RESUMEN – TRABAJO DE GRADO

AUTORES	**DANIEL EDUARDO JIMÉNEZ OVALLOS** **MARTHA BAYONA** **ROBINSON MALDONADO**
FACULTAD	**FACULTAD DE INGENIERIAS**
PLAN DE ESTUDIOS	**ESPECIALIZACIÓN EN AUDITORIA DE SISTEMAS**
DIRECTOR	**ANDRÉS MAURICIO PUENTES VELÁSQUEZ**
TÍTULO DE LA TESIS	**DESARROLLO DE UNA POLÍTICA QUE ORIENTE LA IMPLEMENTACIÓN DEL ARCHIVO DIGITAL DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA, SIGUIENDO LOS LINEAMIENTOS ESTABLECIDOS POR EL ARCHIVO GENERAL DE LA NACIÓN Y QUE GARANTICE LA SEGURIDAD DE LA INFORMACIÓN.**

RESUMEN
(70 palabras aproximadamente)

La Universidad Francisco de Paula Santander Ocaña, es una institución pública de educación superior cuya área de influencia se extiende a múltiples departamentos del país, generando desarrollo en dichas regiones a través de la formación de nuevos profesionales y una ardua tarea de investigación e innovación en diferentes áreas del conocimiento.

Mediante el desarrollo de la política se busca orientar los procesos administrativos y tecnológicos que garanticen la seguridad de la información al momento de implementar un sistema de gestión de documentos electrónicos de archivo, la misma facilitará la formación de una cultura organizacional entorno a la seguridad de la información en la gestión de documentos electrónicos desde su creación hasta su almacenamiento y disposición a futuro.

CARACTERÍSTICAS

PÁGINAS: 57	PLANOS:	ILUSTRACIONES:	CD-ROM: 1

DESARROLLO DE UNA POLÍTICA QUE ORIENTE LA IMPLEMENTACIÓN DEL ARCHIVO DIGITAL DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA, SIGUIENDO LOS LINEAMIENTOS ESTABLECIDOS POR EL ARCHIVO GENERAL DE LA NACIÓN Y QUE GARANTICE LA SEGURIDAD DE LA INFORMACIÓN.

AUTORES:

DANIEL EDUARDO JIMÉNEZ OVALLOS

MARTHA BAYONA

ROBINSON MALDONADO

Trabajo de grado para optar el título de especialista en auditoria de sistemas.

DIRECTOR:

ANDRÉS MAURICIO PUENTES

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

FACULTAD DE INGENIERIA

ESPECIALIZACIÓN EN AUDITORIA DE SISTEMAS

Ocaña, Colombia Junio de 2017

Índice

Lista de Tablas

Lista de Figuras

Capítulo 1: Desarrollo de una política que oriente la implementación del archivo digital de la Universidad Francisco De Paula Santander Ocaña, siguiendo los lineamientos establecidos por el Archivo General de la Nación y que garantice la seguridad de la información.

1.1 Planteamiento del problema

La Universidad Francisco de Paula Santander Ocaña, es una institución pública de educación superior cuya área de influencia se extiende a múltiples departamentos del país, generando desarrollo en dichas regiones a través de la formación de nuevos profesionales y una ardua tarea de investigación e innovación en diferentes áreas del conocimiento.

Dentro de las diferentes dependencias que apoyan el funcionamiento y el desarrollo de procesos en la universidad, se encuentra la dependencia de secretaría general quien se encarga entre otras funciones a dirigir los procesos referentes al archivo de documentos. Para lograr sus objetivos frente a la gestión de documentos legales cuenta con un subproceso denominado archivo, que se encarga de custodiar la documentación histórica de la institución.

El Archivo General de la Nación -AGN, es una entidad del orden nacional adscrita al Ministerio de Cultura, encargada de la organización y dirección del Sistema Nacional de Archivos -SNA, de regir la política archivística en nuestro País y de custodiar, resguardar y proteger el patrimonio documental que conserva, en consecuencia a los grandes trastornos ambientales que se han presentado en el país, se han adoptado ciertas medidas que buscan realizar un aporte positivo en cuanto a la preservación del medio ambiente, una de estas medidas

es la ejecución de un plan de sostenibilidad ambiental denominado “cero papel” que busca reducir los índices de gasto de papel.

Para lograr el total cumplimiento de la política de cero papel la Universidad Francisco de Paula Santander debe dar cumplimiento al acuerdo No 003 del 17 de Febrero de 2015 por el cual se establecen lineamientos generales para las entidades del Estado en cuanto a la gestión de documentos electrónicos.

Uno de los puntos que recomienda cero papel es la digitalización de documentos, por ello la Universidad Francisco de Paula Santander encabezada por la dependencia de Secretaría General, ha trabajado en el desarrollo de una herramienta que garantice que dicho archivo sea puesto en marcha, actualmente la universidad cuenta con un sistema de información documental (SID) que permite la creación y el almacenamiento de un gran número de documentos, todos ellos generados por las diferentes dependencias de la institución.

En el momento de almacenar documentos electrónicos, se debe garantizar la autenticidad del documento y disponibilidad a futuro. En el caso de la autenticidad es necesario manejar con suma precaución el uso de las firmas digitales, para que se genere la confianza necesaria en las personas que reciben dichos documentos, o quienes los consulten en una fecha diferente a su creación y almacenamiento.

1.2 Formulación del problema

¿Desarrollar una política que oriente la implementación del archivo digital de la Universidad Francisco De Paula Santander Ocaña, siguiendo los lineamientos establecidos por el archivo general de la nación y que permitirá mejorar la seguridad de la información en la institución?

1.3 Objetivos

1.3.1 Objetivo General.

Desarrollar una política que oriente la implementación del archivo digital de la Universidad Francisco de Paula Santander Ocaña, siguiendo los lineamientos establecidos por el Archivo General de la Nación, que garantice la seguridad de la información.

1.3.2 Objetivos Específicos

- Diagnosticar el estado de la seguridad de la información de las herramientas y procedimientos asociada a la gestión documental.

- Validar el cumplimiento de los estándares legales necesarios, según lo establecido por el Archivo General de la Nación, para el uso de archivos digitales.

- Documentar una política institucional que garantice la seguridad del archivo digital de documentos, teniendo en cuenta los lineamientos necesarios establecidos por el Archivo General de la Nación.

1.4 Justificación

Desarrollar una política que oriente la implementación del archivo digital de la Universidad Francisco de Paula Santander Ocaña, con el fin de guiar todas las actividades que se deriven o que sean necesarias para llevar a cabo la digitalización, garantizando unas bases y un fin común en toda la institución, y facilitando encaminar las dependencias que participarán directa o indirectamente en la puesta en marcha de la digitalización.

Para lograr la creación de una política eficiente, que garantice la seguridad de la información que se va a manejar o a gestionar, es necesario tener en cuenta estándares como la ISO 27001, y tener un manejo absoluto de los lineamientos establecidos por los entes de control nacional.

La creación de una política garantiza que un proceso o una serie de procesos los cuales estén inmiscuidos en dicha política, no rompan los márgenes allí establecidos y los resultados esperados se alinean bajo un mismo objetivo. Para lograr que la digitalización de documentos en la institución sea un éxito se deben encaminar esfuerzos y demarcar márgenes entorno a la seguridad de la información y regido por lo establecido por el AGN (Archivo General de la Nación).

Una política en cuanto al archivo digital, permitirá agrupar los esfuerzos de toda la institución en miras a ese gran objetivo, llevando a cabo metas claras y organizadas que facilitaran la ejecución de actividades y tareas necesarias para tal fin.

1.5 Delimitaciones y alcances

1.5.1 Delimitación Conceptual

Los conceptos utilizados durante el desarrollo de la política y la investigación que se llevó a cabo para el desarrollo de dicha política maneja toda la terminología referente a archivo, lo enmarcado por el archivo general de la nación, y todo lo referente a la digitalización definido por el mismo ente regulador.

1.5.2 Delimitación Geográfica

La política que se busca establecer está definida bajo el contexto de la Universidad Francisco de Paula Santander Ocaña, beneficiando la región y sirviendo de ejemplo para otras instituciones que busquen lograr la digitalización de documentos.

1.5.3 Delimitación Temporal

La investigación se desarrolló en el transcurso del año 2016 y comienzos del 2017 se espera que la política de seguridad sea implementada a finales del presente año a más tardar.

Capítulo 2: Marco Referencial

2.1 Marco Histórico

La archivística está definida como técnica de conservación y catalogación de archivos, es un área de estudio muy antigua y a la vez muy necesaria, para las empresas, se habla de archivística y de archivo desde la época medieval donde se definía el archivo como lugar de conservación de los documentos, en el presente documento no se va a profundizar en esta área de conocimiento que por su relevancia y trascendencia histórica, se vuelve extensa y desvía la intensión propia de la presente investigación.

Frente al tema del archivo en el mundo actual aparece un nuevo componente que redefine y hace aún más complejo el tema de archivo de documentos, entre las investigaciones emprendidas sobre la conservación del valor evidencial de los documentos electrónicos destacan los proyectos Eros, desarrollado desde 1995 por el Public Record Office del Reino Unido; International research on permanent authentic records in electronic systems (Interpares), realizado entre 1994 y 1997 por seis grupos de investigación internacionales coordinados por la University of British Columbia, y Cerar, de la University of Pittsburgh, actualmente en curso.

Los principales organismos que trabajan en el ámbito de la preservación de los documentos electrónicos publicando informes técnicos y recomendaciones, son los siguientes: European Commission on Preservation and Access, Council on Library and Information Resources, National Preservation Office of United Kingdom y Research Libraries Group: the Commission on Preservation and Access.

En cuanto a las organizaciones que se dedican, de modo global, al estudio de todas las áreas involucradas en la gestión de los documentos de archivo electrónicos destacan: el Comité

de Documentos Electrónicos del Consejo Internacional de Archivos; US National Archives and Records Administration mediante su Electronic Records Archives Program; la American Records Management Association; la Biblioteca del Congreso y la Comisión Europea a través de DLM-Forum.

En Colombia, El Archivo General de la Nación (AGN, 2016), se define como una entidad del orden nacional adscrita al Ministerio de Cultura, encargada de la organización y dirección del Sistema Nacional de Archivos -SNA, de regir la política archivística en nuestro País y de custodiar, resguardar y proteger el patrimonio documental que conserva.

Para el país es muy importante crear políticas de estandarización y homologación de conceptos internacionales en torno a la preservación de documentos electrónicos, por ello el Archivo General de la Nación, como ente encargado de regular todo lo relacionado con temas de archivística, mediante el Decreto 2578 de 2012 en su Artículo 18, se reglamenta el SINAE (Sistema Nacional de Archivos Electrónicos) como un programa especial del Archivo General de la Nación para garantizar la preservación del patrimonio documental digital en Colombia y promover la estandarización de la gestión de documentos electrónicos en el Estado(AGN, 2016)

Además del SINAE, el AGN ha venido trabajando en estrategias que faciliten el estudio e implementación de archivos digitales o electrónicos, por ello a partir de mayo del año 2014 se puso en funcionamiento el Laboratorio de Innovación Digital Archivística -LIDA, cuyo propósito principal está centrado en la creatividad, en la innovación de procedimientos y metodologías aplicables a la gestión electrónica de documentos.

En Febrero del 2015, el Archivo General de la Nación, pone a disposición de la ciudadanía la infografía Preservación Digital a Largo Plazo, como parte del trabajo que viene adelantando la

Entidad, en la construcción de políticas y lineamientos del Estado para la gestión, conservación y preservación del patrimonio documental colombiano.

Este recurso brinda una descripción general de los componentes básicos para la formulación e implementación del Plan de Preservación Digital a Largo Plazo, relacionados con las estrategias de preservación, gestión de los riesgos asociados, así como estándares y normativa vigente en la materia, en concordancia con lo establecido en el Acuerdo 006 de 2014, por medio del cual se desarrollan los artículos 46, 47 y 48 del Título XI “Conservación de Documentos” de la Ley 594 de 2000.

2.2 Marco Contextual

Este trabajo se desarrollará en la Secretaría General de la Universidad Francisco de Paula Santander Ocaña, dado que es el ente encargado de implementar y regular todo lo relacionado con la producción y archivo de documentos en la institución.

2.3 Marco Conceptual

Los temas de estudio en el presente proyecto son: documento electrónico, documento electrónico de archivo, seguridad de la información, características principales de la información, control, amenaza, vulnerabilidad, riesgo, política de seguridad de la información, política de seguridad informática y tecnología de información.

2.3.1 Documento Electrónico.

Es la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares (Congreso de Colombia. Ley 527 de 2009).

2.3.2 Documento Electrónico de Archivo.

Es el registro de información generada, recibida, almacenada y comunicada por medios electrónicos, que permanece en estos medios durante su ciclo vital; es producida por una persona o entidad en razón de sus actividades y debe ser tratada conforme a los principios y procesos archivísticos (AGN, 2001)

2.3.3 Firma Electrónica.

La firma electrónica reconocida es, pues, el umbral mínimo que la seguridad jurídica impone para la producción de actos administrativos válidos y eficaces.

Mediante la aplicación de servicios técnicos y administrativos de seguridad en las comunicaciones permitirá:

- Acreditar la identidad del emisor y del receptor de la comunicación, así como la autenticidad de su voluntad.
- Garantizar la integridad y conservación del contenido del documento en su emisión y recepción.
- Acreditar la presentación o, en su caso, la recepción por el destinatario, de notificaciones, comunicaciones o documentación.
- Igualmente en tanto no se regule en la normativa específica sobre registros telemáticos, el sistema de firma electrónica avanzada servirá como registro de entrada en lo relativo a la fecha y hora de entrada, fecha y hora de presentación, identificación del interesado, contenido del escrito y órgano administrativo al que se envía.
- Su empleo de modo automático por un agente electrónico.

La validez jurídica de los documentos electrónicos se basa en dos elementos clave, según lo afirman Olmo y Grispigni (2006, p68) la identidad del emisor y la garantía de integridad del documento entendida como no alteración de su contenido, ni de los elementos estructurales o contextuales considerados en cada caso como necesarios para dicha validez.

El artículo 27 de la ley 11/2007, refiriéndose a las comunicaciones electrónicas dice que serán válidas siempre que exista constancia de la transmisión y recepción, de sus fechas, del contenido íntegro de las comunicaciones y se identifique fidedignamente al remitente y al destinatario de las mismas.

2.3.4 Metadato.

Los metadatos están destinados a ordenar y describir la información contenida en un documento entendido como objeto electrónico, de tal forma que se erigen como reveladores tanto de la descripción formal, como del análisis de contenido, en aras a mejorar el acceso a esos objetos de información de la Red.

No son más que estructuras de organización de la información, legibles por máquina, cuya finalidad es hacer útiles los datos, de distintas formas, según las necesidades concretas de cada servicio de información digital y según la aplicación que les otorgue. En muchos casos ni siquiera aparecerán visibles en el documento, sino que irán incluidos en su estructura interna mediante metadatos asociados.

Para Eva Mª Méndez (2003), en el contexto digital actual, se consideran los metadatos como una herramienta que garantiza el significado, la facilidad de manejo y la perdurabilidad de los registros de archivos y de la información que contienen.

2.3.5 Seguridad de la información.

La ISO define la seguridad de la información como la preservación de la confidencialidad, integridad y disponibilidad.

2.3.6 Características principales de la información.

Los siguientes términos son definidos según (ICONTEC, 2013):

Confidencialidad o que la información llegue solamente a las personas autorizadas. Contra la confidencialidad o secreto pueden darse fugas y filtraciones de información, así como accesos no autorizados. La confidencialidad es una propiedad de difícil recuperación, pudiendo minar la confianza de los demás en la organización que no es diligente en el mantenimiento del secreto, y pudiendo suponer el incumplimiento de leyes y compromisos contractuales relativos a la custodia de los datos.

Integridad o mantenimiento de las características de completitud y corrección de los datos. Contra la integridad, la información puede aparecer manipulada, corrupta o incompleta. La integridad afecta directamente al correcto desempeño de las funciones de una Organización.

Disponibilidad o disposición de los servicios a ser usados cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio. La disponibilidad afecta directamente a la productividad de las organizaciones.

A estas dimensiones canónicas de la seguridad se pueden añadir otras derivadas que nos acerquen a la percepción de los usuarios de los sistemas de información:

Autenticidad. Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. Contra la autenticidad de la

información podemos tener manipulación del origen o el contenido de los datos. Contra la autenticidad de los usuarios de los servicios de acceso, podemos tener suplantación de identidad.

Trazabilidad. Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento. La trazabilidad es esencial para analizar los incidentes, perseguir a los atacantes y aprender de la experiencia. La trazabilidad se materializa en la integridad de los registros de actividad.

2.3.7 Control.

Según (ISO, 2005) los controles son: "Medios para manejar el riesgo; incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal. El control también se utiliza como sinónimo de salvaguarda o contramedida."

2.3.8 Amenaza.

Es la probabilidad de ocurrencia de un suceso potencialmente desastroso durante cierto periodo de tiempo, en un sitio dado.

En general el concepto de amenaza se refiere a un peligro latente o factor de riesgo externo, de un sistema o de un sujeto expuesto, expresada matemáticamente como la probabilidad de exceder un nivel de ocurrencia de un suceso con una cierta intensidad, en un sitio específico y durante un tiempo de exposición determinado (UNAD, s.f),

Una amenaza informática es un posible peligro del sistema. Puede ser una persona (cracker), un programa (virus, caballo de Troya, etc.), o un suceso natural o de otra índole (fuego, inundación, etc.). Representan los posibles atacantes o factores que aprovechan las debilidades del sistema.

2.3.9 Vulnerabilidad.

"Es el grado de pérdida de un elemento o grupo de elementos bajo riesgo, resultado de la probable ocurrencia de un suceso desastroso expresada en una escala. La vulnerabilidad se entiende como un factor de riesgo interno, expresado como la factibilidad de que el sujeto o sistema expuesto sea afectado por el fenómeno que caracteriza la amenaza." (Administración Electrónica, 2012).

En el campo de la informática, la vulnerabilidad es el punto o aspecto del sistema que es susceptible de ser atacado o de dañar la seguridad del mismo. Representan las debilidades o aspectos falibles o atacables en el sistema informático.

2.3.10 Riesgo.

El riesgo se considera como la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización.

2.3.11 Política de Seguridad.

De acuerdo a (Reynolds, 1991) define Política de seguridad como: "una declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran."

Tecnología de información. Es el estudio, diseño, desarrollo, implementación, soporte o dirección de los sistemas de información computarizados, en particular de software de aplicación y hardware de computadoras.

2.4 Marco Teórico

Las temáticas que soportan el presente documento, son en base a la seguridad de la información, la preservación de documentos electrónicos a través del tiempo y el desarrollo de aplicaciones web con altos niveles de seguridad.

En primer lugar la seguridad de la información, está bien definida por la ISO 27001, para la preservación de documentos electrónicos y en si todo lo relacionado a su seguridad, se tendrá en cuenta los documentos escritos y definidos por la organización OWASP.

ISO 27001. Es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001.

OWASP. Es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que un software sea inseguro, el hecho de no estar ligado comercialmente a ninguna

empresa, hace que OWASP genere contenido objetivo, sin tendencias o preferencias hacía algún producto de tipo comercial o privado.

La comunidad OWASP se encuentra claramente dividida en dos áreas, y se evidencia dicha división en el tipo de productos que se obtienen. Las categorías principales son: proyectos de desarrollo y proyectos de documentación.

Los proyectos de documentación actualmente son:

- **La guía:** Este documento proporciona una orientación detallada sobre la seguridad de las aplicaciones web.
- **El top ten de las vulnerabilidades más críticas de aplicaciones web:** Este documento es más resumido y específico que la guía, además es considerado un documento de alto nivel dada la precisión con la cual se presentan los casos de inseguridad.
- **Métricas:** Un proyecto viable para definir las métricas de seguridad de aplicaciones web.
- **Legal:** Un proyecto de software para ayudar a compradores y vendedores negociar una seguridad adecuada en sus contratos.
- **Guía de Testeo:** Una guía eficaz centrada en pruebas de la seguridad de aplicaciones web.
- **ISO17799:** Los documentos de soporte para las organizaciones haciendo revisiones ISO17799
- **AppSec FAQ:** Preguntas frecuentes y respuestas sobre seguridad de aplicaciones

Los proyectos de desarrollo incluyen:

- **WebScarab:** una aplicación Web que incluye una suite de evaluación de vulnerabilidades y herramientas Proxy.

- **Los filtros de validación:** (Stinger para J2EE, filtros para PHP) filtros de frontera genéricos de seguridad que los desarrolladores pueden utilizar en sus propias aplicaciones.
- **WebGoat:** una herramienta de capacitación y evaluación interactiva que los usuarios pueden utilizar para aprender sobre seguridad de aplicaciones web en un lugar seguro y legal.
- **DotNet:** una variedad de herramientas para asegurar entornos .NET.

2.5 Marco Legal

El presente proyecto está enmarcado con las leyes que protegen entre otras cosas, la información personal, la gestión documental de archivos electrónicos y todo lo referente al desarrollo de aplicaciones y sus respectivas licencias, dichas leyes son:

2.5.1 Ley 1581 de 2012

El Congreso de Colombia decretó que esta ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política de Colombia; así como el derecho a la información consagrado en el artículo 20 de la misma (MINTIC, 2012).

2.5.2 Ley 1266 del 31 de diciembre de 2008

El Congreso de Colombia decretó: “Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en

especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones" (SIC, 2008).

2.5.3 Acuerdo No 003 del 2015

Este acuerdo emitido por el consejo directivo del archivo general de la nación, establece los lineamientos generales para las entidades del estado en cuanto a la gestión de documentos electrónicos generados como resultado del uso de medios electrónicos de conformidad con lo establecido en el capítulo IV de la ley 1437 de 2011.

2.5.4 Ley 527 de 1999

Para el uso de firmas electrónicas se debe tener en cuenta esta ley dado que en ella se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

Capítulo 3: Diseño Metodológico

3.1 Tipo de Investigación

La investigación es cualitativa, dado que estudia ciertos comportamientos de la población investigada y además evalúa la cultura organizacional en cuanto al buen uso de la información manejada. Pero también se usa como apoyo a la investigación herramientas cuantitativas como encuestas con el fin de desarrollar una política que describa y oriente el archivo de documentos electrónicos en una institución pública como lo es la Universidad Francisco de Paula Santander Ocaña.

3.2 Población

La población motivo de estudio en esta investigación son todas aquellas personas con cargos administrativos en la Universidad Francisco de Paula Santander Ocaña, y particularmente aquellos quienes poseen un usuario del actual Sistema de Información Documental.

3.3 Muestra

Una muestra bastante significativa e incluyente son los empleados que cubren el cargo de secretarias de facultades, dado a su conocimiento tanto en temas de archivo y del sistema de información documental, y complementado con información que puede facilitar el encargado de manejar y dar soporte a dicho sistema.

3.4 Recolección de Información

Dadas las características de la investigación, y la información necesaria para su estudio, las técnicas a usar serán encuestas, entrevistas y observación, que a su vez puede estar acompañada de una lista de chequeo.

Capítulo 4: Presentación de Resultados

4.1 Diagnosticar el estado de la seguridad de la información de las herramientas y procedimientos asociada a la gestión documental.

En primer lugar se realizó una entrevista al ingeniero a cargo de dar soporte y mantener actualizado el Sistema de Información Documental, el resultado se presenta a continuación:

4.1.1 Resultado de la entrevista realizada al ingeniero a cargo del soporte del SID.

¿Cuáles son tus funciones en la Universidad Francisco de Paula Santander Ocaña?

"En primer lugar dejar claro que el jefe directo es el secretario general dado que el cargo ocupado es profesional de apoyo a la dependencia de secretaria general y dentro de las funciones se encuentra la administración de dos sistemas de información, el Sistema de Información Documental y con igual cantidad de obligaciones el sistema de PQRS" (J. L. Sarabia, comunicación personal, 19 de junio del 2017)

¿Permítenos conocer una breve descripción del funcionamiento del SID?

"El Sistema de Información Documental, fue producto de una tesis de grado de un estudiante de Ingeniería de Sistemas, la cual ha sido actualizada según las necesidades de la institución y de los usuarios en general, la herramienta está orientada a la web, desarrollada en PHP y usando tecnologías como jQuery para realizar transacciones asincrónicas, de tal forma que podríamos decir que la base del funcionamiento está centrado en PHP y jQuery, con un diseño en html y css, además cuenta con una tabla relacional gestionada por el motor de base de datos de ORACLE.

Dado que el objetivo del SID, es facilitar la elaboración de documentos institucionales, la mayor parte de sus usuarios son secretarias o auxiliares administrativos que desempeñan funciones de dicho rol.

Tanto la base de datos, como el servidor funcionan bajo la responsabilidad y el cuidado de la División de Sistemas de la Universidad, esta dependencia se encarga de brindar las herramientas necesarias, para que la aplicación funcione en la web correctamente." (J. L. Sarabia, comunicación personal, 19 de junio del 2017)

¿El SW está desarrollado bajo que patrón de diseño, por ejemplo, MVC, MVC usando DAO y VO u otros patrones de diseño diferentes a los mencionados? ¿Cuáles?

"El sistema tiene un patrón de diseño MVC usando DAO y VO, bajo las libertades de codificación que PHP permite y teniendo en cuenta que luego de su creación, dos desarrolladores han trabajado sobre él y han creado nuevas funcionalidades tratando de respetar la arquitectura con la que fue creado." (J. L. Sarabia, comunicación personal, 19 de junio del 2017)

¿El sistema almacena una copia de los documentos generados, o solo son re construibles a través de la base de datos?

"El sistema fue creado con la finalidad de convertirse en un archivo digital, por ello se buscó cumplir con estándares y normas que facilitaran dicho fin, es por esto que se almacenan los documentos finalizados en el servidor, teniendo una unidad con normas de seguridad especiales en el servidor." (J. L. Sarabia, comunicación personal, 19 de junio del 2017)

¿Quién es el encargado de seguir el funcionamiento del servidor, en el cual funciona el sistema?

"El SID está almacenado y se ejecuta sobre los servidores de la institución, donde el Ingeniero José Luis no cuenta con los permisos suficientes para desarrollar funciones de administración del servidor." (J. Sarabia, comunicación personal, 19 de junio del 2017)

Dichos servidores son custodiados por el área de sistemas de la institución, además el "ingeniero Molina dio a conocer que dentro de las políticas de seguridad de la institución está la ejecución de ataques éticos de hacking anuales para evaluar la seguridad de los sistemas y los servidores, dando siempre buenos resultados en los servidores y en específicamente en el SID." (N. Molina, comunicación personal, 19 de junio del 2017)

¿Teniendo en cuenta sus conocimientos de programación, el SID podría convertirse en una herramienta que facilite la digitalización del archivo de documentos?

"Dado que el SID es una herramienta que lleva varios años en la institución, que cumple actualmente a cabalidad todas sus funciones y que a la fecha no ha sufrido ataques ni inconvenientes de seguridad, se puede considerar una excelente opción." (J. L. Sarabia, comunicación personal, 19 de junio del 2017)

¿Considera que la comprensión del código fuente de este sistema es sencilla, o le costó trabajo comprender algunas funcionalidades?

"A pesar de que el sistema está desarrollado en PHP y que por las características del lenguaje permita realizar una misma operación de diferentes maneras, el actual sistema funciona correctamente y es de fácil comprensión toda su codificación." (J. L. Sarabia, comunicación personal, 19 de junio del 2017)

4.1.2 Análisis del resultado de la entrevista, teniendo en cuenta las respuestas proponer hipótesis de posibles falencias que se puedan estar presentando.

Luego de analizar las respuestas dadas por el ingeniero encargado de dar soporte al SID y el complemento dado por los encargados de custodiar los servidores, en primer lugar podemos observar que el ingeniero se encuentra copado de obligaciones y que en caso tal de necesitar el desarrollo de nuevas funcionalidades sería bastante complicado conseguirlo en un corto o mediano plazo.

En cuanto al lenguaje de programación y el motor de base de datos, podemos decir que es bastante robusta la seguridad del motor, y que la organización del código fuente y la arquitectura utilizada son lo suficientemente organizadas para continuar con la elaboración de nuevas funciones dando continuidad a lo que se tiene en la actualidad.

Por último podemos considerar que aunque el sistema es bastante complejo no ha tenido problemas de seguridad ni de perdida de información desde su creación, además fue elaborado con la finalidad de archivar documentos electrónicos y desde ese punto es muy favorable a la hora de pensar en usar dicha herramienta para continuar en el proceso de digitalización y en proyección a un archivo digital.

4.1.3 Contrastar los posibles fallos, con pruebas acompañadas por el ingeniero de soporte.

Luego de analizar los resultados de la entrevista y teniendo en cuenta ciertos errores comunes presentados en la arquitectura y la tecnología usada en el desarrollo del SID, se desarrollaron las siguientes pruebas de seguridad:

1. Tratar de entrar a una URL sin haber ingresado las credenciales de acceso al sistema.
2. Ver las contraseñas de los usuarios.

3. Inyección de código SQL.
4. Luego de ingresar las credenciales de acceso con un rol sin permisos administrativos, ingresar a una URL no permitida para ese rol.

Y se obtuvieron los siguientes resultados:

1. El Sistema cuenta con un seguro y efectivo control de acceso al sistema, vigilando todas las posibles intrusiones, por lo tanto no es posible acceder a ninguna URL sin haber ingresado al sistema.

2. Una de las falencias que se tenía conocimiento, era la falta de un sistema de encriptación para las credenciales de acceso, pero con la implementación de una nueva tecnología, el sistema no almacena ninguna credencial ni contraseña de usuario.

3. El sistema no permite ningún tipo de inyección SQL en el formulario de ingreso, pues cuenta con un sistema de verificación que no permite escribir ciertos caracteres que podrían ser utilizados para dicho ataque.

4. Los roles del sistema se encuentran muy bien definidos y los accesos muy bien restringidos, por ello no se puede tener acceso a ningún área de mayor responsabilidad.

4.1.4 Encuestar y observar las secretarias seleccionadas para la investigación, para detectar riesgos de seguridad en el usuario final del sistema.

Describe las principales falencias que has detectado en el SID?

Los usuarios no han tenido problemas en cuanto a la seguridad y la integridad de la información por el contrario ven como un problema que no permita eliminar algunos documentos, cuyo estado se conoce como inicial, habiendo sido creado por usuarios que en su

mayoría ya no laboran en las dependencias, y que se presentan de primeros en las listas de documentos creados, generando de cierta manera un desorden para los usuarios activos.

Las demás falencias encontradas son referentes al editor de textos, el cual no corrige ortografía y es un poco complicado a la hora de elaborar tablas.

Marca con una x si tu contraseña tiene las siguientes características. (Puedes marcas varias opciones)

( ) Letras.

( ) Letras en mayúscula.

( ) Letras en minúscula.

( ) Números.

( ) Símbolos.

Para facilitar la comprensión de los resultados se elaboró **la figura 1** la cual podemos observar a continuación.

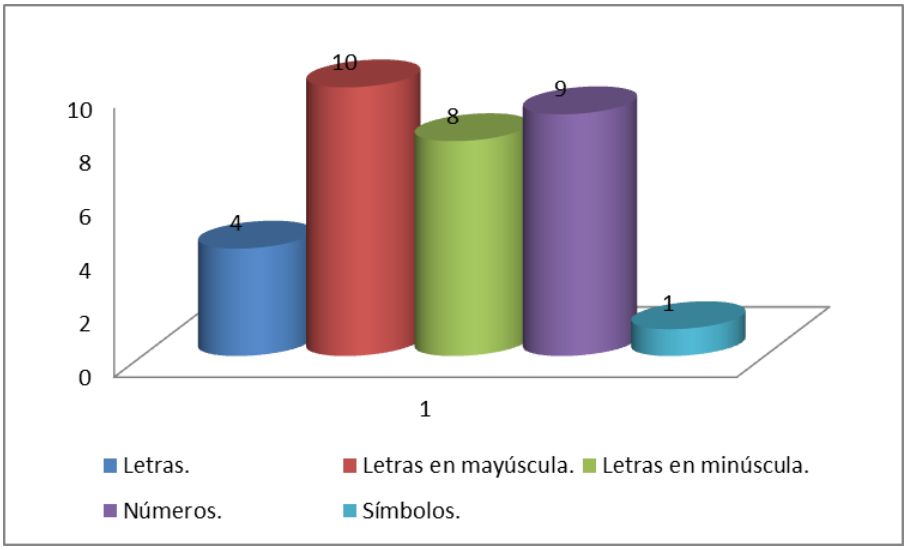

Figura 1 Características de las contraseñas usadas.

Podemos observar que en su mayoría las contraseñas usadas son seguras dado que combinan letras en mayúsculas y minúsculas y números, y a pesar que no se usan símbolos no quiere decir que las contraseñas no sean robustas.

¿Mantienes la contraseña oculta en algún lugar de tu escritorio o puesto de trabajo?

Si __ No __

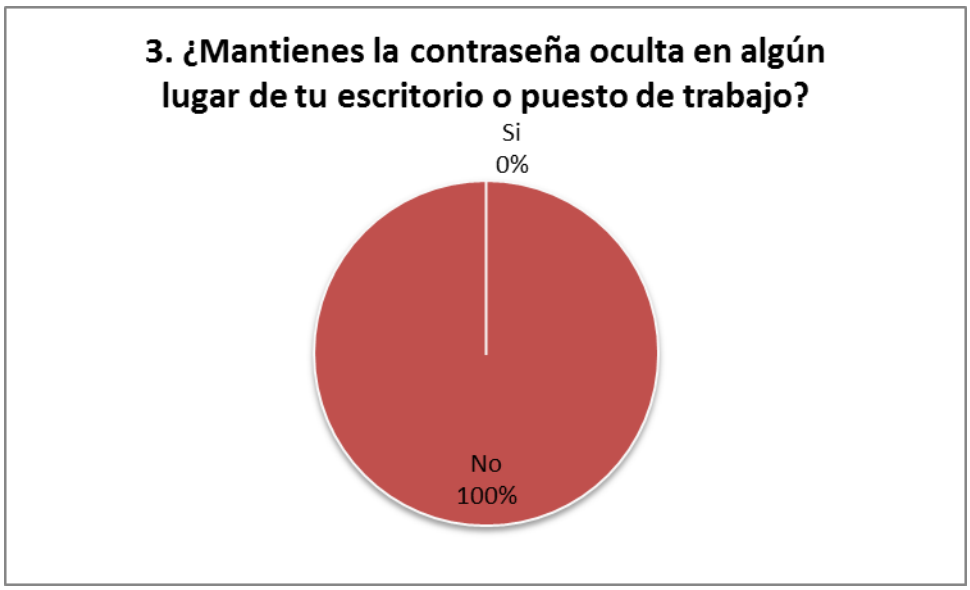

Figura 2 Almacenar contraseñas en el puesto de trabajo.

Según el resultado obtenido por las encuestas podríamos decir que existe conciencia en cuanto al uso adecuado de las contraseñas, pero en el momento de aplicar la encuesta se pudo observar que las encuestadas usan memos o documentos adheridos a los monitores que por su contenido y la forma como se presentan podrían hacer referencia a una contraseña de algún sistema de información incluido el SID.

¿En algún momento has almacenado un documento el SID, y sin tu autorización ha sido eliminado? Si __ No __

Figura 3 Percepción de seguridad de la información.

La percepción de permanencia de la información podríamos considerarla perfecta, dado que no se reportan perdidas en más de cinco años en funcionamiento.

¿Si tuvieras las facultades para solicitar cambios al SID, ¿qué cambios ordenarías que se hicieran?

Los usuarios tienen una buena percepción del sistema, en su mayoría llevan más de tres años utilizándolo y los cambios a realizarse son básicamente orientados al editor de texto embebido en el sistema.

4.2 Validar el cumplimiento de los estándares legales necesarios, según lo establecido por el Archivo General de la Nación, para el uso de archivos digitales.

Para cumplir el objetivo específico planteado se llevaron a cabo las siguientes actividades:

4.2.1 Recopilar de forma resumida y de fácil comprensión cuales son los requisitos para la implementación tecnológica de un archivo de documentos electrónicos en una institución de carácter público.

El 7 de abril de 2017 el Archivo General de la Nación, publicó un modelo de requisitos para la implementación de un Sistema de Gestión de Documentos Electrónicos de Archivo (SGDEA) el cual evalúa de forma detallada nueve elementos esenciales para la puesta en funcionamiento de un sistema de este tipo. Los elementos que evalúa el modelo son:

4.2.1.1 Clasificación y organización documental.

Este elemento prueba la existencia de un buen número de funcionalidades que en su mayoría giran en torno a la gestión de las tablas de retención documental (TRD) y su integración con el Sistema de Gestión de Documentos Electrónicos de Archivo (SGDEA).

4.2.1.2 Retención y disposición.

Para la archivística es fundamental el manejo de tiempos, previamente definidos y establecidos según el tipo de documento, al igual como se maneja en los archivos donde se almacenan documentos en físico, un SGDEA debe cumplir con una serie de características según el modelo planteado por el Archivo General de la Nación (AGN).

4.2.1.3 Captura e ingreso de documentos.

El modelo planteado por el Archivo General de la Nación, detalla los requerimientos que debe cumplir el SGDEA, en cuanto a la captura e ingreso de documentos, no solo en cuanto a la digitalización de documentos físicos, sino que propone cuidados respecto al manejo de todo tipo de archivo electrónico como videos o imágenes, que pueden ser almacenados.

4.2.1.4 Búsqueda y presentación.

El SGDEA debe permitir la búsqueda de documentos de acuerdo a roles y permisos de usuarios, cumpliendo con requisitos de efectividad y flexibilidad para facilitar la recuperación y presentación de los archivos almacenados.

4.2.1.5 Metadatos.

Los metadatos son definidos como “datos sobre los datos” o “información sobre la información” es decir los metadatos son una estructura de datos que describen de forma detallada un objeto o archivo electrónico. Para el caso específico del SGDEA, los metadatos deben cumplir ciertas características, las cuales se encuentran claramente definidas en el modelo propuesto por el AGN.

4.2.1.6 Control y seguridad.

Todos los sistemas deben garantizar la seguridad de la información, para un sistema de este tipo no es la excepción, para garantizar que los archivos custodiados permanezcan a través del tiempo, el sistema debe cumplir todos los ítems en cuanto a seguridad propuestos por el modelo para la implementación de un SGDEA.

4.2.1.7 Flujos de Trabajo.

El Sistema de Gestión de Documentos Electrónicos de Archivo, debe permitir dentro de sus funciones la completa gestión de flujos de trabajo, cumpliendo a cabalidad lo establecido en el modelo propuesto por el AGN.

4.2.1.8 Flujos electrónicos.

Al igual que los flujos de trabajo, el SGDEA debe permitir una completa gestión de los flujos electrónicos ceñidos a lo establecido por el modelo.

4.2.1.9 Requerimientos no funcionales.

Los requerimientos no funcionales, son aquellos que no se orientan a funciones específicas del software, tales como mostrar cierta información o gestionar cierto tipo de elementos, sino que se orientan al comportamiento del software frente a ciertas tareas del usuario, para este caso el modelo define muy claramente cuales son dichos requerimientos.

4.2.2 Chequear el cumplimiento de los requisitos recolectados en la actividad seis (6) y el conocimiento que se obtuvo en las actividades previas respecto al Sistema de Información Documental.

Tabla 1

Lista de chequeo, ítem clasificación y organización documental.

N°	REQUISITO	CUMPLE	NO CUMPLE
1	El sistema permite la gestión de las Tablas de Retención Documental		X
2	El SGDEA debe permitir que las Tablas de Retención Documental tengan asociados los siguientes campos de manera opcional: Una descripción y/o justificación, versión de la TRD, fecha de actualización de la TRD en el sistema, Identificador único cuando se crea.		X
3	El SGDEA debe garantizar que los documentos producidos y asociados a una TRD, mantienen los criterios de tiempos y de disposición final de la versión correspondiente.		X
4	El SGDEA debe representar la organización de los expedientes y documentos, incluyendo sus metadatos, a partir del esquema del cuadro de clasificación documental.		X
5	El SGDEA debe validar la información que se ingresa en el esquema de la Tabla de Retención Documental a través de generación de alertas o incorporación de opciones que incluyan asistentes paso a paso (listas desplegables, alertas, listas de chequeo, ventanas de ayuda, entre otras) que indiquen si existe información similar o igual en el sistema.		X
6	El SGDEA debe permitir la importación y exportación total o parcial de la Tabla de Retención Documental		X
7	El SGDEA debe permitir a usuarios autorizados la selección y uso de las diferentes versiones de la Tabla de Retención Documental		X
8	El SGDEA debe permitir la integración con los diferentes servidores de correo electrónico de acuerdo a las necesidades o políticas de cada organización.	X	
9	Los documentos dentro del SGDEA deberán heredar los metadatos de su serie o subserie.		X
10	El SGDEA debe permitir exportar el directorio, de todos los expedientes y/o carpetas clasificadas en una serie específica y su contenido.		X
11	El SGDEA debe permitir ingresar los datos de localización de un expediente híbrido (referencia cruzada al expediente físico).		X

Tabla 2

Lista de chequeo, ítem retención y disposición.

N°	REQUISITO	CUMPLE	NO CUMPLE
12	El SGDEA debe permitir sólo al rol administrador crear y/o gestionar tiempos de retención y disposición.		X
13	El SGDEA debe mantener una historia inalterable de modificaciones (pistas de auditoría) que se realizan en los tiempos de retención y disposición, incluida la fecha del cambio o eliminación y el usuario que lo registra.		X
14	El SGDEA debe garantizar que cualquier cambio a un tiempo de retención y disposición se aplique inmediatamente a todas las series, subseries a las que se asigna.		X
15	El SGDEA no debe limitar la duración de los tiempos de retención.		X
16	El SGDEA debe activar automáticamente un alerta al rol administrador cuando el período de retención aplicable está a punto de cumplir el tiempo establecido.		X
17	El SGDEA deberá generar un reporte del estado de la transferencia o exportación realizada y guardar datos de la acción realizada en las pistas de auditoria.		X
18	Conserva todos los Documentos Electrónicos de Archivo (DEA) que se hayan transferido, al menos hasta que se reciba la confirmación de que el proceso de transferencia ha concluido satisfactoriamente.		X

Tabla 3

Lista de chequeo, ítem captura e ingreso de documentos.

N°	REQUISITO	CUMPLE	NO CUMPLE
19	El SGDEA debe permitir la definición y parametrización de formatos de captura y el mantenimiento de los mismos, teniendo en cuenta los estándares, formatos abiertos y formatos recomendados por el AGN		X
20	El SGDEA debe permitir gestionar contenidos como: videos, audio, imagen, entre otros, de la misma forma que los documentos electrónicos de texto		X
21	El SGDEA no debe limitar el número de documentos que pueden ser capturados en cualquier serie o subserie.		X
22	Para la captura de documentos que tienen anexos el SGDEA deberá gestionarlos como unidad, restringiendo el uso de formatos comprimidos.		X
23	Cada vez que un archivo adjunto se captura como un documento por separado, el sistema debe permitir asignar el vínculo archivístico en el registro de metadatos.		
24	El SGDEA debe restringir y generar una alerta cuando se importe un documento en un formato no configurado en el sistema e indicar al usuario los formatos permitidos.	X	
25	El SGDEA debe permitir la captura automática de metadatos pertenecientes a mensajes de correo electrónico y sus archivos adjuntos.		X
26	El SGDEA debe permitir al usuario capturar un mensaje de correo electrónico asignándolo dentro de una serie, subserie o expediente.		X
27	El SGDEA debe tener la opción de capturar en una sola operación, varios correos electrónicos seleccionados manualmente.		X
28	El SGDEA debe soportar formatos de firma digital tales como CADES, PADES Y XADES		X

Tabla 4

Lista de chequeo, ítem búsqueda y presentación

N°	REQUISITO	CUMPLE	NO CUMPLE
33	El SGDEA debe permitir al usuario buscar y recuperar información que se encuentre dentro de documentos, listas de documentos y metadatos, de acuerdo al perfil de acceso.	X	
34	El SGDEA debe proporcionar herramientas para la generación de informes y reportes.		X
35	El SGDEA debe permitir generar informes que incluyan como mínimo gráficos y tablas.		X
36	El SGDEA debe proporcionar al usuario maneras flexibles de imprimir los documentos de archivo y sus correspondientes metadatos.		X
37	El SGDEA debe permitir que se impriman listas de los resultados de búsquedas.		X

Tabla 5

Lista de chequeo, ítem metadatos

N°	REQUISITO	CUMPLE	NO CUMPLE
38	El SGDEA debe permitir incorporar diferentes esquemas de metadatos.		X
39	El SGDEA debe permitir al usuario autorizado parametrizar modificar y aplicar las reglas de los elementos del esquema de metadatos.		X
40	El SGDEA debe presentar en pantalla los metadatos de los documentos capturados.		X
41	El SGDEA debe validar y controlar la entrada de los metadatos mínimos obligatorios.		X
42	El SGDEA permite la extracción automática de metadatos de los documento s al momento de la captura o cargue al sistema.		X

Tabla 6

Lista de chequeo, ítem control y seguridad

N°	REQUISITO	CUMPLE	NO CUMPLE
46	El SGDEA debe permitir la creación y administración de usuarios, roles y permisos.	X	
47	El SGDEA debe permitir revocar privilegios de un grupo o usuarios seleccionados.	X	
48	El SGDEA debe ofrecer opciones de configuración para asignar o eliminar roles después de un período predefinido automáticamente.		X
49	El SGDEA debe soportar diferentes mecanismos de autenticación.		X
50	El SGDEA debe generar y mantener pistas de auditoria inalterables de las acciones realizadas por cada uno de los usuarios que ingresan al sistema.		X
51	Cualquier intento de violación de los mecanismos de control de acceso deberá ser registrado en las pistas de auditoria.		X

52	El sistema debe impedir desactivar la generación y almacenamiento de las pistas de auditoria.	X

Tabla 7

Lista de chequeo, ítem flujos de trabajo

N°	REQUISITO	CUMPLE	NO CUMPLE
53	El SGDEA debe permitir diagramar y modelar flujos de trabajo.		X
54	El SGDEA debe generar los flujos de trabajo en un formato estándar.		X

Tabla 8

Lista de chequeo, ítem flujos electrónicos

N°	REQUISITO	CUMPLE	NO CUMPLE
55	El SGDEA debe permitir diagramar y modelar flujos electrónicos.		X
56	El SGDEA debe permitir visualizar de manera gráfica el estado de cada flujo electrónico.		X

Tabla 9

Lista de chequeo, ítem requisitos no funcionales

N°	REQUISITO	CUMPLE	NO CUMPLE
60	El SGDEA deberá estar disponible las 24 horas del día, 7 días de la semana, 365 días del año.	X	
61	El SGDEA debe ser 100% web y su administración y parametrización debe realizarse desde el navegador.	X	

El SID, Sistema de Información Documental, diseñado y usado en la Universidad Francisco de Paula Santander Ocaña, está orientado a la gestión documental, este tipo de sistemas está definido por el AGN como SGDE, que a diferencia de los SGDEA, el primero está orientado a la gestión documental y el segundo está orientado a la gestión del archivo de documentos, teniendo en cuenta esto, se puede calcular que un porcentaje mayor al 80% de los

requisitos propuestos por el modelo para la implementación de un sistema de gestión de documentos electrónicos de archivo, no se cumplen por el SID, dado que dicho sistema fue creado para fines diferentes al cual está siendo evaluado.

4.2.3 Dar un diagnostico técnico del estado del Sistema de Información Documental frente a los estándares requeridos.

El sistema de información documental de la Universidad Francisco De Paula Santander Ocaña denominado SID, en la actualidad permite la creación de una gran variedad de documentos, como son oficios, actas, citaciones, circulares y otros documentos, además se encarga de llevar un seguimiento a toda la correspondencia de la institución, almacenando la información de los documentos que se reciben y que se reparten al interior y exterior de la institución.

La percepción de los usuarios frente a la usabilidad y seguridad del SID, es bastante buena, lo cual se podría considerar como un sistema totalmente funcional para la gestión de documentos electrónicos, pero dada la diferencia que existe entre la gestión de documentos electrónicos y la gestión del archivo de documentos electrónicos, es necesario realizar un buen número de modificaciones para lograr adaptar el SID a lo modelado por el AGN.

También cabe resaltar que el modelo para la implementación de un archivo de documentos electrónicos fue creado en el año 2017 y el SID fue puesto en marcha 5 años previos al año mencionado.

En conclusión podemos determinar que el SID en estos momentos no cumple los requisitos necesarios, sería necesario poner bajo un estudio la posibilidad de realizar las modificaciones

necesarias al SID o de lo contrario la creación o adquisición de una herramienta que permita realizar propiamente la gestión del archivo según los establecidos por los entes reguladores.

4.3 Documentar una política institucional que garantice la seguridad del archivo digital de documentos, teniendo en cuenta los lineamientos necesarios establecidos por el Archivo General de la Nación.

4.3.1 Política institucional para la seguridad del archivo digital de documentos en la UFPSO.

4.3.1.1 Introducción

La gestión documental en la Universidad Francisco de Paula Santander Ocaña, es administrada y controlada por la dependencia de Secretaría General, tal como se encuentra descrito en el manual especifico de dicha dependencia. Para la elaboración de documentos, la dependencia de secretaria general cuenta con un sistema que facilita la elaboración y a su vez el almacenamiento de todos los documentos generados a través de dicho sistema.

Con el fin de ajustarse a políticas nacionales de manejo ambiental y usar las más modernas tecnologías en cuanto al uso de documentos electrónicos la institución desea implementar esta política que permita organizar el proceso de gestión de archivo de documentos electrónicos la cual será contemplada en la presente política.

4.3.1.2 Misión y Visión de la UFPS Ocaña.

Misión. La Universidad Francisco de Paula Santander Ocaña, institución pública de educación superior, es una comunidad de aprendizaje y autoevaluación en mejoramiento continuo, comprometida con la formación de profesionales idóneos en las áreas del

conocimiento, a través de estrategias pedagógicas innovadoras y el uso de las tecnologías; contribuyendo al desarrollo nacional e internacional con pertinencia y responsabilidad social.

Visión. La Universidad Francisco de Paula Santander Ocaña para el 2019, será reconocida por su excelencia académica, cobertura y calidad, a través de la investigación como eje transversal de la formación y el uso permanente de plataformas de aprendizaje; soportada mediante su capacidad de gestión, la sostenibilidad institucional, el bienestar de su comunidad académica, el desarrollo físico y tecnológico, la innovación y la generación de conocimiento, bajo un marco de responsabilidad social y ambiental hacia la proyección nacional e internacional.

4.3.1.3 Objetivo

Propender por el cuidado del archivo histórico de la institución, frente a la implementación de herramientas tecnológicas para la custodia de documentos electrónicos, teniendo en cuenta los modelos establecidos por el Archivo General de la Nación.

4.3.1.4 Alcance

Este documento proporciona la información necesaria para garantizar el uso de modelos nacionales frente al archivo de documentos electrónicos, en busca de adquirir o desarrollar un sistema de gestión de documentos electrónicos de archivo, para la universidad francisco de paula Santander Ocaña. Del buen uso de la herramienta desarrollada dependerá el éxito del archivo de documentos electrónicos. De igual forma todo este documento está sujeto a las políticas de seguridad tecnológicas y procedimentales establecidas por la división de sistemas de la institución. Por último, esta política no enmarca sanciones para quienes incumplan, se hará de

dichas sanciones la dependencia con facultades sancionatorias, dependiendo el fallo que se presente.

4.3.1.5 Referencias normativas.

La presente política está enmarcada bajo las normativas vigentes emanadas por el archivo general de la nación y las directrices de seguridad de la información contenidas en la norma técnica ISO 27001:2013.

4.3.1.6 Revisión y aprobación.

La respectiva revisión y aprobación de la presente política debe realizar en un periodo no mayor a un año y estará a cargo del Secretario General y el jefe de la división de sistemas, dadas las responsabilidades documentales y las directrices tecnológicas que la fundamentan.

4.3.1.7 Actualizaciones.

Las solicitudes de cambio a la presente política deben ser presentadas al Secretario General mediante el formato establecido para tal fin, llevando además la aceptación tecnológica de la división de sistemas.

4.3.1.8 Términos y definiciones.

AGN: Abreviatura de Archivo General de la Nación, ente regulador en Colombia de todo lo referente al archivo, encargado de documentar y hacer cumplir normas en pro de todos los procesos archivísticos y las actualizaciones incluso tecnológicas que se presentan en esta área.

Acceso: derecho, oportunidad, medio de encontrar, usar o recuperar información.

Autenticidad: característica técnica para preservar la seguridad de la información que busca asegurar su validez en el tiempo, forma y distribución. Así mismo, garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

Disponibilidad: característica de seguridad de la información, que garantiza que los usuarios autorizados tengan acceso a la misma y a los recursos relacionados, toda vez que lo requieran asegurando su conservación durante el tiempo exigido por ley.

Documento Electrónico: es la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares.

Documento Electrónico de Archivo: registro de la información generada, recibida, almacenada, y comunicada por medios electrónicos, que permanece en estos medios durante su ciclo vital. Es producida por una persona o entidad en razón de sus actividades y debe ser tratada conforme a los principios y procesos archivísticos.

Expediente: unidad documental compleja formada por un conjunto de documentos generados orgánica y funcionalmente por una instancia productora en la resolución de un mismo asunto.

Expediente Electrónico de Archivo: conjunto de documentos electrónicos de archivo relacionados entre sí. / El expediente electrónico es un conjunto de documentos electrónicos que hacen parte de un mismo trámite o asunto administrativo, cualquiera que sea el tipo de información que contengan y que se encuentran vinculados entre sí para ser archivados.

Integridad: característica técnica de seguridad de la información con la cual se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento asociados

a la misma. / Hace referencia al carácter completo e inalterado del documento electrónico. Es necesario que un documento esté protegido contra modificaciones no autorizadas.

Las políticas y los procedimientos de gestión de documentos deben decir qué posibles anotaciones o adiciones se pueden realizar sobre el mismo después de su creación y en qué circunstancias se pueden realizar. No obstante, cualquier modificación que se realiza debe dejar constancia para hacerle su seguimiento. Propiedad de salvaguardar la exactitud y estado completo de los documentos.

Metadatos para la Gestión de Documentos: información estructurada o semi-estructurada que permite la creación, gestión y uso de los documentos a lo largo del tiempo.

SGDE: Abreviatura de Sistema de Gestión de Documentos Electrónicos, según el AGN (2017) a un sistema de información que integra todas las actividades centradas en la gestión de documentos electrónicos que no necesariamente son documentos de archivo, ni están armonizados con los procesos de la gestión documental (documentos en producción, revisión, gestión o tramite)

SGDEA: Abreviatura de Sistema de Gestión de Documentos Electrónicos, según lo contempla el AGN (2017) se centra en los documentos cuando son declarados como documentos electrónicos de archivo y adicionalmente, ha sido pensado para integrar el archivo total independiente del ciclo de vida en los cuales se hallen los documentos.

4.3.1.9 Clasificación y organización documental.

La clasificación y organización documental se encuentran establecidas en las tablas de retención documental (TRD) el SGDEA debe permitir la completa gestión de dichas tablas, además debe garantizar la integridad de los expedientes una vez cerrados, no permitiendo la

adición, ni sustracción de ninguno de sus archivos, solo en casos excepcionales el administrador del sistema tiene las facultades para realizar estas acciones, con la salvedad que toda acción debe ser auditada y de fácil seguimiento.

Las series y subseries organizadas en las Tablas de Retención Documental registradas y gestionadas por el SGDEA deben cumplirse a cabalidad, dicha organización debe verse reflejada tanto en los archivos de documentos físicos como aquellos almacenados de forma electrónica.

Secretaría general es la dependencia encargada de aprobar cambios y modificaciones en las Tablas de Retención Documental, de ninguna manera se pueden realizar cambios sin su previa aprobación o autorización.

4.3.1.10 Retención y disposición

El SGDEA debe garantizar la retención de documentos, permitiendo diferentes formatos de audio, imágenes, video y texto, dichos documentos deben ser almacenados según lo previamente establecido por las tablas de retención documental, según su respectiva serie y subserie.

El SGDEA debe restringir algunos formatos y extensiones de archivo, dado que algunos archivos pueden ser un riesgo para el sistema y los servidores en los cuales se encuentra funcionando el sistema, también se debe garantizar la respuesta automática del sistema frente a cualquier intento de retención en formatos indebidos, dejando claridad de aquellos permitidos.

El SGDEA debe permitir la creación y modificación de tiempos de retención y disposición de documentos electrónicos, dejando huella auditable de todos los cambios y modificaciones que se realicen.

Para la eliminación de archivos, expedientes o series se debe garantizar la seguridad de dicha información permitiendo agregar pasos de seguridad, como lo es la confirmación por parte

de un rol administrador, para la eliminación de una respectiva serie o sub serie según lo establecido en la TRD.

En el caso de presentarse una migración se debe garantizar el éxito del proceso y debe existir la posibilidad de observar con detalle el proceso de migración, además se deben preservar los archivos en el sistema de origen hasta no emitir un mensaje de transferencia total y exitosa.

4.3.1.11 Búsqueda y presentación.

El SGDEA debe garantizar que las búsquedas no sean complicadas para los usuarios de tal manera que se pueda usar búsquedas complejas y teniendo en cuenta diferentes criterios, pero en cuanto a seguridad de la información el sistema no puede revelar información no autorizada a los usuarios según como se establezcan los roles, esta información puede ser contenido o metadatos del archivo.

El SGDEA se encuentra ligado al archivo de documentos de forma física y debe facilitar la búsqueda de archivos no solo electrónicos sino también debe brindar información de la ubicación física de los archivos.

La búsqueda de documentos dentro del sistema de archivo debe ser lo más flexible posible, permitiendo realizar búsqueda con características complejas y el uso de operadores booleanos que presenten en forma de lista un conjunto de documentos según las condiciones dadas.

El sistema de archivo no solo buscará archivos, sino que dentro de sus funciones de búsqueda debe generar reportes con tablas y gráficos de ser necesarios, dichas graficas deben estar relacionadas a los documentos y a la actividad del sistema, considerando la presentación de reportes de errores presentados en procesos de carga de documentos o todo lo relacionado al sistema.

4.3.1.12 Metadatos

El archivo de documentos electrónicos debe incluir además del contenido, todos los metadatos relacionados al mismo, los metadatos se capturaran tanto de los documentos generados por el sistema, como también por aquellos capturados o retenidos de diferentes maneras.

El SGDEA debe garantizar la gestión de metadatos y es de carácter obligatorio la generación de los mismos para los documentos elaborados por medio del sistema.

Los metadatos podrán ser modificados en su contenido o estructura solo por usuarios con permisos para tal fin, la integridad de la información dependerá del buen uso de roles y permisos en los usuarios.

4.3.1.13 Control y Seguridad.

Los roles y permisos de usuarios son deben realizarse y administrarse de forma dinámica en el SGDEA, permitiendo la creación de usuarios, la asignación de roles, la revocación de permisos entre otros.

El SGDEA debe capturar y almacenar en las pistas de auditoria, los elementos enmarcados en la tabla 10, que se presenta a continuación.

Tabla 10

Pistas de auditoria

PISTAS DE AUDITORIA
Toda acción realizada sobre cada documento, expediente, usuario y metadatos
Toda acción realizada en los parámetros de administración
Usuario que realiza la acción
Fecha y hora de la acción;
Cambios realizados a los metadatos
Cambios realizados a los permisos de acceso
Creación, modificación o eliminación de usuarios, grupos o roles del sistema

País, navegador, dirección ip, tipo de dispositivo, sistema operativo, desde donde fue abierta la sesión del sistema.

Las pistas de auditoria no deben ser alterables bajo ninguna circunstancia y de ninguna manera se podrán desactivar los seguimientos de las pistas de auditoria.

4.3.1.13 Requisitos no funcionales.

El SGDEA debe funcionar sobre una arquitectura tecnológica que garantice su disponibilidad las 24 horas al día, los 7 días de la semana, durante los 365 días del año, en caso de inactividad no prevista, se debe garantizar que dicha inactividad no supere las 10 horas trimestrales o las 40 horas anuales.

El sistema debe ser elaborado para funcionar en la web en su totalidad, su administración y funcionamiento debe realizarse por medio de un navegador y es permitido realizar módulos de escritorio que complementen su funcionamiento.

4.3.1.14 Copias de respaldo de la información

Dado que el sistema se encuentra funcionando en la web y aunque los riesgos frente a un fallo o perdida por ataques se encuentren minimizados al máximo, se hace necesario realizar respaldos a la información contenida en las bases de datos y a los archivos almacenados, con el fin de tener acceso a ellos en caso tal de presentarse una situación donde sea necesario recuperar información.

El SGDEA debe contar con un manejo de versiones a la hora de ser actualizado o mejorado en sus funciones permitiendo llevar control total de los cambios, dejando documentado dichos cambios y facilitando la restauración a versiones previas en caso de fallos.

4.3.1.15 En relación a los recursos humanos

La dependencia de personal, debe trabajar conjuntamente con Secretaria General, para buscar concientizar a todo el personal de la institución respecto a la información manejada en los diferentes sistemas de información, para ello es necesario que se realice una charla al inicio de cada semestre académico.

Las personas vinculadas a la institución deben recibir una capacitación respecto a buenas prácticas en el uso de sistemas de información, enseñándoles a manejar con prudencia sus credenciales de acceso y la importancia de la información que van a manejar desde el momento de quedar vinculados con la universidad.

A la hora de finalizar un contrato, por no renovación o por renuncia, se debe dar a conocer a la persona desvinculada, que la información que manejo durante el tiempo que laboró en la universidad es solo para el uso de la misma debe tener precaución a la hora de manejar dicha información.

Para el caso específico del cargo de administrador del sistema de gestión documental de archivo, es necesario capacitar al ingeniero a cargo en cuanto a la importancia de la información que maneja, dado que en sus manos se encuentra el archivo histórico de la institución y debe manejarse con total precaución para no incurrir en sanciones.

4.3.1.16 Vigencia

Este documento tiene una vigencia de 12 meses a partir de la fecha de aprobación mediante acto administrativo.

4.3.1.17 Sanciones

El incumplimiento a la presente Política da lugar a las sanciones que estipule el Comité Disciplinario de la UFPS Ocaña

4.3.1.18 Contacto

Secretaría General

PBX: (+57) (7) 5690088 - línea gratuita: 01-8000-121022 - Ext. 146

Correo: secretariageneral@ufpso.edu.co

Capítulo 5. Conclusiones

Se realizó el diagnóstico del estado de seguridad del Sistema de Información Documental (SID), se realizaron entrevistas, visitas y encuestas, donde se obtuvo la información necesaria para conocer la herramienta, también se logró concluir que la herramienta cumple con todos los lineamientos de seguridad, también se logró observar una excelente percepción en cuanto a la integridad de la información que se maneja y solo se encuentran inconformidades en el uso de ciertas funcionalidades a nivel operativo.

Se validaron los estándares legales que el Archivo General de la Nación ha venido proponiendo en cuanto al manejo de documentos electrónicos y su posterior procedimiento de archivo, se encontró que en la actualidad se usan dos tipos de herramientas tecnológicas que acompañan el proceso de archivo de documentos electrónicos, según el AGN se clasifican o se conocen como SGDE y SGDEA, y al contrastar con las funcionalidades del SID, se encontró que las características del SID lo enmarcan como un SGDE o Sistema de Gestión de Documentos Electrónicos y deben realizarse un buen número de modificaciones para llegar a considerarse un SGDEA o Sistema de Gestión de Documentos Electrónicos de Archivo.

Por último se documentó la política en búsqueda de garantizar la seguridad de la información del archivo digital, dejando abierta la posibilidad de usar el SID como SGDEA o la búsqueda de una nueva herramienta, dejando claro que la política está enfocada en la seguridad de la información y que no contempla todas las funcionalidades necesarias establecidas por el AGN para la implementación de un sistema de gestión de documentos electrónicos de archivo, contemplando dicho sistema como el conjunto de procedimientos, que usan o no medios electrónicos o magnéticos en procesos de archivo y digitalización.

Capítulo 6. Recomendaciones

Para lograr poner en funcionamiento el Sistema de Gestión de Documentos Electrónicos de Archivo, o como se denominaba en un principio, el Archivo de Documentos Electrónicos, es necesario adquirir una herramienta tecnológica adecuada o en su defecto realizar las modificaciones pertinentes al actual sistema de información documental – SID.

Debe realizarse un estudio presupuestal para decidir la viabilidad de adquirir una herramienta tecnológica o modificar el actual sistema, dado que las funciones encargadas al administrador del actual sistema no permiten avanzar de forma constante en las modificaciones necesarias.

Luego de poner en marcha el Sistema de Gestión de Documentos Electrónicos de Archivo debe tenerse en cuenta a cabalidad lo establecido en la política documentada en el presente documento, para asi garantizar el estado y la integridad de la información que se va a custodiar.

Referencias

Esteban Navarro, Miguel Ángel. “Los archivos de documentos electrónicos”. En: El profesional de la información, 2001, diciembre, v. 10, n. 12, pp. 41-45.

Archivo General de la Nación (s.f). Recuperado el 08 de junio de 2017, de http://www.archivogeneral.gov.co/sites/all/themes/nevia/PDF/Transparencia/ACUERDONo.003del17deFebrerode2015.pdf

Administración electrónica (2012). Recuperado el 10 de junio de 2017, de http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Documentacion/Metodologias-y-guias/Mageritv3/2012_Magerit_v3_libro1_metodo_ES_NIPO_630-12-171-8/2012_Magerit_v3_libro1_m%C3%A9todo_es_NIPO_630-12-171-8.pdf

Archivo General de la Nación, (2017) Modelo de requisitos para la implementación de un sistema de gestión de documentos electrónicos. Recuperado de http://observatoriotic.archivogeneral.gov.co/

Archivo General de la Nación, (2017) Requisitos mínimos de digitalización. Recuperado de http://observatoriotic.archivogeneral.gov.co/

Archivo General de la Nación, (2017) Guía de Implementación de un Sistema de Gestión de Documentos Electrónicos de Archivo - SGDEA. Recuperado de http://observatoriotic.archivogeneral.gov.co/

Archivo General de la Nación, (2014) Compilación normativa 2014. Recuperado de http://observatoriotic.archivogeneral.gov.co/

Duran, A. & Peinado, J (2016), Política de seguridad de la información de la secretaría general de la Universidad Francisco De Paula Santander Ocaña de acuerdo a la norma ISO/IEC 27001:2013 (Trabajo de Grado), Universidad Francisco de Paula Santander, Ocaña

Apéndices

ENTREVISTA DE RECONOCIMIENTO DEL SID

Entrevista dirigida al Ingeniero **Jose Luis Sarabia** encargado de dar soporte técnico al Sistema de Información Documental SID.

¿Cuáles son tus funciones en la Universidad Francisco de Paula Santander Ocaña?

¿Permítenos conocer una breve descripción del funcionamiento del SID?

¿El SW está desarrollado bajo que patrón de diseño, por ejemplo, MVC, MVC usando DAO y VO u otros patrones de diseño diferentes a los mencionados? ¿Cuales?

¿Con que motor de base de datos trabaja el sistema?

¿El sistema almacena una copia de los documentos generados, o solo son re construibles a través de la base de datos?

¿Quién es el encargado de seguir el funcionamiento del servidor, en el cual funciona el sistema?

¿Teniendo en cuenta sus conocimientos de programación, el SID podría convertirse en una herramienta que facilite la digitalización del archivo de documentos?

¿Desde su llegada a la administración del SID, que errores de seguridad del sistema ha detectado y posteriormente ha corregido?

¿Considera que la comprensión del código fuente de este sistema es sencilla, o le costó trabajo comprender algunas funcionalidades?

¿En cuanto a la usabilidad del sistema, cuales son los principales inconvenientes con los que se enfrentan los usuarios?

ENCUESTA

OBJETIVO: Detectar posibles riesgos de seguridad en el Sistema de Información Documental de la UFPSO.

Antes de comenzar la encuesta agradecemos tu sinceridad en cada una de las respuestas, dado que de esto depende el éxito de la presente investigación.

1. Describe las principales falencias que has detectado en el SID?

_____

_____

2. Marca con una x si tu contraseña tiene las siguientes características. (Puedes marcas varias opciones)

   ( ) Letras.
   ( ) Letras en mayúscula.
   ( ) Letras en minúscula.
   ( ) Números.
   ( ) Símbolos.

3. ¿Mantienes la contraseña oculta en algún lugar de tu escritorio o puesto de trabajo?
   Si __ No __
4. ¿En algún momento has almacenado un documento el SID, y sin tu autorización ha sido eliminado?
   Si __ No __
5. Si tuvieras las facultades para solicitar cambios al SID, ¿que cambios ordenarías que se hicieran?

   _____

   _____

Tu información y tu tiempo han sido demasiado valiosos para el desarrollo de esta investigación, ¡agradecemos enormemente tu colaboración!