAL INFORMATION SYSTEM (OAIS)*. Obtenido de <http://public.ccsds.org/publications/archive/650x0b1s.pdf>
- UNESCO. (2003). Directrices para la Preservación del Patrimonio Digital. *National Library of Australia*, 12. Obtenido de <http://unesdoc.unesco.org/images/0013/001300/130071s.pdf>
- Universidad de la Plata. (s.f.). Bibliotecas y Repositorios Digitales. *Tecnología y Aplicaciones: la preservación en el RI*. Argentina, Argentina: SEDICI.
- Viedma, C. d. (2009). *Complutense, S. A*. Madrid: Complutense, S. A. .
- Viedma, C. d. (2009). *Estadística descriptiva e inferencial y una introducción al método científico*. Madrid: Complutense, S. A. .
- Voutssas, J. (2010). Preservación documental digital. *Centro Universitario de Investigaciones Bibliotecológicas de la UNAM*, 127-155.

ANEXO A: Encuesta Inicial Gestión de Documento Digital

En este anexo se detalla la entrevista inicial que se realizó a los encargados de la gestión del archivo digital en el Instituto Superior Tecnológico Juan de Velasco.

El objetivo de estas entrevistas es revisar los casos de estudio de acuerdo a los procesos de lleva cada uno de los entrevistados el archivo digital a preservar y ver las normas que siguen para salvaguardarlos.

Datos de las entrevistas:

Fuente de los datos: Casos de Estudio

Departamento de Secretaria – Secretaria

Coordinación Académica – Director de la Unidad

Departamento TI – Encargado de Servidores

ENTREVISTA INICIAL - SECRETARIA

- Las tesis de los estudiantes se procesan como un archivo digital, ¿en qué tipo de soporte guardan la información?
- ¿Cuál es el formato en el que se reciben y guardan las tesis?
- ¿Aplican algún tipo de normativa institucional o nacional para guardar la información en el archivo digital? Especifique:
- ¿Las personas que se encargan de la custodia del archivo digital, poseen el perfil adecuado?
- ¿Generan algún tipo de metadatos al momento de archivar una producción académica?
- Cuando alguien pide acceso a las investigaciones, ¿pueden hacerlo? ¿Siguen un protocolo o proceso?

ANEXO B: Encuesta Inicial Lineamientos Gestión de Documento Digital

COORDINACIÓN ACADÉMICA

- ¿Tienen políticas internas sobre preservación de documentos digitales establecidas?
- ¿Posee conocimiento de algún tipo de normativa institucional o nacional para guardar la información digital por varios años? Indique.
- ¿El personal que está a cargo de la custodia de la producción científica posee el perfil adecuado para su cargo?
- Existe difusión de reglas en la gestión de preservar archivos entre empleados, docentes, administrativos y alumnos.

ANEXO C: Encuesta Inicial de Procesos de Preservación del Repositorio

ENCARGADO DE SERVIDORES

- ¿El instituto cuenta con un repositorio digital donde se gestione la producción académica – científica?
- ¿Tiene conocimiento de preservación digital a largo plazo de documentos digitales?
- ¿Emplea preservación digital en el patrimonio académico-científico de la institución?
- ¿Cree que son apropiados los métodos utilizados en la institución para preservar la producción académica-científica?
- ¿Los productos académicos–científicos de la institución son publicitados de forma que este accesible a la comunidad?
- ¿Conoce usted sobre la Norma Técnica de Gestión Documental y Archivo que las instituciones públicas aplicar?
- ¿La institución Educativa posee Plan de Preservación a Largo Plazo de la producción académica–científica?

ANEXO D: Encuesta de Validación del Modelo a Expertos

ENCUESTA DE VALIDACIÓN PARA EXPERTOS

DATOS DEL EXPERTO EVALUADOR

Título profesional más alto: Magister

Área del conocimiento: Seguridad Telemática

Fecha: 19/05/2021

Objetivo: Conocer la pertinencia y objetividad del instrumento de validación de la estrategia de implementación de un modelo de preservación de documentos digitales a largo para institutos de educación superior tecnológicos.

Instrucciones: Escriba su valoración a lado de cada criterio por pregunta, se debe recordar que repositorio se refiere al modelo de preservación elaborado.

Agradecemos sus respuestas, las cuales son fundamentales para el proceso validación y mejoramiento de preservación a largo plazo de documentos digitales. La encuesta es anónima y solo será utilizada para los fines indicados.

NIVEL DE IMPORTANCIA DE LOS ASPECTOS QUE DEBE CONTENER UN MODELO DE PRESERVACIÓN DIGITAL PARA PRESERVAR ARCHIVOS DIGITALES POR LARGO TIEMPO

ESCALA DE IMPORTANCIA

5.- ALTA 4.- INTERMEDIA 3.- MODERADA 2.- BAJA 1.- INSIGNIFICANTE

A	INFRAESTRUCTURA ORGANIZACIONAL	Importancia
i	GOBERNABILIDAD Y VIABILIDAD ORGANIZATIVA	
P111	¿El repositorio tiene una misión que refleja un compromiso con la preservación gestión y acceso a la información digital en el largo plazo?	5
P112	¿El repositorio dispone un plan estratégico de preservación que define el enfoque que tiene el repositorio en el apoyo a largo plazo de su misión?	5

P113	¿El repositorio dispone de una política de colección u otro documento que especifica el tipo de información a preservar, almacenar, administrar y proporcionar acceso?	5
ii ESTRUCTURA ORGANIZACIONAL Y PERSONAL		
P121	¿El repositorio tiene identificado y establecido las tareas que debe realizar?	5
P122	¿El repositorio dispone del número adecuado de personal para apoyar todas las funciones y servicios?	5
P123	¿El repositorio tiene un programa de desarrollo profesional que ofrece personal desarrollar habilidades y conocimientos?	5
iii MARCO DE RENDICIÓN DE CUENTAS Y LA POLÍTICA DE PRESERVACIÓN PROCEDIMIENTOS		
P131	¿El repositorio ha definido su comunidad y tiene definiciones apropiadamente accesibles?	5
P132	¿El repositorio dispone de políticas de preservación propias para cumplir su Plan estratégico de preservación?	5
P133	¿El repositorio dispone de un historial documentado de los cambios en sus operaciones, procedimientos, software y hardware?	5
P134	¿El repositorio dispone de herramientas de transparencia y rendición de cuentas en todas las acciones apoyando la operación y administración del repositorio que afectan la preservación de contenido digital en el tiempo?	5
P135	¿El repositorio dispone de funciones para definir, recoger, rastrear y proporcionar información de integridad?	5
P136	¿El repositorio dispone de funciones para comprometerse a un horario regular de autoevaluación y certificación externa?	5
iv SOSTENIBILIDAD FINANCIERA		
P141	El repositorio dispone de procesos de planificación y presupuesto a corto y largo plazo.	5
P142	¿El repositorio dispone información sobre prácticas financieras y procedimientos que son transparentes, cumple con las normas de contabilidad y permite ser auditados por terceros conforme a los requisitos legales territoriales?	5
P143	¿El repositorio tiene un proceso continuo para analizar e informar sobre riesgos financieros, beneficios, inversión y gastos (incluyendo licencias, activos y pasivos)?	5

v	CONTRATOS, LICENCIAS Y PASIVOS	
P151	¿El repositorio dispone de contratos apropiados o acuerdos para materiales digitales que administra, preserva, o a los que proporciona acceso?	5
P152	¿El repositorio dispone rastrear y administrar los derechos de propiedad intelectual y dispone restricciones sobre el uso del contenido del repositorio según lo requerido por el contrato de depósito o licencia?	5
B	ADMINISTRACIÓN DE OBJETOS DIGITALES	
vi	INGERIR: ADQUISICIÓN DE CONTENIDOS	
P211	¿El repositorio dispone de un procedimiento para identificar la información de contenido y las propiedades de la información que preservará el repositorio?	5
P212	¿El repositorio dispone específica y claramente la información que necesita para ser asociado con contenido específico de la información en el momento de su depósito?	5
P213	¿El repositorio dispone de las especificaciones adecuadas que permite el reconocimiento y análisis de los SIP?	5
P214	¿El repositorio dispone de mecanismos para verificar adecuadamente la identidad del productor de todos los materiales?	5
P215	¿El repositorio dispone de un control suficiente sobre los objetos digitales para preservarlos?	5
P216	¿El repositorio dispone de registros contemporáneos de acciones y procesos de administración que son relevantes para la adquisición de contenidos?	5
vii	INGERIR: CREACIÓN DE LA AIP	
P221	¿El repositorio tiene para cada AIP o clase de AIPs preservada por el repositorio una definición asociada que es adecuada para el análisis de la AIP y apto para necesidades de conservación a largo plazo?	5
P222	¿El repositorio dispone de una descripción de cómo se construyen AIPs?	5
P223	¿El repositorio dispone documentar la disposición final de todos los DIP's?	5

P224	¿El repositorio tiene y utiliza una estándar que genera identificadores persistentes, únicos para todos AIPs?	5
P225	¿El repositorio tiene acceso a las herramientas necesarias y los recursos para proporcionar información de representación autorizada para todos los objetos digitales que contiene?	5
P226	¿El repositorio ha documentado los procesos para adquirir información de descripción de preservación (PDI) por su contenido e información asociada?	5
P227	¿El repositorio se asegura de que la información de contenido de las AIPs es comprensible para su comunidad designada en el momento de la creación?	5
P228	¿El repositorio verifica cada AIP para integridad y exactitud en el momento que se crea?	5
P229	El repositorio proporciona un mecanismo independiente para verificar la integridad de la colección/contenido del repositorio?	5
viii	PLANIFICACIÓN DE PRESERVACIÓN	
P231	¿El repositorio ha documentado estrategias de preservación correspondientes a sus participaciones?	5
P232	¿El repositorio dispone de mecanismos para monitorear el entorno de su preservación?	5
P233	¿El repositorio dispone de mecanismos para cambiar sus planes de preservación como resultado de sus actividades de vigilancia?	5
P234	¿El repositorio dispone proporcionar evidencia de la efectividad de sus actividades de preservación?	5
ix	PRESERVACIÓN DEL AIP	
P241	¿El repositorio dispone de las especificaciones de cómo las AIPs se almacenan hasta el nivel de bits?	5
P242	¿El repositorio dispone de registros contemporáneos de acciones y procesos de administración que son relevantes para el almacenamiento y preservación de las AIPs?	5
x	GESTIÓN DE LA INFORMACIÓN	
P251	¿El repositorio especifica los requisitos de información mínima para permitir a la comunidad designada descubrir e identificar los materiales de interés?	5

P252	¿El repositorio permite crear información descriptiva y asegurar de que está asociada con el AIP?	5
P253	¿El repositorio dispone de vínculos bidireccionales entre cada AIP y su información descriptiva?	5
xi	GESTIÓN DE ACCESO	
P261	¿El repositorio verifica el cumplimiento de las directivas de acceso?	5
P262	¿El repositorio dispone seguir las políticas y procedimientos que permiten la difusión de objetos digitales que son trazables a los originales, con evidencias que apoyen su autenticidad?	5
C	GESTIÓN DE INFRAESTRUCTURA Y RIESGO PARA LA SEGURIDAD	5
xii	GESTIÓN DE RIESGOS DE LA INFRAESTRUCTURA TÉCNICA	
P311	¿El repositorio emplea tecnología de notificación de vigilancia tecnológica?	5
P312	¿El repositorio dispone de suficiente hardware y software de soporte para la de copia de seguridad del contenido del repositorio y seguimiento de las funciones del repositorio?	5
P313	¿El repositorio dispone de mecanismos eficaces para detectar la pérdida o corrupción de bit?	5
P314	El repositorio permite registrar y reaccionar a la disponibilidad de nuevas actualizaciones de seguridad basada en una evaluación del riesgo / beneficio?	5
P315	¿El repositorio ha definido procesos de cambio de medio de almacenamiento (por ejemplo, refrescar, migrar)?	5
P316	¿El repositorio tiene identificado y documentado los procesos críticos que afectan su capacidad para cumplir con sus responsabilidades obligatorias?	5
P317	¿El repositorio permite gestionar el número y la ubicación de copias de todos los objetos digitales?	5
xiii	GESTIÓN DE RIESGOS DE SEGURIDAD	
P321	¿El repositorio dispone de un análisis sistemático de los factores de riesgo de seguridad asociados con datos, sistemas, personal y planta física?	5

P322	¿El repositorio tiene implementado controles para responder adecuadamente a cada uno de los riesgos de seguridad definidos?	5
P323	¿El personal del repositorio tiene definido roles, responsabilidades y autorizaciones relacionadas con implementar cambios dentro del sistema?	5
P324	¿El repositorio tiene adecuada preparación escrita y planes de recuperación, incluyendo al menos una copia de seguridad de toda la información preservada junto con una copia de los planes de recuperación?	5
D ASPECTOS ESPECIFICOS DEL ENTORNO		
xiv	GESTION DE LA INTEGRIDAD	
P41	Legalidad del archivo. El repositorio controla que el archivo cumpla la disposición legal para la preservación.	
	¿Existe un documento legal que dispone la preservación del archivo?	5
	¿Se permite almacenar el documento de autorización?	5
	¿Permite validar el nombre de la autorización del documento con el usuario autorizado en el repositorio?	5
P42	Confidencialidad El repositorio garantiza que el archivo digital este accesible únicamente a personal autorizado para acceder la información.	
	Permite determinar el o los usuarios permitidos para el ingreso y acceso al archivo digital.	5
	¿Existe control de uso del aplicativo, con el debido registro de usuario autorizado?	5
	¿Emite una alerta de seguridad al intentar acceder al archivo digital no permitida?	5
P43	Control de calidad ingesta	

	El repositorio permite la validación de formatos, contenidos o aplicaciones activas	
	¿El sistema dispone de un mecanismo de verificación del archivo digital ingresada?	4
	¿El sistema guarda información adicional relacionada con el contenido del objeto digital?	4
	¿El sistema solicita verificación del archivo digital a preservar antes de ejecutar el proceso de preservación?	4
P44	Ingesta parcial, El repositorio permite recibir información o contenido dividido en partes.	
	¿El sistema permite incrementar seguridad a un documento específico?	5
	¿El sistema mantiene un listado del ingreso del archivo digital cronológicamente organizada?	5
P45	Metadatos del entorno del archivo digital a preservar El repositorio provee información técnica y descriptiva sobre el medio ambiente de la colección del archivo digital	
	¿El sistema permite preservar datos técnicos y descriptivos adicionales sobre el entorno de adquisición del archivo digital?	5
	¿El sistema permite almacenar la herramienta de creación, de recogida y de preservación del archivo digital?	5
	¿El sistema emite un reporte de los metadatos del archivo digital a preservar?	5
P46	AIP, SIP, DIP. Transmisión El repositorio dispone de procesos para la transmisión de archivo digital, según el modelo	
	¿El sistema emite un reporte del proceso de preservación de la del archivo digital?	5

	¿El sistema genera un reporte de la actividad del archivo digital dentro del repositorio?	5
P47	Museo de Herramientas El repositorio permite para conservar herramientas utilizadas para acceder a los objetos digitales	
	¿El sistema permite acceder a la evidencia y a las herramientas vinculadas para su recreación?	5
	¿El sistema emite un reporte sobre el entorno hardware en el que fue generado el archivo digital?	5
P48	Garantizar la integridad del original, El repositorio establece técnicas adicionales para la seguridad, integridad, fiabilidad y accesibilidad de los datos	
	¿El sistema reporta la ubicación del archivo digital original y de las copias que mantiene el sistema?	5
	El sistema tiene un mecanismo de verificación de integridad del archivo digal (código hash)	5
	¿El sistema reporta actividad sobre los objetos digitales preservados?	5
P49	Almacenamiento distribuido El repositorio permite almacenar datos en repositorios compartidos	
	¿El sistema permite dirigir el almacenamiento de la información a preservar?	5
	¿El sistema permite acceder al archivo digital almacenada en otros repositorios vinculados?	5
P410	Terminología El repositorio permite usar términos de interpretación que son únicos para este entorno.	

	¿El sistema mantiene un listado de términos utilizados en el aplicativo?	5
	¿El sistema permite acceder a las definiciones e interpretaciones de los términos?	5
	¿El sistema permite incrementar la interpretación de términos?	5
P411	Evaluación de riesgos El repositorio permite determinar, supervisión o alertas de riesgos.	
	¿El sistema emite alertas de seguridad?	5
	¿El sistema emite alertas de errores de operación?	
	¿El sistema emite alertas de cumplimiento de políticas de preservación?	5
P412	Tiempo de preservación, El repositorio determina el horizonte de tiempo de conservación	
	¿El sistema permite definir el tiempo de preservación del archivo digital?	5
	¿El sistema emite una alerta de cumplimiento del tiempo de preservación?	5
	¿El sistema permite modificar el tiempo de preservación?	5
P413	Certificaciones de la estrategia. El repositorio establece los certificados digitales con una estrategia de conservación aplicada o una combinación de ellos	
	¿El sistema permite una verificación de la técnica de preservación aplicada al archivo digital?	5
	¿El sistema genera una certificación de garantía de proceso de preservación?	5

P414	Trazabilidad y Continuidad de la preservación. El repositorio tiene la capacidad para reconstruir el historial de la utilización o la localización de un archivo digital	
	¿El sistema mantiene un monitoreo del acceso del archivo digital durante el periodo de preservación?	5
	¿El sistema emite un reporte periódico de la actividad sobre el archivo digital durante el periodo de preservación?	5
	¿El sistema emite un reporte sobre la actividad de los usuarios durante el periodo de preservación?	5
P415	¿Con el uso de este modelo para preservación del archivo digital, en este caso específico, usted considera que la admisibilidad se elevaría o disminuiría?	
	Según corresponda responda por favor:	
	¿En qué nivel de porcentaje considera usted se elevaría la admisibilidad del archivo digital de este caso específico?	5

Realizado por: Verónica Paucar, 2021 (basado en (Nestor, 2006))



ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

**DIRECCIÓN DE BIBLIOTECAS Y RECURSOS DEL APRENDIZAJE
UNIDAD DE PROCESOS TÉCNICOS Y ANÁLISIS BIBLIOGRÁFICO Y DOCUMENTAL**

REVISIÓN DE NORMAS TÉCNICAS, RESUMEN Y BIBLIOGRAFÍA

Fecha de entrega: 25 / 08 / 2021

INFORMACIÓN DEL AUTOR/A (S)
Nombres – Apellidos: <i>Verónica Judith Paucar León</i>
INFORMACIÓN INSTITUCIONAL
<i>Instituto de Posgrado y Educación Continua</i>
Título a optar: <i>Magíster en Seguridad Telemática</i>
f. Analista de Biblioteca responsable: <i>Lic. Luis Caminos Vargas Mgs.</i>



0088-DBRAI-UPT-IPEC-2021