RESUMEN – TRABAJO DE GRADO

AUTORES	**ÁLVARO JAVIER DURÁN SANJUÁN** **JORGE LUIS PEINADO RODRÍGUEZ**
FACULTAD	**INGENIERÍAS**
PLAN DE ESTUDIOS	**ESPECIALIZACION EN AUDITORÍA DE SISTEMAS**
DIRECTOR	**MSC TORCOROMA VELÁSQUEZ PÉREZ**
TÍTULO DE LA TESIS	**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**

RESUMEN

(70 palabras aproximadamente)

EL PRESENTE TRABAJO CONSISTE EN LA DEFINICIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA EL PROCESO DE SECRETARÍA GENERAL DE LA UFPS OCAÑA, LUEGO DE MODELAR EL NEGOCIO CON EL MÉTODO BPM, Y TOMANDO COMO BASE LOS RESULTADOS DE LA AUDITORÍA PASIVA QUE SE REALIZÓ A LA MISMA, BASADA EN LA NORMA ISO/IEC 27001:2013. POR ÚLTIMO, SE ELABORÓ EL DOCUMENTO FORMAL DE LA POLÍTICA MENCIONADA, QUE PROPORCIONA EL CONJUNTO DE LINEAMIENTOS PARA PROTEGER LOS ACTIVOS DE INFORMACIÓN DE SECRETARÍA GENERAL.

CARACTERÍSTICAS

PÁGINAS: 76	PLANOS: 0	ILUSTRACIONES: 10	CD-ROM: 1

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

AUTORES:

ÁLVARO JAVIER DURÁN SANJUÁN

JORGE LUIS PEINADO RODRÍGUEZ

Trabajo de grado para optar el título de Especialista en Auditoría de Sistemas

Directora:

MSC. TORCOROMA VELÁSQUEZ PÉREZ

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

FACULTAD DE INGENIERÍAS

ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS

Ocaña, Colombia Abril de 2016

Dedicatoria

Al Dios Todopoderoso, la persona que ha permitido llevar a cabo este estudio de posgrado, que por su voluntad ha dado siempre su respaldo.

Agradecimientos

Las autores agradecen:

A la MSc. Torcoroma Velásquez Pérez, por haberse desempeñado como directora del proyecto, dedicando valioso tiempo y esfuerzo en el desarrollo del presente trabajo.

Al MSc. Edwin Edgardo Espinel Blanco, quien facilitó la ejecución de diferentes actividades basadas en la información de la Secretaría General de la Universidad, así como a todo el personal del proceso que colaboró en la realización de las mismas.

A la Universidad Francisco de Paula Santander Ocaña.

Índice

Lista de Tablas

Lista de Figuras

Introducción

En definitiva, la información es el activo más valioso de cualquier organización, debido a esto, protegerla debe ser un objetivo claramente establecido. La necesidad de garantizar por lo menos la integridad, confidencialidad y disponibilidad de la información, ha conllevado a las organizaciones a ocuparse de lo que actualmente se conoce como sistema de gestión de la seguridad de la información (SGSI), apoyado por la trascendencia que han tomado las normas internacionales y las buenas prácticas para la gestión de dicho activo. Con miras a establecer el SGSI, organizaciones de todos los tipos han iniciado el proceso con la definición de políticas de seguridad de la información, de modo que son una herramienta organizacional que busca contribuir a la sensibilización del talento humano en cuanto a la importancia y criticidad de la información.

La Secretaría General de la Universidad Francisco de Paula Santander Ocaña (UFPS Ocaña) es precisamente un claro ejemplo de un proceso que es responsable de gestionar información crítica de la Institución; entre sus principales funciones se destaca: establecer las directrices para la producción documental institucional, agilizar el proceso administrativo de la Universidad teniendo como base la comunicación de todas las dependencias, y llevar a cabo la recepción de la correspondencia externa. El presente trabajo muestra la definición de la Política de Seguridad de la Información para el proceso de Secretaría General de la UFPS Ocaña como el producto de los resultados de la auditoría pasiva que se realizó a dicho proceso, basada en la norma ISO/IEC 27001:2013, que a su vez, se llevó a cabo luego de haber diseñado el modelo de negocio del mismo, con el método BPM.

Capítulo 1: Título

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.

1.1 Planteamiento del problema

La Secretaría General de la UFPS Ocaña es una dependencia de vital importancia para la institución; lo anterior, teniendo en cuenta que coordina el trabajo de los organismos de dirección y gobierno universitario, notificando las disposiciones emitidas por los mismos; así también, tiene a su cargo tanto la gestión documental, como las funciones de asesoría y de interpretación de normas internas.

De los procesos ejecutados por Secretaría General, dos de ellos ponen de manifiesto cómo esta dependencia se encarga de procesos críticos: el primero es la gestión documental, que entre otras actividades, implica la custodia y conservación de las comunicaciones internas de la universidad; y el segundo es la coordinación de las jornadas electorales que se realizan en la institución; en ambos casos, se identifica claramente la presencia de vulnerabilidades que puedan ser aprovechadas en el detrimento de la información.

Finalmente, considerando el significativo crecimiento que la Universidad ha tenido en los últimos diez años, y por ende, el aumento en el flujo de información, queda claro que se ha incrementado el riesgo de que pueda verse afectada la integridad, confiabilidad y disponibilidad

del activo más importante de la organización, debido la inexistencia de una política de seguridad de la información claramente definida.

1.2 Formulación del problema

¿Cómo por medio de una política de seguridad de la información se protege la información de Secretaría General de la UFPS Ocaña y se gestiona el riesgo que tiene la misma en pro de preservar su integridad, confiabilidad y disponibilidad?

1.3 Objetivos

1.3.1 Objetivo General

Definir la política de seguridad de la información para la Secretaría General de la Universidad Francisco de Paula Santander Ocaña de acuerdo a la norma ISO/IEC 27001.

1.3.2 Objetivos específicos

- Diseñar el modelo de negocio de Secretaría General con el método de Gestión de Procesos de Negocio (BPM).
- Realizar una auditoría pasiva a la Secretaría General basados en la norma ISO/IEC 27001:2013.
- Elaborar el documento formal que incorpore la política de seguridad de la información de la Secretaría General de la UFPS Ocaña.

1.4 Justificación

La información se encuentra expuesta a infinidad de amenazas que no están asociadas solamente a la tecnología, como probablemente algunas organizaciones lo han visto, olvidando que garantizar la seguridad de la misma es, en principio, una responsabilidad corporativa y de gestión. En este sentido, una manera de defenderse ante tales amenazas es mediante la adopción de lineamientos estipulados por estándares internacionales que plantean el diseño de una política de seguridad de la información.

La definición formal de una política no solo contribuye a la preservación y cuidado de la información, sino que también alinea la institución a las bases legales exigidas actualmente en el territorio nacional. Es por esto que El (Archivo General de la Nación [AGN], 2015), dicta el marco legal relacionado con la gestión documental, y mediante el Acuerdo 003 de 17 de febrero de 2015, presenta medidas para garantizar aspectos fundamentales de la información: originalidad, autenticidad, integridad, disponibilidad y confiabilidad, así como la conservación a largo plazo de los documentos electrónicos. Asimismo, la Política de Archivos del AGN en la línea de acción de organización y preservación, define que debe garantizarse la conservación y accesibilidad de los archivos, resultados esperados con el establecimiento de la política de seguridad de la información.

Por otro lado, según el eje estratégico Sostenibilidad administrativa y financiera del Plan de Desarrollo 2014 – 2019 de la (Universidad Francisco de Paula Santander Ocaña [UFPSO],2013) es pertinente definir una política de seguridad de la información por dos razones trascendentales: primero, se puede considerar como un primer acercamiento a una futura

certificación en el estándar internacional ISO/IEC 27001:2013, y segundo, contribuye al mejoramiento de la gestión segura de la información de Secretaría General, con el fin de minimizar la afectación que se le pudiera generar.

1.5 Hipótesis

Con la política de seguridad de la información se logrará minimizar los factores de riesgo e identificar las vulnerabilidades de la información manejada por el proceso de Secretaría General de la UFPS Ocaña.

1.6 Delimitaciones

1.6.1 Delimitación geográfica

El desarrollo de este proyecto de grado tiene lugar en la dependencia Secretaría General de la UFPS Ocaña, sede el Algodonal vía Acolsure, en el municipio de Ocaña, Colombia.

1.6.2 Delimitación temporal

Este proyecto tendrá un tiempo de realización de siete (7) meses, de acuerdo a las diferentes actividades a realizar durante el desarrollo del mismo.

1.6.3 Delimitación conceptual

Los conceptos pertenecientes al área de conocimiento de este proyecto se relacionan con la Seguridad de la Información, Sistema de Gestión de Seguridad de la Información (SGSI), Riesgos, Políticas de Seguridad de la Información y Controles.

1.6.4 Delimitación operativa

Este proyecto diseñará una Política de Seguridad de la Información para la dependencia Secretaría General de la UFPS Ocaña, buscando establecer controles que reduzcan los riesgos de afectación sobre la información.

Capítulo 2: Marco referencial

2.1 Marco histórico

La preocupación por asegurar la información se remonta a las antiguas civilizaciones en las que mediante técnicas como los jeroglíficos, se inició lo que hoy se conoce como cifrado. En la Segunda guerra Mundial, por ejemplo, Alemania utiliza la Máquina Enigma para cifrar información. Actualmente, en diferentes campos, resguardar y proteger la información es imprescindible, y por ello, se introdujeron buenas prácticas para la gestión de la seguridad de la información, que a su vez, dieron lugar a la denominadas "políticas de seguridad".

Una de los estándares más reconocidos mundialmente para la gestión de la seguridad de la información es la serie ISO/IEC 27000 que proviene de la norma BS 7799 de la British Standars Institution. Esta familia de normas se compone de siete estándares, de los cuales el ISO/IEC 27001 contiene los requisitos del sistema de gestión de seguridad de la información, que además, contempla en su primer dominio la definición de políticas.

Multitud de organizaciones en todo el mundo, vienen adoptando buenas prácticas para la gestión de la información y gran parte de ellas con miras a obtener la certificación en normas como la ISO/IEC 27001. A continuación se presentan trabajos que se han realizado en esta área:

2.1.1 Política detallada de usuario final para la seguridad de la información

Este trabajo tuvo lugar en la Pontificia Universidad Católica del Ecuador y emitida desde la Oficina de Seguridad de la Información.

De acuerdo con (Pontificia Universidad Católica del Ecuador ,[PUCE], 2012), el objetivo de la presente política es alcanzar un grado aceptable y sostenido de seguridad de los computadores personales, de la información almacenada en ellos y el uso de los servicios de correo electrónico e Internet, en función del perfil de riesgos tecnológicos y las vulnerabilidades, para lo cual se requiere normar los aspectos relacionados con las seguridades físicas y lógicas que deben precautelar los usuarios finales de los equipos, servicios y aplicaciones tecnológicas. En particular, se proporciona una guía a los usuarios para la utilización segura, eficiente y efectiva de los computadores personales, y de los servicios de correo electrónico e Internet, con el fin de racionalizar y optimizar el uso de dichos recursos y servicios y asegurar una mayor calidad en el desarrollo de las funciones.

2.1.2 Generación de un plan de capacitación para el sector privado en temas de ciberseguridad y de seguridad de la información

En Colombia, por parte del Ministerio de las Tecnologías de la Información y la Comunicación, dentro de sus objetivos de desarrollo 2011- 2014 ha planteado el impulso a la masificación y uso eficiente de las TIC para el cumplimiento de los objetivos del Gobierno Nacional de: disminuir pobreza, aumentar seguridad y aumentar empleo.

Bajo esa concepción se ha hecho necesario también la capacitación en temas relacionados con la seguridad de la información de acuerdo a lo planteado en el documento CONPES 3701 por parte del Departamento Nacional de Planeación : "Solicitar al Ministerio de Tecnologías de la Información y las Comunicaciones realizar las gestiones necesarias con el Ministerio de Educación Nacional y el SENA, para la generación de un plan de capacitación para el sector privado en temas de ciberseguridad y de seguridad de la información."(MINTIC, 2011, p.35)

El documento CONPES tiene como objetivo central fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético (ciberseguridad y ciberdefensa), creando el ambiente y las condiciones necesarias para brindar protección en el ciberespacio.

2.1.3 Política de Seguridad de la Información de la Universidad Distrital Francisco José de Caldas

En la Universidad Distrital Francisco José de Caldas (UD,s,f).

Los sistemas y red de información enfrentan amenazas de seguridad que incluyen, entre muchas otras: el fraude por computadora, espionaje, sabotaje, vandalismo, fuego, robo e inundación. Las posibilidades de daño y pérdida de información por causa de código malicioso, mal uso o ataques de denegación de servicio se hacen cada vez más comunes. Con la promulgación de la Política de Seguridad de la Información la institución formaliza su compromiso con el proceso de gestión responsable de información que tiene como objetivo

garantizar la integridad, confidencialidad y disponibilidad del importante activo, teniendo como eje el cumplimiento de los objetivos misionales. (UD,s.f)

2.1.4 Modelo de gestión de seguridad de la información ICETEX

De acuerdo con El (Instituto Colombiano de Crédito Educativo y Estudios Técnicos en el Exterior [ICETEX], s.f.): La información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección de sus propiedades más significativas como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad.

Consciente de sus necesidades actuales, ICETEX implementa un modelo de gestión de seguridad de la información como la herramienta que permite identificar y minimizar los riesgos a los cuales se expone la información, ayuda a la reducción de costos operativos y financieros, establece una cultura de seguridad y garantiza el cumplimiento de los requerimientos legales, contractuales, regulatorios y de negocio vigentes. El proceso de análisis de riesgos de los activos de información es el soporte para el desarrollo de las Políticas de Seguridad de la Información y de los controles y objetivos de control seleccionados para obtener los niveles de protección esperados en ICETEX; este proceso será liderado de manera permanente por el Oficial de Seguridad de la Información.

2.1.5 Fuga de datos a nivel mundial: El elevado costo de las amenazas internas

En un estudio de seguridad a nivel mundial sobre la fuga de información reveló que la pérdida de datos debido a la conducta de los empleados es una amenaza más grande de lo que creen muchos profesionales de TI. Encargado por Cisco y realizado por InsightExpress, una compañía de investigación de mercado con sede en Estados Unidos, el estudio encuestó a más de 2000 empleados y profesionales de tecnología de la información en 10 países. Cisco seleccionó los países por sus culturas sociales y comerciales distintivas, a fin de comprender mejor si estos factores influyen en la fuga de información.

En manos de empleados desinformados, descuidados o descontentos, cada dispositivo que accede a la red o almacena datos se transforma en un riesgo potencial para la propiedad intelectual o la información confidencial de los clientes. Para acrecentar aún más el problema, en muchas empresas existe una dicotomía entre lo que creen los profesionales de TI y la realidad actual del entorno de seguridad. Los nuevos hallazgos muestran que las "amenazas internas" pueden causar mayores pérdidas financieras que los ataques provenientes del exterior. (CISCO, 2008)

- La preocupación principal del 33% de los profesionales de TI era la pérdida o robo de datos a través de dispositivos USB.

- El 39% de los profesionales de TI a nivel mundial estaba más preocupado por las amenazas provenientes de sus propios empleados que por la de los piratas informáticos externos.
- El 27% de los profesionales de TI admitió que no conocía las tendencias de la pérdida de información de los últimos años.

Mitigar la fuga de información desde fuentes internas es un desafío complicado. Las empresas deben aprovechar cada oportunidad que tengan para comprender mejor cómo la conducta y las intenciones de los empleados se relacionan con la seguridad, y para hacer de la seguridad una prioridad en cada aspecto de las operaciones comerciales.

2.1.6 Política de la seguridad de la información en la Alcaldía de Río de Oro, Cesar

Según lo expuesto por (Areniz &Sánchez, 2014) para definir el nivel de seguridad en la Alcaldía del municipio de Río de Oro, departamento del Cesar, se realizó una investigación mediante la aplicación de encuestas dirigida al personal de planta y OPS con el fin de determinar el nivel de efectividad de los controles que actualmente aseguran la información manejada por esta.

Este estudio fue desarrollado en el año 2014 y finalmente, se recomendó aplicar las Políticas de Seguridad de la Información ajustadas a la Alcaldía, para fomentar el compromiso de uso.

2.2 Marco contextual

Este trabajo se llevará a cabo en la dependencia Secretaría General de la UFPS Ocaña, que tiene sus instalaciones en el municipio de Ocaña, departamento Norte de Santander, Colombia. Para esta dependencia antes mencionada, se definirá la política de seguridad de la información.

2.3 Marco conceptual

Los conceptos pertinentes a este proyecto son: seguridad de la información, características principales de la información, sistema de gestión de seguridad de la información, control, amenaza, vulnerabilidad, riesgo, política de seguridad de la información, política de seguridad informática y tecnología de información.

2.3.1 Seguridad de la información

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

2.3.2 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.

2.3.3 Sistema de Gestión de Seguridad de la Información (SGSI)

SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System.

2.3.4 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."

2.3.5 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.

2.3.6 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.

2.3.7 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.

2.3.8 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."

2.3.9 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

En lo correspondiente a la temática del presente trabajo compete exponer lo relacionado con las buenas prácticas para el manejo de la información.

Como buenas prácticas para el manejo de información aparece la familia de normas ISO/IEC 27000, estas normas han sido muy aceptadas por las empresas de todo tipo a nivel internacional, también es importante mencionar los marcos de trabajo como CobIT e Itil que a un nivel corporativo más alto también definen aspectos relacionados con la protección de la información.

2.4.1 Norma ISO/IEC 27000

Según (INCONTEC, 2005) esta norma ha sido elaborada para suministrar requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información. La adopción de un sistema de gestión de seguridad de la información es una decisión estratégica para una organización.

La norma ISO/IEC 27000 es más precisamente un conjunto de normas las cuales cada una trata un aspecto determinado dentro del área de estudio, a continuación se describe brevemente las normas más reconocidas de la familia 27000

ISO 27001: Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la única norma de la familia que es certificable.

Ciclo PDCA: Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001, se utiliza el ciclo continuo PDCA, tradicional en los sistemas de gestión de la calidad.

• Plan (planificar): establecer el SGSI.

• Do (hacer): implementar y utilizar el SGSI.

• Check (verificar): monitorizar y revisar el SGSI.

• Act (actuar): mantener y mejorar el SGSI.

ISO 27002: Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. En la más reciente versión ISO/IEC 27002:2013 presenta 14 dominios, 35 objetivos de control Y 114 controles.

ISO 27003: Consiste en una guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases.

ISO 27004: Especifica las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados. Estas métricas se usan fundamentalmente para la medición de los componentes de la fase "Do" (Implementar y Utilizar) del ciclo PDCA.

ISO 27005: Establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está

diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.

ISO 27006: Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.

ISO 27007: Es una guía para la aplicación de auditorías a un SGSI como complemento especificado en ISO 19011.

2.4.2 ITIL

ITIL - Information Technology Infrastructure Library, es una colección de las mejores prácticas observadas en la industria de TI. Es un conjunto de libros en los cuales se encuentran documentados todos los procesos referentes a la provisión de servicios de tecnología de información hacia las organizaciones.

ITIL presenta procedimientos, roles, tareas, y responsabilidades que se pueden adaptar a cualquier organización de TI, genera una descripción detallada de mejores prácticas, que permitirán tener mejor comunicación y administración en la organización de TI.

La gestión de servicios de TI se refiere a la planificación, aprovisionamiento, diseño, implementación, operación, apoyo y mejora de los servicios de TI que sean apropiados a las necesidades del negocio. ITIL proporciona un marco de trabajo de mejores prácticas integral, consistente y coherente para la gestión de servicios de TI y los procesos relacionados,

la promoción de un enfoque de alta calidad para el logro de la eficacia y eficiencia del negocio en la gestión de servicios de TI. ITIL intenta respaldar más no fijar los procesos de negocio de una organización. En este contexto, la OGC no aprueba el término "Cumplimiento con ITIL". El papel del marco de trabajo de ITIL es describir los enfoques, las funciones, los roles y procesos en los que las organizaciones pueden basar sus propias prácticas. El rol de ITIL es brindar orientación en el nivel organizacional más bajo que pueda aplicarse. Debajo de ese nivel, para implementar ITIL en una organización se requieren los conocimientos específicos de sus procesos de negocio para ajustar ITIL a fin de lograr una eficacia óptima (IT Governance Institute, 2008).

2.4.3 COBIT

CobiT, (Control Objectives for Information and Related Technology), de acuerdo a (Fonseca,2011), es una herramienta de Tecnología de Información (TI) para uso de las entidades. (...) el CobiT proporciona buenas prácticas para los procesos de negocios y la información resultantes de la aplicación combinada de recursos que requieren ser administrados, apoyados por la tecnología de información. Estas prácticas están enfocadas más al fortalecimiento del control que a su ejecución, siendo una estructura apropiada para la seguridad y el control de TI. CobiT, plantea que los principios básicos de su Marco de Referencia se encuentran representados por siete (7) objetivos de control: efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad. Este modelo enlaza los objetivos de negocios con los objetivos de TI, proporcionando métricas y modelos de madurez para evaluar el grado de

confiabilidad o dependencia que el negocio puede tener en un proceso, al alcanzar las metas y objetivos deseados.

Estos requerimientos interactúan con cuatro (4) Dominios: Planteamiento y organización; Adquisición e implementación; Servicios y soporte; y, Monitoreo y evaluación. Para que una compañía asegure el logro de los objetivos de soporte del TI e su negocio de acuerdo a los lineamientos del CobiT, primero debe establecer las necesidades de los objetivos de control que definen las metas finales para implementar políticas, procedimientos y prácticas en la estructura organizacional, y segundo, necesita diseñar los objetivos de evaluación para mejorar sus requerimientos e implementar herramientas gerenciales para monitorear las mejoras efectuadas (p.26)

2.5 Marco legal

2.5.1 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).

2.5.2 Ley 1273 del 5 de enero de 2009

El Congreso de Colombia decretó: "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones" (MINTIC,2009).

2.5.3 Ley 1581 del 17 de octubre 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).

2.5.4 Artículo 71 de la Constitución Política de Colombia

Este artículo otorga al Estado la responsabilidad de promover el desarrollo tecnológico e incentivar a quienes se dediquen a trabajar en este ámbito "(…) El Estado creará incentivos para personas e instituciones que desarrollen y fomenten la ciencia y la tecnología y las demás

manifestaciones culturales y ofrecerá estímulos especiales a personas e instituciones que ejerzan estas actividades (Senado 1991)".

Es de gran importancia lo que se acaba de mencionar puesto que es precisamente la Constitución Política que estando por encima de todas las leyes, ampara la actividad de desarrollo tecnológico.

Capítulo 3: Diseño metodológico

3.1 Tipo de investigación

La presente investigación será de carácter descriptivo, su propósito es elaborar una política de seguridad de la información para la dependencia Secretaría General de la UFPS Ocaña, partiendo del estado actual el cual fue analizado con la elaboración de algunas auditorías en diferentes aspectos del proceso.

3.2 Población

Al considerar el territorio al cual corresponde la realización de este trabajo de grado, se identifica la información manejada por la Secretaría General de la UFPS Ocaña, por tanto, la población está conformada por los funcionarios pertenecientes a este proceso: quienes laboran en la oficina Secretaría General, Archivo Central e Histórico, y en Ventanilla Única.

3.3 Muestra

La muestra abarca la totalidad la población de la dependencia, contemplando además los procesos, la tecnología e información de la Secretaría General.

3.4 Técnicas e instrumentos de recolección de información

Luego de haber revisado las definiciones de algunas de las técnicas de recolección de datos como la observación y la encuesta, y teniendo en cuenta lo que dice Grasso:

> (…)La encuesta permite obtener datos de manera más sistemática que otros procedimientos de recolección de datos. Hace posible el registro detallado de los datos, el estudiar una población a través de muestras con garantías de representatividad, la generalización de las conclusiones con conocimiento de los márgenes de error y el control de algunos factores que inciden sobre el fenómeno a observar, como por ejemplo las formas de efectuar las preguntas y el contexto en que están se formulan y contestan (Grasso, 2006, pág.13)

Es posible determinar la encuesta y la observación técnicas de recolección de datos para este proyecto, además, revisión documental e instrumentos como listas de chequeo basadas en las Normas NTC ISO 27001, NTC ISO 27002.

Capítulo 4: Presentación de resultados

4.1 Diseño del modelo de negocio de Secretaría General

Se diseñó el modelo de negocio de la Secretaría General utilizando el método de Gestión de Procesos de Negocio (BPM).

4.1.1 Misión de la UFPS Ocaña

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.

4.1.2 Visión de la UFPS Ocaña

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 hacía la proyección nacional e internacional.

4.1.3 Objetivos de la UFPS Ocaña

- Investigación y formación académica
- Desarrollo físico y tecnológico
- Impacto y proyección social
- Visibilidad nacional e internacional
- Bienestar institucional
- Sostenibilidad administrativa y financiera

4.1.4 Estructura orgánica de la UFPS Ocaña

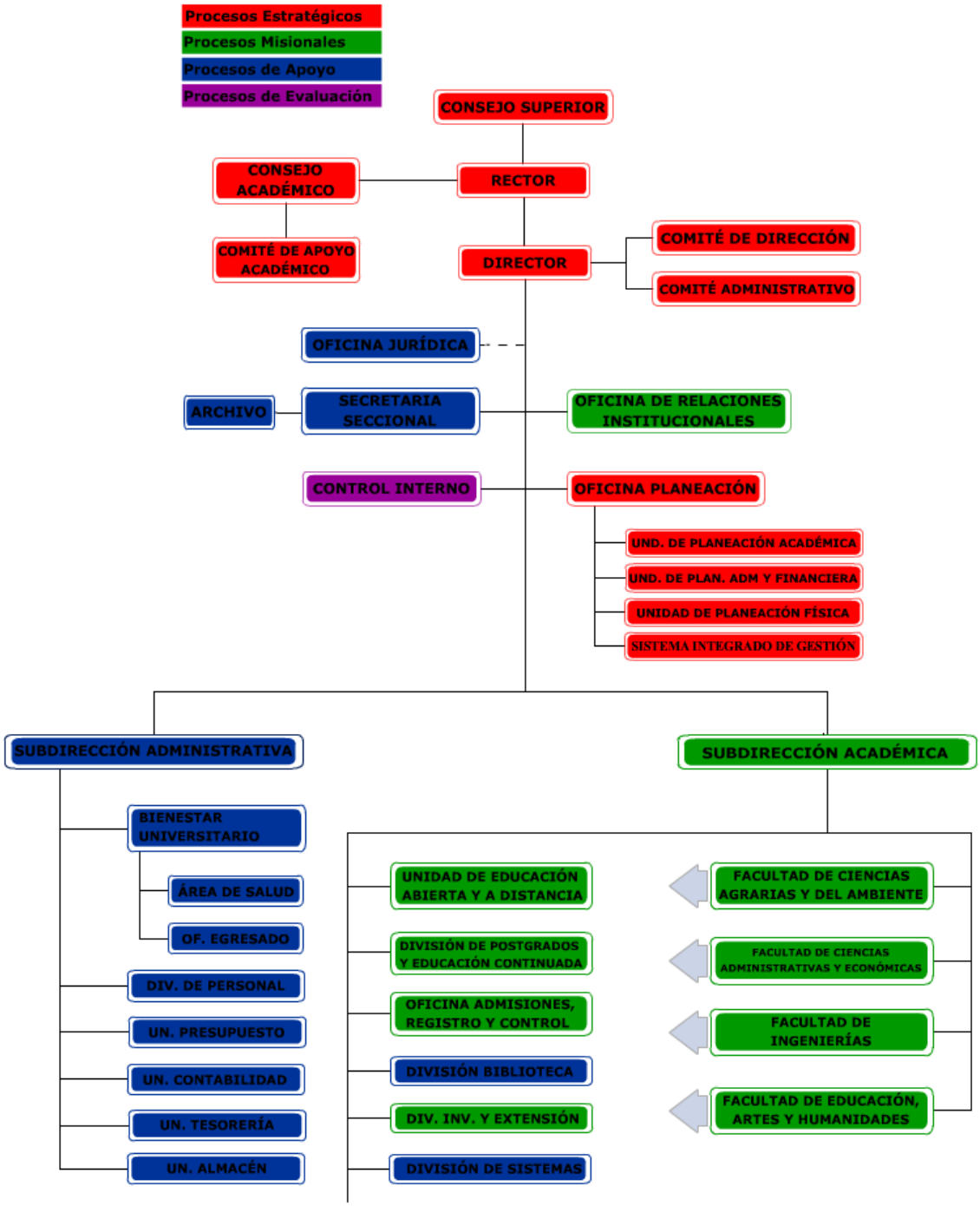


Figura 1. Estructura orgánica de la Universidad Francisco de Paula Santander Ocaña. (2016). Estructura Orgánica [Gráfico]. Recuperado de https://ufpso.edu.co/Estructura

4.1.5 Cadena de valor de la UFPS Ocaña

La cadena de valor describe claramente los procesos que se llevan a cabo al interior de la UFPS Ocaña y la manera como se desarrollan las actividades, pueden identificarse los procesos misionales donde fundamenta su carácter de institución de educación superior, también se identifican los procesos estratégicos y aquellos sirven de apoyo al funcionamiento. Ver figura 2.

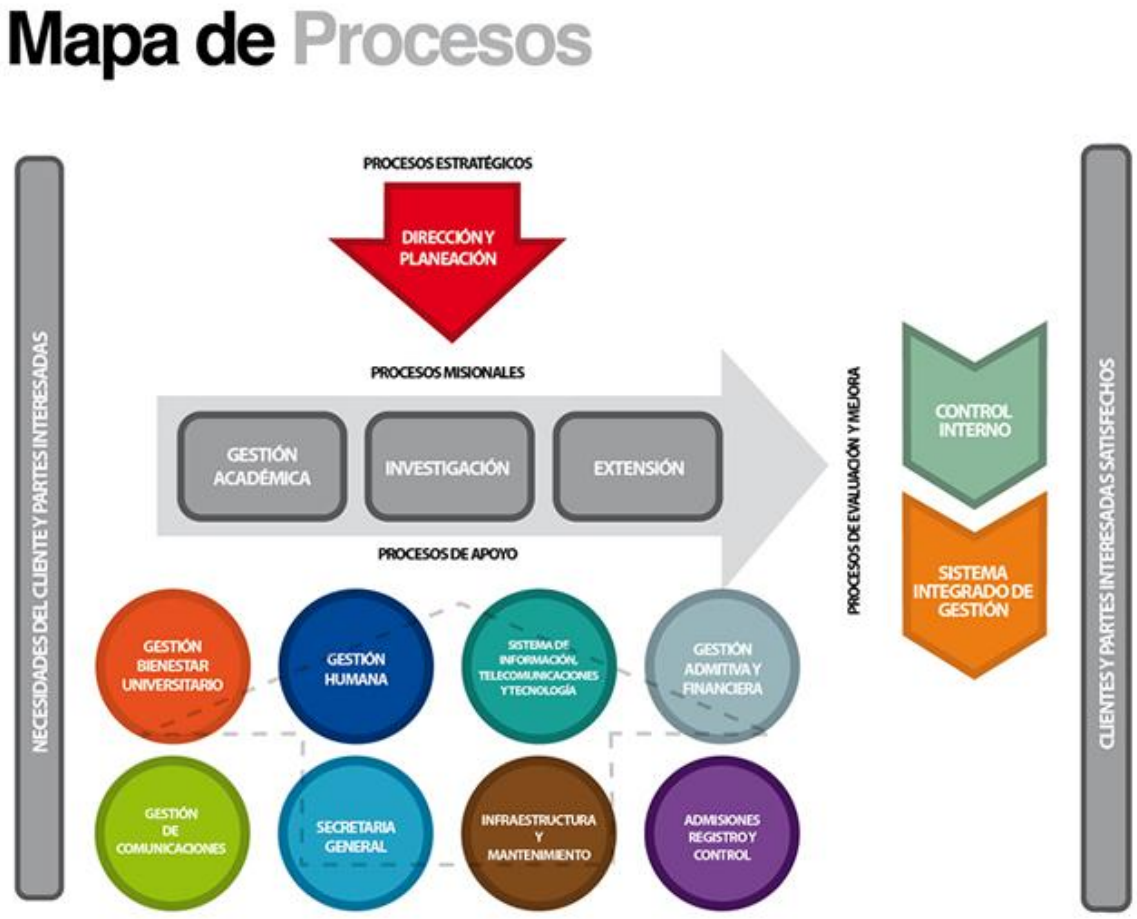


Figura 2. Mapa de procesos de la Universidad Francisco de Paula Santander Ocaña. (2016). Mapa de Procesos [Gráfico]. Recuperado de https://ufpso.edu.co/sig/procedimientos_sig

4.1.6 Proceso de Secretaría General

La UFPS Ocaña ha logrado consolidar un modelo de operación por procesos alineando su funcionamiento a normas internacionales lo que ha permitido lograr la certificación en la norma ISO 9001-2008. De esta manera, Secretaría General es un proceso de apoyo, adscrito a la dirección de la Seccional con funciones de elaboración, refrendación y notificación de los actos administrativos y académicos de la Dirección de la Universidad y de los diferentes organismos colegiados de dirección y gobierno de la Seccional.

En la figura 3 se muestra el diagrama de descripción del proceso Secretaría General, en la cual se puede observar aquellos elementos que son insumo o entrada para las actividades que se llevan a cabo, así como las salidas que generan, dicho funcionamiento está regulado por las normativas nacionales e institucionales, también permite identificar el personal responsable y aquellos procesos que apoyan y supervisan los procedimientos de Secretaría General.

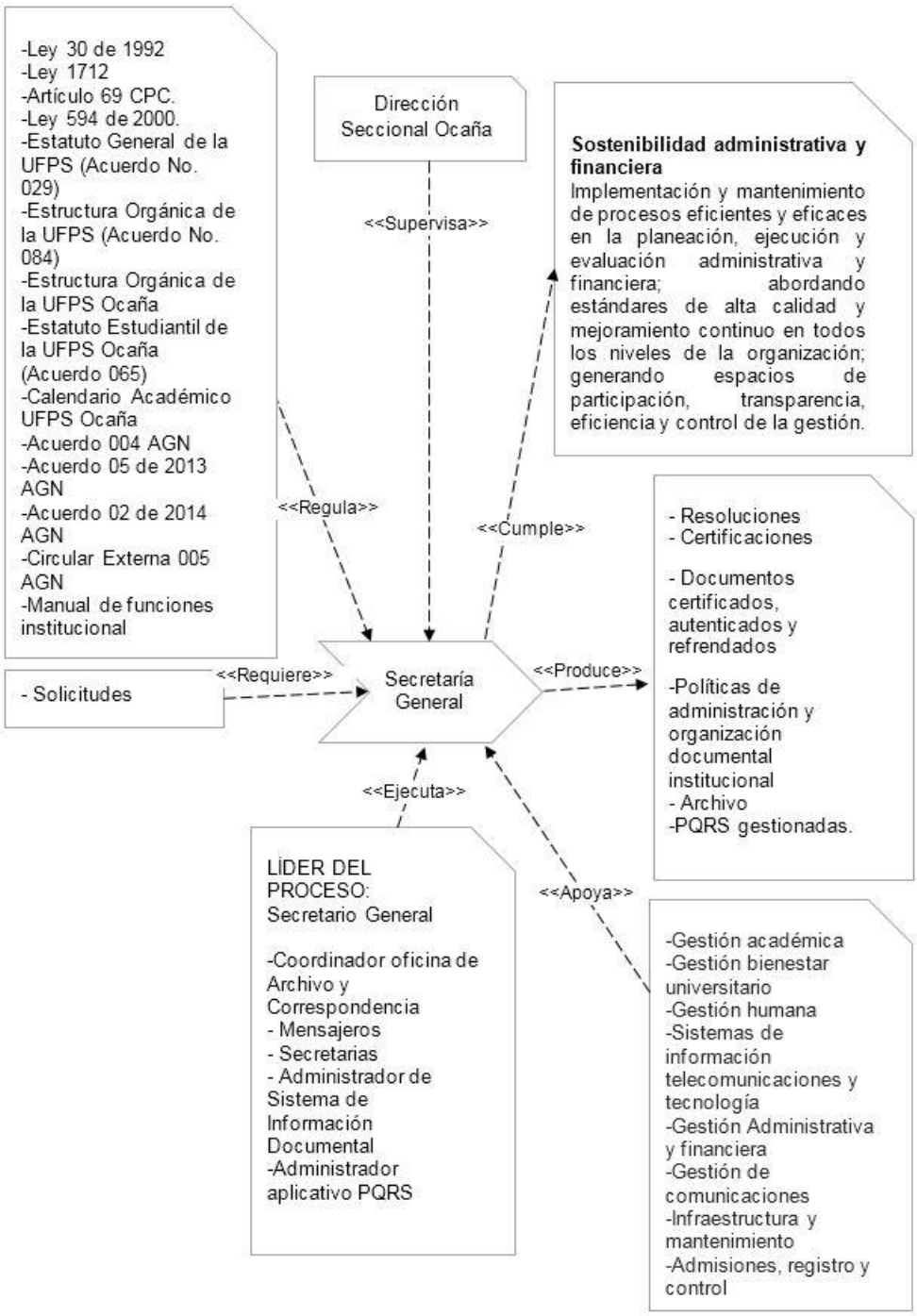


Figura 3. Diagrama de descripción de Secretaría General (2016).

4.1.6.1 Subprocesos de Secretaría General

Luego del estudio y análisis de la documentación del proceso, se logró establecer que sus funciones se organizan en cuatro subprocesos: Proceso electoral, Gestión documental, Gestión de PQRS, Certificación y refrendación, tal como se muestra en la figura 4.

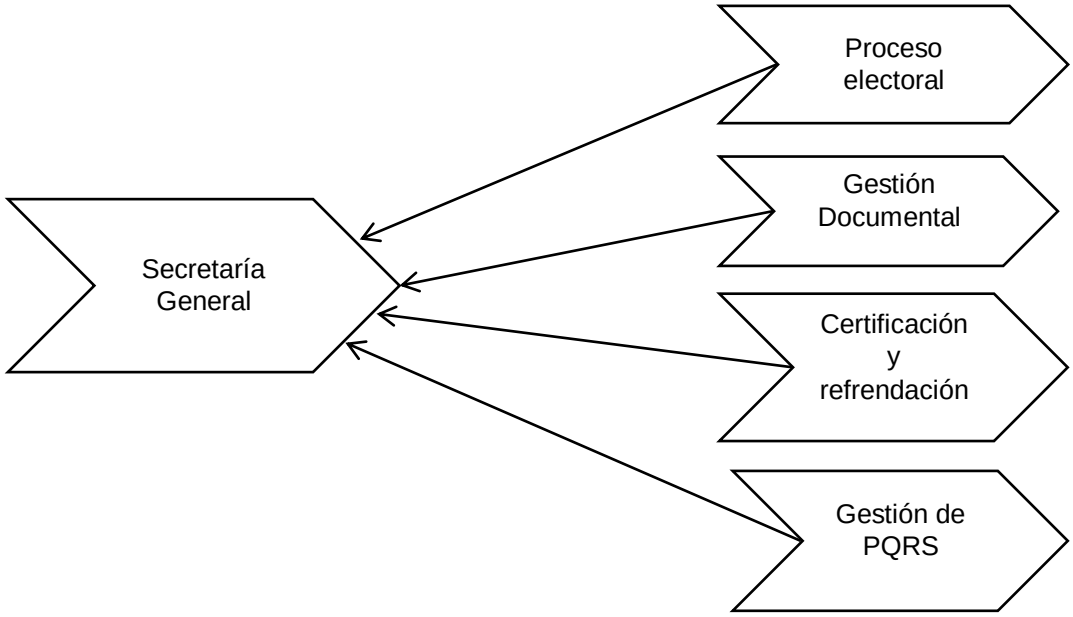


Figura 4. Diagrama de subprocesos de Secretaría General. (2016).

A continuación se presentan los diagramas de descripción de los subprocesos de Secretaría General.

4.1.6.2 Subproceso Electoral

La Universidad, como institución de carácter público debe elegir democráticamente de acuerdo a la constitución todo organismo de gobierno; de este modo, el subproceso Electoral maneja las actividades relacionadas con: organización de los procesos electorales para representaciones estudiantiles, administrativas, docentes y los que designe la UFPS Sede Central.

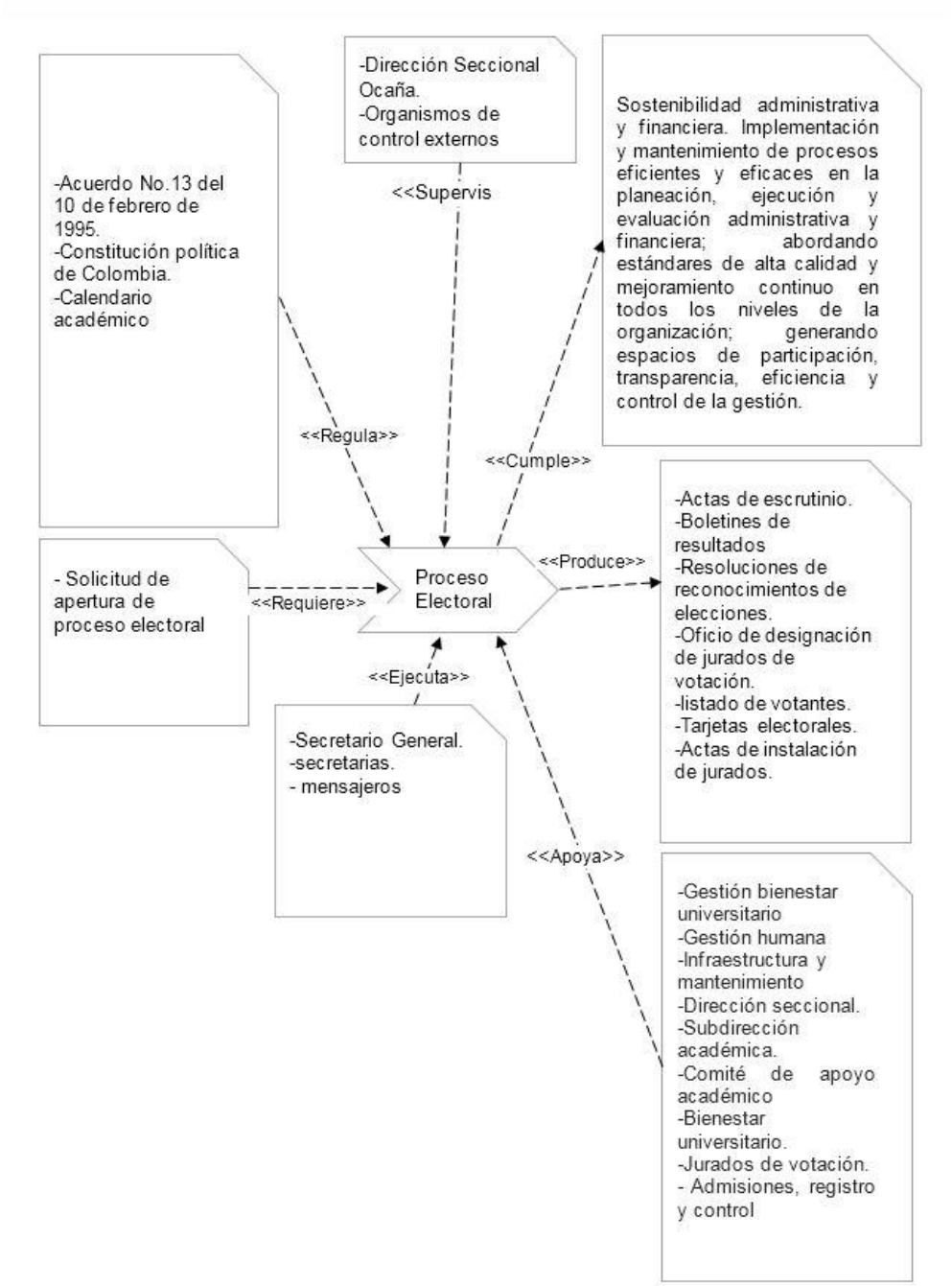


Figura 5. Diagrama de descripción del subproceso Electoral. (2016).

4.1.6.3 Subproceso Gestión documental

Al analizar el funcionamiento de Secretaría General se enmarcó dentro del subproceso Gestión Documental, actividades como: generación de los documentos realizados por las

dependencias en cumplimiento de las funciones particulares de cada oficina, verificación, recepción, radicación, clasificación y distribución de las comunicaciones oficiales, control de documentos oficiales, y procedimientos orientados a la organización de fondos acumulados, como se aprecia en la figura 6.

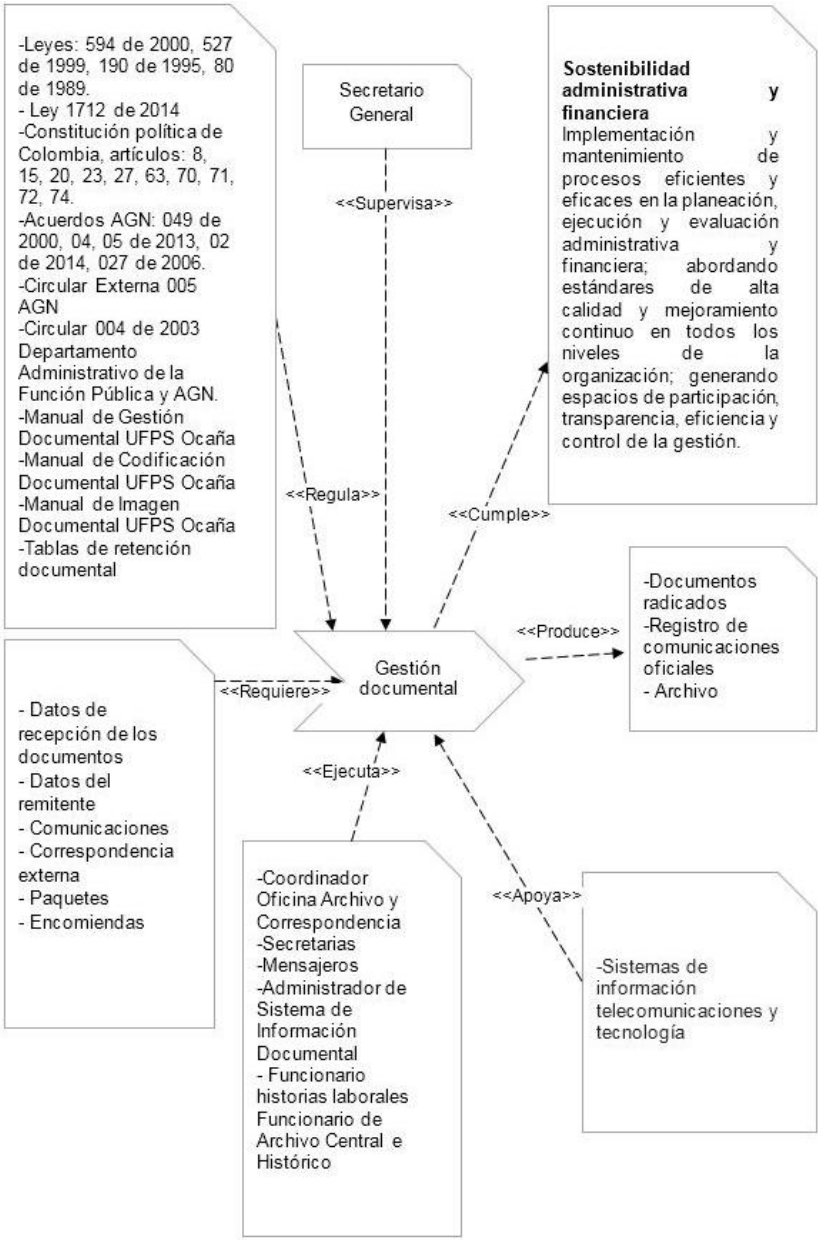


Figura 6. Diagrama de descripción del subproceso Gestión Documental. (2016).

4.1.6.4 Subproceso Certificación y Refrendación

Secretaría General es el proceso encargado de los aspectos notariales en la Universidad, es por esto que a su cargo se encuentran como responsabilidades la refrendación y certificación, esta última, dando fe de los actos administrativos de la Dirección de la Institución. Ver figura 7.

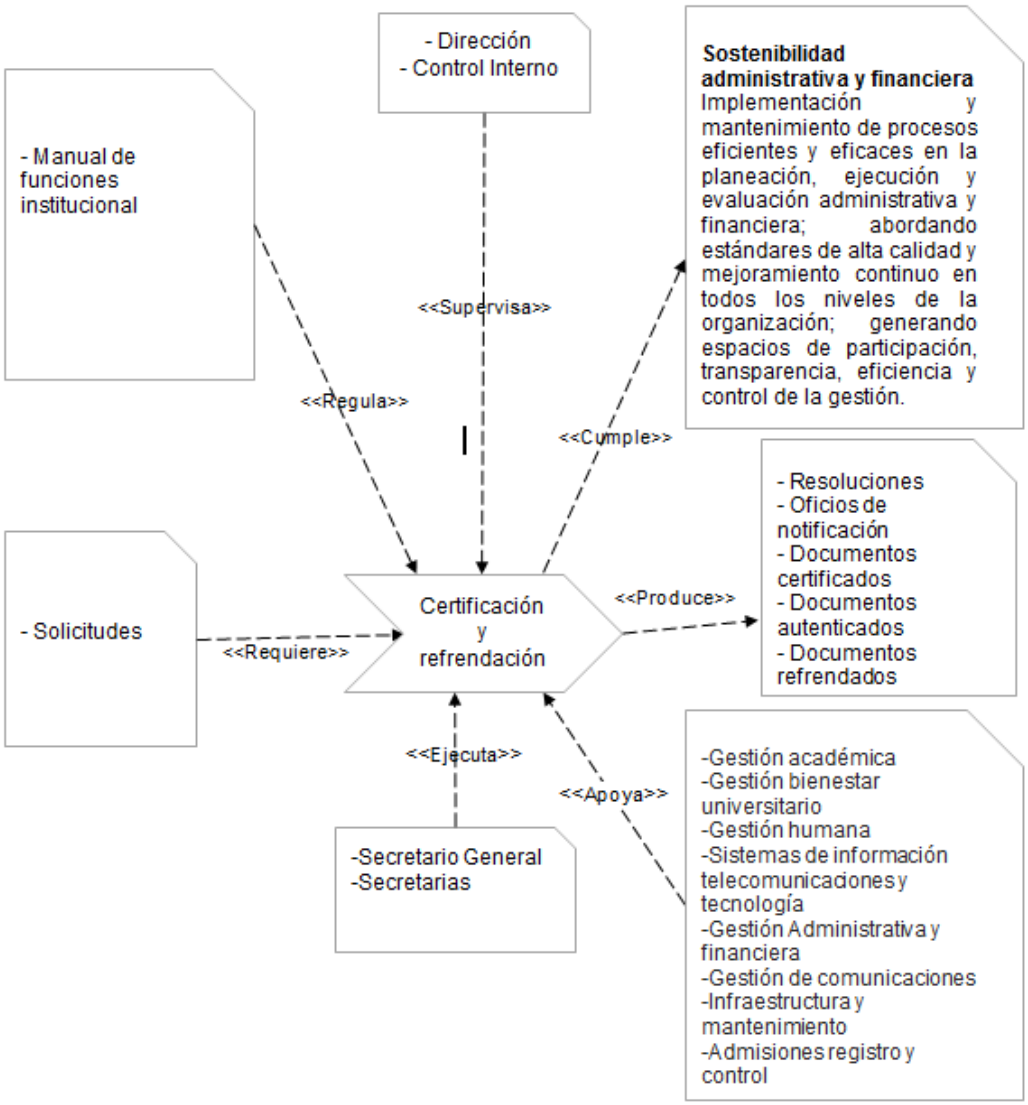


Figura 7. Diagrama de descripción del subproceso Certificación y Refrendación. (2016).

4.1.6.5 Subproceso Gestión de PQRS

Dando cumplimiento a la legislación vigente, la UFPS Ocaña, mediante Resolución No. 0147 de 2009 emitió el procedimiento interno para la recepción y trámite de PQRS, ofreciendo así una herramienta para que el usuario reporte peticiones, quejas, reclamos, sugerencias, felicitaciones y denuncias de actos de corrupción, que tenga sobre los procesos y servicios que brinda la Universidad. Ver figura 8.

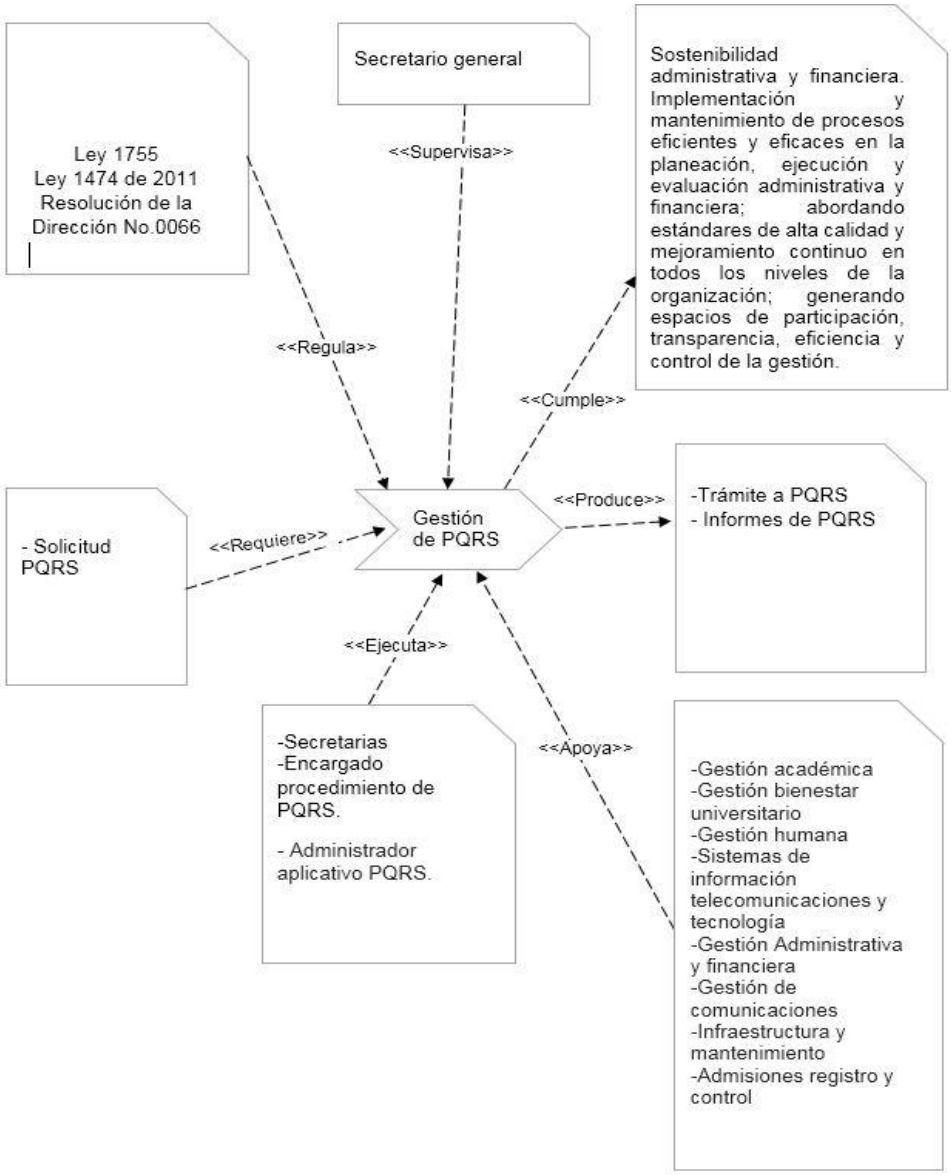


Figura 8. Diagrama de descripción del subproceso Gestión de PQRS. (2016).

4.1.7 Modelo de actores

A continuación se presenta el modelo de actores para cada uno de los subprocesos de Secretaría General. Mediante estos se pudo definir los responsables de las actividades así como los procesos que apoyan y supervisan.

Tabla 1

Modelo de actores del subproceso Electoral.

SUBPROCESO: ELECTORAL			
ACTORES	EJECUTA	SUPERVISA	APOYA
Secretario General	X		
Secretarias	X		
Entes de control		X	
Dirección seccional			X
Todos los procesos			X
Jurados de votación			X

Nota. La tabla despliega los actores que intervienen en el subproceso Electoral, y el papel que juega cada uno de ellos.

Tabla 2

Modelo de actores del subproceso Gestión Documental.

SUBPROCESO: GESTIÓN DOCUMENTAL			
ACTORES	EJECUTA	SUPERVISA	APOYA
Coordinador Archivo y Correspondencia	X		
Secretarias	X		
Mensajeros	X		
Secretarias Ventanilla Única	X		
Administrador SID	X		
Secretario General		X	
Todos los procesos			X

Nota. La tabla muestra los actores que intervienen en el subproceso Gestión Documental, y el papel que juega cada uno de ellos.

Tabla 3

Modelo de actores del subproceso Certificación y Refrendación.

SUBPROCESO: CERTIFICACIÓN Y REFRENDACIÓN			
ACTORES	EJECUTA	SUPERVISA	APOYA
Secretario General	X		
Secretarias	X		
Dirección seccional		X	
Control Interno		X	
Comité de Apoyo Académico			X
Comité de Dirección			X
Comité Administrativo			X
Todos los procesos			X

Nota. La tabla presenta los actores que intervienen en el subproceso Certificación y Refrendación, y el papel que juega cada uno de ellos.

Tabla 4

Modelo de actores del subproceso Gestión de PQRS.

SUBPROCESO: GESTIÓN DE PQRS			
ACTORES	EJECUTA	SUPERVISA	APOYA
Secretario General		X	
Secretarias	X		
Encargado procedimiento de PQRS	X		
Administrador aplicativo PQRS			X
Todos los procesos dela UFPS Ocaña			X

Nota. La tabla enseña los actores que intervienen en el subproceso Gestión de PQRS, y el papel que juega cada uno de ellos.

4.2 Auditoría pasiva practicada a la Secretaría General basada en la norma ISO/IEC 27001:2013

Secretaría General es un proceso de apoyo de la UFPS Ocaña, el cual tiene a su cargo el manejo de información sensible para la Institución, lo que pone de manifiesto una alta necesidad de una gestión segura de la misma.

Auditar es, en términos generales, realizar un proceso de evaluación; en este sentido, llevar a cabo una auditoría a la Secretaría General es indispensable para identificar las amenazas, las vulnerabilidades y los riesgos a los que se ve sometida la información. En este proyecto se planeó, se efectuó y finalmente se documentó la auditoría que ya se ha mencionado, partiendo de la base de que el criterio para la misma fue determinados dominios de la norma ISO/IEC 27001:2013, lo que permitió establecer el estado actual de Secretaría General en cuanto a la seguridad de la información.

4.2.1 Plan de auditoría

La elaboración del plan es el comienzo de cualquier auditoría, en este caso, se construyó un plan que provee una estructura diseñada por etapas, y que a su vez, se descompone en actividades como se aprecia en la figura 9.

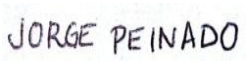
Proceso a auditar	Equipo de auditoría	Fecha auditoría	Lugar	Firma auditor líder
Secretaría General	Jorge Luis Peinado Rodríguez Álvaro Javier Durán Sanjuán	14/12/2015 al 20/12/2015	Instalaciones de Secretaría General UFPS Ocaña	
Objetivo	Evaluar la seguridad de la información en el proceso Secretaría General de la UFPS Ocaña.			
Alcance	Esta auditoría comprende una revisión de los mecanismos existentes para garantizar la seguridad de la información del proceso Secretaría General de la UFPS Ocaña, durante el periodo que va del 1 de noviembre al 19 de diciembre de 2015.			
Criterio	Se regirá por los siguientes dominios de la norma ISO/IEC 27001: 2013. Política de seguridad de la información, Seguridad ligada a los recursos humanos, Control de acceso, Gestión de activos, Cumplimiento, Aspectos de seguridad de la información en la gestión de la continuidad del negocio, Gestión de incidentes en la seguridad de la información, Seguridad de las operaciones, Seguridad física y ambiental.			
Etapa	Actividad			Auditor
Contacto inicial	Realizar reunión de contacto inicial con el jefe de Secretaría General, Magister. Edwin Edgardo Espinel Blanco.			Equipo de auditoría
Inicio de la auditoría	Realizar reunión de apertura de la autoría con funcionarios de las oficinas que hacen parte del proceso Secretaría General (Ventanilla única, Archivo central e histórico, oficina de Secretaría General)			
Recolección de información	Solicitar los siguientes documentos: manuales, instructivos, reglamentos, guías y procedimientos, documentación corporativa: estructura orgánica, misión, visión, objetivos institucionales y mapa de procesos.			
	Elaboración de los instrumentos de recopilación de información.			
Ejecución de la auditoría	Revisión documental.			
	Aplicación de los instrumentos de recopilación de información.			
	Definición de situaciones encontradas.			
Comunicación de resultados	Diseñar y preparar una estructura de informe.			
	Elaboración del informe de auditoría.			

Figura 9. Plan de auditoría practicada a Secretaría General. (2016).

4.2.2 Preparación de los documentos de trabajo

Teniendo en cuenta los acuerdos establecidos entre el equipo auditor y el cliente auditado, se llevó a cabo una revisión documental del proceso, donde fue estudiado tanto la estructura organizacional como el funcionamiento de Secretaría General.

Bajo el análisis de la información recolectada y considerando los criterios establecidos por la norma ISO 27001:2013, se construyeron los instrumentos de recolección de información que se presentan como anexos al final del presente documento y se relacionan en la tabla 5.

Tabla 5

Documentos de trabajo creados en la auditoría a Secretaría General.

Documento de trabajo	Anexo
DT1_EntrevistaSG	A
DT2_EntrevistasSecretariasDependencia	B
DT3_EntrevistaVentanillaUnica	C
DT4_EntrevistaArchivoCentralHistórico	D

Nota. La tabla muestra la lista de documentos de trabajo elaborados en la auditoría a Secretaría General, y a cuál anexo corresponde en el presente trabajo.

4.2.3 Informe de auditoría

En el anexo E del presente documento, se da a conocer la carta que el equipo de auditoría remitió al Secretario General, por medio de la cual se le presenta los resultados obtenidos.

4.2.4 Resultados de la auditoría

En la figura 10 se visualiza la información relevante de la auditoría realizada a la Secretaría General, dentro de la cual se destaca los resultados obtenidos en la misma.

Informe de auditoría			
Proceso auditado	Líder del proceso		
Secretaría General	Edwin Edgardo Espinel Blanco		
Objetivo de la auditoría	Alcance de la auditoría		
Evaluar la seguridad de la información en el proceso Secretaría General de la UFPS Ocaña.	Esta auditoría comprende una revisión de los mecanismos existentes para garantizar la seguridad de la información del proceso Secretaría General de la UFPS Ocaña, durante el periodo que va del 1 de noviembre al 19 de diciembre de 2015.		
Equipo de auditoría	Jorge Luis Peinado Rodríguez Álvaro Javier Durán Sanjuán		
Fecha auditoría	Del 14 de diciembre de 2015 al 20 de diciembre de 2015		
Criterio de la auditoría	Se regirá por los siguientes dominios de la norma ISO/IEC 27001: 2013. Política de seguridad de la información, Seguridad ligada a los recursos humanos, Control de acceso, Gestión de activos, Cumplimiento, Aspectos de seguridad de la información en la gestión de la continuidad del negocio, Gestión de incidentes en la seguridad de la información, Seguridad de las operaciones, Seguridad física y ambiental.		
Resultados de la auditoría			
Hallazgo	Criterio	NC	Observaciones
El proceso Secretaría General no cuenta con una política de seguridad.	5.1.1	x	Algunos funcionarios por iniciativa propia establecen controles de seguridad.
No existen copias de respaldo de la información ni el procedimiento para obtenerla.	12.3.1	x	
Se evidencia que las áreas de archivo no cuentan con elementos que permitan la protección contra amenazas externas y ambientales.	11.1.4	x	
No se da cumplimiento a la reglamentación emanada por el archivo general de la nación.	18.1.3	x	
No se ha definido un plan para la continuidad de la seguridad de la información.	17.1.1	x	
No existe una clasificación formal de la información.	8.2.1		Los funcionarios clasifican la información y la organizan bajo un criterio personal que facilite su posterior búsqueda. Las tablas de retención documental no están convalidadas por el AGN.
En las actividades donde se almacenan archivos no existe una copia de seguridad en caso de pérdida o deterioro de estos documentos.		x	
El personal no está debidamente capacitado con respecto a la seguridad de la información.	7.2.2	x	
No existe un procedimiento de gestión de incidentes de la seguridad de la información.	16.1.1	x	
Las instalaciones de procesamiento de información de ventanilla única no se encuentran aisladas del área de despacho y carga.	11.1.6	x	

Figura 10. Informe de auditoría practicada a Secretaría General. (2016).

De los resultados de la auditoría, mostrados en la figura 10, es posible afirmar que se identificaron nueve (9) no conformidades (NC) y una (1) oportunidad de mejora (OM), reflejando la clara necesidad de la definición de la política de seguridad de la información para Secretaría General con la cual se garantiza el mejoramiento continuo en estos aspectos.

Estos resultados de auditoría son lo que precisamente se convirtieron en el insumo principal para la formulación de la Política de Seguridad de la Información para Secretaría General, que se presenta en la siguiente sección.

4.3 Elaboración del documento formal que incorpora la Política de seguridad de la información para la Secretaría General de la UFPS Ocaña

Luego de haber conocido el funcionamiento del proceso Secretaría General, se realizó la auditoría pasiva permitiendo obtener una radiografía del estado actual de la misma en cuanto a la seguridad de la información. La Política de Seguridad de la Información se elaboró con base a los resultados obtenidos de la auditoría, las regulaciones del Archivo General de la Nación, y tomando como referencia la norma ISO/IEC 27001:2013.

4.3.1 Política de Seguridad de la Información para la Secretaría General de la UFPS Ocaña

4.3.1.1 Introducción

La Dirección de la UFPS Ocaña, consciente de los riesgos a los que se ve sometida la información, y siendo este el activo más importante de cualquier entidad, tiene dentro de sus prioridades, la identificación y protección de sus activos de información.

Por lo anterior, el proceso de Secretaría General ha definido la Política de Seguridad de la Información, acatando la legislación que le atañe y teniendo en cuenta los lineamientos de la norma ISO 27001:2013. Esta política contribuye al cumplimiento de los objetivos institucionales puesto que es un elemento fundamental para el mejoramiento continuo y la alineación a los estándares internacionales.

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 la protección de la información de la Secretaría General de tal modo que se garantice, como mínimo, la confidencialidad, disponibilidad e integridad de este activo. El logro

de este objetivo depende en gran medida del compromiso por parte la Dirección de la Universidad y de los demás involucrados.

4.3.1.4 Alcance

Este documento proporciona el conjunto de políticas para proteger los activos de información que están a cargo de la Secretaría General, y es aplicable a los empleados de la misma, así como a aquellos, que por razón de sus funciones, interactúen directamente con esta. Los aspectos relacionados con: infraestructura de red, equipos de cómputo, servicios web, dispositivos móviles, mecanismos de seguridad informática y demás elementos tecnológicos que apoyan las actividades de Secretaría General, son responsabilidad de la División de Sistemas de la Institución. Finalmente, esta política no estipula las sanciones para quienes la incumplan, puesto que esto es propio de los respectivos organismos universitarios responsables de las funciones sancionatorias.

4.3.1.5 Referencias normativas

La presente política fue elaborada teniendo en cuentas las directrices de control contemplados en la norma ISO/IEC 27001:2013, y la normatividad vigente estipulada por el Archivo General de la Nación que se especifica a largo del documento.

4.3.1.6 Revisión y aprobación

Esta Política debe ser revisada por el Secretario General anualmente o en los siguientes casos: debido a cambios de la Institución y de las condiciones legales aplicables. La aprobación es responsabilidad del Comité de Archivo.

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.

4.3.1.8 Términos y definiciones

Activo: los activos son bienes que la empresa posee, dentro de este grupo entra la información, que actualmente es catalogado como el más importante para una organización.

Amenaza: las amenazas son eventos que pueden generar incidentes a la organización a tal punto de comprometer los activos de la organización.

Archivo central: es el conjunto formado por todos los archivos de gestión de la institución.

Archivo de gestión: corresponde al archivo que está en constante manipulación y que se ha producido en un período no mayor a un año.

Archivo histórico: corresponde a toda la documentación transferida del archivo central y que por su alto valor debe ser conservado.

Archivo General de la Nación (AGN): es un organismo del Estado, adscrito al Ministerio de Cultura, y tiene como funciones: la organización y dirección del Sistema Nacional de Archivos -SNA, establecer política archivística para la nación, y tanto resguardar como proteger el patrimonio documental que conserva.

Confidencialidad: se ocupa de asegurar que únicamente accedan a la información quienes están autorizados.

Control: los controles son mecanismos que las organizaciones o responsables de la seguridad de la información establecen con el objetivo de minimizar el riesgo de pérdida de información.

Disponibilidad: asegura que los usuarios autorizados tengan acceso a la información cuando se requiera.

Documento: los documentos pueden estar en diferentes medios como papel o soporte magnético; el documento de archivo específicamente es el registro de información producida o recibida por una entidad en razón de sus actividades.

Integridad: consiste en garantizar que la información sea fiable y exacta.

ISO: Organización Internacional de Normalización, este organismo es el encargado de promover el desarrollo de normas internacionales en diferentes áreas como industria, comercio y comunicaciones.

Norma ISO/IEC 27001: es el estándar internacional para la seguridad de la información, más precisamente esta norma proporciona los elementos necesarios para la construcción de un sistema de gestión de seguridad de la información (SGSI). La revisión más reciente de esta norma fue publicada en 2013. Este estándar pertenece al conjunto de normas que se conoce comúnmente como la serie 27000.

Política de seguridad de la información: la política de seguridad de la información es un documento que tiene como objetivo brindar directrices para la gestión de la seguridad de la información, mediante un conjunto de normas alineadas a las necesidades del negocio y legislación nacional.

Riesgo: es catalogado como esa posibilidad de que una amenaza se materialice.

Sistema de información PQRS: software desarrollado por la UFPS Ocaña por medio del cual los ciudadanos pueden registrar peticiones, quejas, reclamos, sugerencias, felicitaciones y denuncias de actos de corrupción, sobre los procesos y servicios prestados por la Institución.

Seguridad de la información: hace referencia a la protección del activo más importante de la empresa, la información, independiente del soporte donde se encuentre, esto contempla aquella información que no es almacenada en dispositivos informáticos.

Seguridad informática: está orientada a definir medidas con el propósito de proteger los recursos de hardware y software, así como las comunicaciones que se pueden llegar a establecer entre estos.

Sistema de Información Documental (SID): software que apoya la gestión de documentos de la UFPS Ocaña. Fue desarrollado por la Institución.

Tabla de retención documental (TRD): son un listado de series o sub series, con sus correspondientes tipos documentales, a las cuales se le asigna el tiempo de permanencia en cada etapa del ciclo vital de los documentos (Archivo de Gestión y Archivo Central) y establece la

disposición final de los documentos de acuerdo a la normatividad aplicable a cada caso particular.

4.3.1.9 Responsabilidades

Es responsabilidad del Secretario General comunicar la Política de Seguridad de la Información a todo el personal del proceso Secretaría General y a terceros que, por razón de sus funciones, presten servicios en la Secretaría General.

Para la difusión de la Política de Seguridad se debe emplear los medios que el Secretario General disponga.

- La Secretaría General debe definir e implementar un plan de difusión de la Política de Seguridad.

- Cada funcionario es responsable de la información que por razón de sus funciones le sea asignada.

- Se deben documentar todos los procedimientos del proceso y mantener un control de cambios de los mismos.

4.3.1.10 Gestión de activos

- Hace referencia al manejo que debe hacerse sobre los bienes de Secretaría General, dentro de los que se incluye la información.

- Los activos de información deben ser clasificados de acuerdo a los niveles de seguridad que el Comité de Archivo establezca.

- La organización documental debe realizarse de conformidad con las Tablas de Retención Documental de la Universidad.

- Los dispositivos de procesamiento de información con que cuenta la Secretaría General son responsabilidad del líder del proceso.

4.3.1.11 En relación a los recursos humanos

- Es fundamental la inclusión de la seguridad de la información en la gestión de los recursos humanos, puesto que es uno de los componentes más sensibles en lo que respecta a garantizar la integridad, confidencialidad y disponibilidad de la información.

- El contrato de trabajo de quienes laboran en Secretaría General debe incluir una cláusula que defina la información que el empleado va a manejar y establezca las responsabilidades con la misma.

- Los empleados de Secretaría General deben recibir una capacitación al año, que incluya la concientización en cuanto a la importancia de la seguridad de la información, así como la socialización de las actualizaciones realizadas a la presente Política.

- Secretaría General debe definir los perfiles de los cargos, teniendo en cuenta las necesidades del proceso, la clasificación de la información a la que se va a tener acceso, y los riesgos asociados a ésta.

- Se debe delegar la responsabilidad de selección, verificación de antecedentes, términos y condiciones del contrato y demás, al área de recursos humanos.

- Secretaría General debe comunicar al Comité Disciplinario de la UFPS Ocaña, los casos de empleados del proceso que cometan violaciones a la seguridad de la información.

4.3.1.12 Copias de respaldo de la información

- La información siempre está expuesta a diversas amenazas que pueden provocar la pérdida de la misma, por lo tanto, con el objetivo de recuperar los datos cuando sea requerido, es indispensable contar con copias originales de los mismos.

- Se debe establecer un procedimiento para la digitalización de acuerdo a lo establecido en la Circular Externa 005 del Archivo General de la Nación, y tomando como base la guía 'Pautas para la utilización de la digitalización', de la misma entidad.

- Los documentos del Archivo Central deben ser digitalizados y dichos ficheros deben ser almacenados en un centro de datos definido por Secretaría General;

además, en un lugar geográfico diferente de las instalaciones de la Universidad, debe existir copias de seguridad de los documentos digitalizados.

- Cada funcionario de Secretaría General debe hacer las copias de respaldo de la información a su cargo, de conformidad con la política establecida por la División de Sistemas para este fin.

- Las copias de respaldo de información de los aplicativos de apoyo de Secretaría General, Sistema de Información Documental y PQRS, deben ser gestionadas por el proceso de Sistemas de Información, telecomunicaciones y tecnología.

4.3.1.13 Protección física

- Medidas que tienen como objetivo prevenir accesos físicos no autorizados, así como mantener en buen estado documentos que por su valor institucional deben ser conservados.

- Se debe restringir el acceso a personal no autorizado a las zonas de archivo.

- Se debe diseñar y aplicar una guía para la conservación y protección de archivos, la cual especifique las condiciones de edificación, almacenamiento, medio ambiental, de seguridad y de mantenimiento, de conformidad con los lineamientos del Archivo General de la Nación en el Acuerdo 48 del 2000, Acuerdo 49 del 2000, Acuerdo 50 del 2000 y la Ley 594 del 2000.

- La protección física de los centros de datos donde se aloja la información de los sistemas SID y PQRS está bajo responsabilidad de la División de Sistemas.

- Se debe definir un procedimiento para las transferencias de documentos que defina las medidas que garanticen la conservación del material, tales como la manipulación, embalaje y transporte entre otras, y aquellas que eviten la contaminación y propagación de factores nocivos, cumpliendo con lo establecido en el Acuerdo 07 de 1994, artículo 60, del Archivo General de la Nación.

- Para la consulta de archivos de gestión está prohibido el préstamo de documentos originales, por lo tanto, el usuario debe solicitar una copia por escrito, y posteriormente, debe diligenciar el formulario de préstamo. Las copias se le entregarán toda vez que éste haya realizado el pago de las mismas.

- El préstamo de documentos sólo será autorizado por el jefe de la oficina donde se presenta la solicitud.

4.3.1.14 Área de despacho y carga

- Son aquellos espacios dentro del área física que son usados para tareas de recepción y entrega de elementos, como la correspondencia y otros artículos para dentro y fuera del campus universitario.

- La oficina de Ventanilla Única debe estar aislada de las instalaciones de procesamiento de información.

4.3.1.15 Continuidad de la seguridad de la información

- Existen muchos factores que pueden llegar a afectar el funcionamiento diario de Secretaría General, para esto se define un plan de continuidad del negocio que permita garantizar el no pare de las labores, no obstante, dada las responsabilidades que tiene a cargo el proceso, también debe gestionarse la seguridad de las actividades aun en situaciones adversas.

- La continuidad de la seguridad de la información debe ser incluida en el plan de continuidad del negocio de Secretaría General; este plan debe ser definido por el líder del proceso.

- Se debe definir y documentar procedimientos que permitan el funcionamiento de los controles de seguridad de la información aun en situaciones adversas.

4.3.1.16 Cumplimiento

- En el ámbito nacional y local existe una serie de normatividades y legislación que son aplicables y de obligatorio cumplimiento por parte de Secretaría General.

- Secretaría General debe evitar incumplimientos de cualquier ley, estatuto, regulación u obligación de carácter institucional o nacional.

- Se debe identificar y documentar la normatividad nacional que sea aplicable al proceso de Secretaría General.

- Secretaría General debe identificar y vigilar que los aplicativos de apoyo: SID y PQRS, estén cumpliendo con la normativa nacional.

4.3.1.17 Gestión de incidentes

La gestión de incidentes hace referencia al tratamiento que se le debe dar a todas aquellas situaciones no comunes que puedan presentarse y que se consideren puedan dañar, alterar, la información.

Todo funcionario debe reportar a su jefe inmediato por los medios que Secretaría General disponga, y en el menor tiempo posible, los eventos asociados al daño, deterioro, pérdida o destrucción de archivos, así como cualquier situación o debilidad que ponga en riesgo los activos de información.

4.3.1.18 Vigencia

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

4.3.1.19 Sanciones

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

4.3.1.20 Contacto

Secretaría General

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

Correo: secretariageneral@ufpso.edu.co

Capítulo 5: Conclusiones

Se diseñó el modelo de negocio de la Secretaría General de la UFPS Ocaña con el método de Gestión de Procesos de Negocio (BPM), identificando los siguientes elementos propios de la Universidad: misión y visión, objetivos institucionales, estructura orgánica y cadena de valor; asimismo, se determinó los sub procesos de los que se compone Secretaría General, que son: Electoral, Gestión de PQRS, Gestión documental, y Certificación y refrendación, junto a los que se diseñó el modelado tanto del proceso principal como de sus subprocesos y los respectivos modelos de actores.

Se realizó la auditoría pasiva a la Secretaría General basados en la norma ISO/IEC 27001:2013, tomando como criterios de evaluación la seguridad ligada a los recursos humanos, control de accesos, gestión de activos, gestión de la continuidad del negocio, gestión de incidentes, seguridad física y ambiental y cumplimiento, detectándose nueve (9) no conformidades y una (1) oportunidad de mejora.

Se elaboró un documento formal donde se incorpora la política de seguridad de la información de la Secretaría General de la UFPS Ocaña, la cual pretende contribuir con el mejoramiento de la cultura orientada a la seguridad de la información y el establecimiento de medidas que permitan minimizar los riesgos inherentes al proceso, debido a que la Secretaría General es un proceso crítico de la UFPS Ocaña, su importancia se evidencia en el conjunto de actividades trascendentales que tiene a su cargo.

Capítulo 6: Recomendaciones

Después de diseñada la política es indispensable que se apruebe formalmente, de tal manera que el siguiente paso es la implementación, para lo cual se requiere el apoyo de la alta dirección.

Conjuntamente, se recomienda realizar una serie de capacitaciones sobre: seguridad de la información, norma ISO/IEC 27001:2013, y normatividad nacional establecida por el Archivo General de la Nación a los funcionarios de la Secretaría General.

La definición de la presente Política de Seguridad de la Información, es un logro y un paso adelante para Secretaría General, por lo tanto, se recomienda mantener el compromiso por parte de todos los involucrados en el proceso, con el fin de actualizar dicha política en función del entorno dinámico que caracteriza a todas las organizaciones.

Referencias

Archivo General de la Nación (s.f). Recuperado el 20 de julio de 2015, de http://www.archivogeneral.gov.co/sites/all/themes/nevia/PDF/Transparencia/ACUERDONo.003del17deFebrerode2015.pdf

Administración electrónica (2012). Recuperado el 1 de agosto de 2015, 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

Fonseca Luna, O. (2011). *Sistemas de Control Interno para Organizaciones: Guía práctica y orientaciones para evaluar el control interno: COSO, CoCo, BASEL, guía TURNBULL, COBIT, ERM, SOx, INTOSAI, OMB A – 123.*Recuperado de https://books.google.com.co/books?id=plsiU8xoQ9EC&hl=es&source=gbs_navlinks_s

ICETEX (s.f.).Recuperado el 2 de agosto de 2015, de http://www.archivogeneral.gov.co/sites/all/themes/nevia/PDF/Transparencia/ACUERDONo.003del17deFebrerode2015.pdf

IT GOVERNANCE INSTITUTE (2008).Recuperado el 7 de agosto de 2015, de http://www.isaca.org/Knowledge-Center/Research/Documents/Alineando-COBIT-4-1-ITIL-v3-y-ISO-27002-en-beneficio-de-la-empresa_res_Spa_0108.pdf

ICONTEC (s.f.). Recuperado el 9 de agosto de 2015, de http://tienda.icontec.org/brief/NTC-ISO-IEC27001.pdf

ISO (2005).Recuperado el 8 de agosto de 2015, de https://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf

Grasso, L. *Encuestas elementos para su diseño y análisis.* (2006). Córdoba, Argentina: Editorial Encuentro.

Landeau, R. *Elaboración de trabajos de investigación*. (2007). Caracas, Venezuela: Editorial Alfa.

MINTIC (2009). Recuperado el 1 de agosto de 2015, de http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

MINTIC (2012). Recuperado el 1 de agosto de 2015, de http://www.sena.edu.co/acerca-del-sena/naturaleza-juridica/normatividad/Lists/Leyes/ley_1581_2012.pdf

PUCE (2012). Recuperado el 12 de diciembre de 2015, de http://www.puce.edu.ec/intranet/documentos/Reglamentos/OF-SEGURIDAD-Politica-Seguridad-Usuario-Final-2012.pdf

Sanchez, K., & Areniz, Y. (2014). *Diseño de las políticas de la seguridad de la información para la alcaldía municipal de Río de Oro, Cesar* (Tesis de pregrado). Universidad Francisco de Paula Santander, Ocaña

Senado (1991). Recuperado el 13 de noviembre de 2015, de http://www.secretariasenado.gov.co/senado/basedoc/cp/constitucion_politica_1991_pr002.html

UFPSO (s.f.). Recuperado el 25 de julio de 2015, de https://ufpso.edu.co/sec_gnral

Apéndices

Apéndice A. Entrevista dirigida al Secretario General

Proceso a auditar	Secretaría General.
Equipo de auditoría	Jorge Luis Peinado Rodríguez Álvaro Javier Durán Sanjuán
Fecha auditoría	14/12/2015 al 20/12/2015
Documento de trabajo	DT1_EntrevistaSG
1. ¿Existe una política de seguridad de la información para Secretaría General?	
2. ¿Está aprobada por la dirección?	
3. ¿Está publicada?	
4. ¿Comunicada a empleados y partes externas?	
5. ¿Comunicada a empleados y partes externas?	
6. ¿Se tiene un proceso de selección de empleados teniendo en cuenta leyes, reglamentaciones, requisitos del negocio, ética, clasificación de la información a la que se va a tener acceso, y a los riesgos percibidos?	
7. ¿Se especifican términos y condiciones de contratación para el personal de Secretaría General, teniendo en cuenta la información que manejan en el desempeño de sus funciones?	
8. ¿Existe un conjunto de exigencias a empleados y contratistas para que se aplique la seguridad de la información?	
9. ¿Se tiene un plan de concienciación, educación y capacitación en seguridad de la información?	
10. ¿Está definido un Proceso disciplinario para las sanciones en caso de infracciones?	
11. ¿Las responsabilidades y deberes de seguridad de la información que permanecen válidos se definen, comunican y hacen cumplir?	
12. ¿Existe restricción del acceso a la información?	

Apéndice B. Entrevista dirigida a las secretarias del proceso

Proceso a auditar	Secretaría General.
Equipo de auditoría	Jorge Luis Peinado Rodríguez Álvaro Javier Durán Sanjuán
Fecha auditoría	14/12/2015 al 20/12/2015
Documento de trabajo	DT2_EntrevistasSecretariasProceso

1. ¿Existe un inventario de activos? ¿Con qué frecuencia se revisa este inventario?
2. ¿Existe un propietario identificado de cada uno de los activos?
3. ¿Existen criterios definidos para la clasificación de la información? (pública o confidencial)
4. ¿Existe un procedimiento de devolución de activos?
5. ¿Se tiene un procedimiento para el etiquetado y tratamiento de la información, de acuerdo con el esquema de clasificación adoptado por la Organización?
6. ¿Se cumple la normatividad aplicable a las PQRS?
7. ¿Se cumple la normatividad aplicable a la gestión documental?
8. ¿Se aplica la ley de protección de datos personales?
9. ¿Existe normatividad para el proceso electoral?
10. ¿Existe planificación de la continuidad de la seguridad de la información?
11. ¿Se han implantado planes para la continuidad de la seguridad de la información?
12. ¿Existe verificación, revisión y evaluación de la continuidad de la seguridad de la información. ?
13. ¿Existe disponibilidad de instalaciones para el procesamiento de la Información.
14. ¿Están definidos las responsabilidades y procedimientos para la gestión de los incidentes en la seguridad de la información?
15. ¿Existe un procedimiento para la notificación de los eventos de seguridad de la información?
16. ¿Se notifican puntos débiles de la seguridad de la información?
17. ¿Existe un perímetro de seguridad física?
18. ¿Se tienen controles físicos de entrada?
19. ¿Existen mecanismos para la seguridad de oficinas, despachos y recursos. ?
20. ¿Existe protección contra las amenazas externas y ambientales?
21. ¿Las exigencias del AGN son cumplidas?
22. ¿Quién es el responsable de las llaves de las oficinas?

Apéndice C. Entrevista dirigida al personal de Ventanilla Única

Proceso a auditar	Secretaría General.
Equipo de auditoría	Jorge Luis Peinado Rodríguez Álvaro Javier Durán Sanjuán
Fecha auditoría	14/12/2015 al 20/12/2015
Documento de trabajo	DT3_EntrevistaVentanillaUnica
1. ¿Se cumple la normatividad aplicable a las PQRS? 2. ¿Se cumple Ley 1266 de 2008, Ley 1581 de 2012, Ley 1755 de 2015, Ley 1437 de 2011?	
3. ¿Se cumple la normatividad aplicable a la gestión documental?	
4. ¿Se aplica la ley de protección de datos personales?	
5. ¿Existe Normatividad para el proceso electoral?	
6. ¿Existen Responsabilidades y procedimientos definidos?	
7. ¿Se tienen un procedimiento para la notificación de los eventos de seguridad de la información?	
8. ¿Se tienen un procedimiento para notificación de puntos débiles de la seguridad?	
9. ¿Existe un perímetro de seguridad física?	
10. ¿Existe controles físicos de entrada?	
11. ¿Se cuenta con seguridad en oficinas, despachos y recursos?	
12. ¿Protección contra las amenazas externas y ambientales?	
13. ¿El trabajo en áreas seguras?	
14. ¿Las exigencias del AGN son cumplidas?	

Apéndice D. Entrevista dirigida al personal de Archivo Central e Histórico

Proceso a auditar	Secretaría General.
Equipo de auditoría	Jorge Luis Peinado Rodríguez Álvaro Javier Durán Sanjuán
Fecha auditoría	14/12/2015 al 20/12/2015
Documento de trabajo	DT4_EntrevistaArchivoCentralHistórico
1. ¿Qué información se tiene almacenada?	
2. ¿Existe restricción del acceso a la información?	
3. ¿Cómo es el procedimiento de solicitudes?	
4. ¿Cómo es el retiro de información?	
5. ¿Cómo se clasifican los archivos, rotulados, etiquetados?	
6. ¿Protección contra daños ambientales?	
7. ¿Existen copias de respaldo?	
8. ¿Existe manejo de temperatura, humedad relativa, ventilación, contaminantes atmosféricos e iluminación?	
9. ¿Se realiza un programa de limpieza?	
10. ¿Existe señalización, rutas de evacuación, rescate de unidades documentales?	
11. ¿De qué manera se realiza la eliminación de archivos?	

Apéndice E. Carta de Informe de Auditoría

Ocaña, 18 de diciembre de 2015

Magíster
EDWIN EDGARDO ESPINEL BLANCO
Secretario General
Universidad Francisco de Paula Santander Ocaña
Ocaña

Cordial saludo.

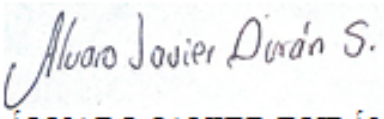
Nos permitimos entregar a usted el informe de resultados de la auditoría de sistemas practicada al proceso Secretaría General donde se evaluó la seguridad de la información. Dicho trabajo se llevó a cabo del 1 de noviembre al 19 de diciembre del presente año.

De los resultados obtenidos en la ejecución de la evaluación, se le comunica a usted lo siguiente:
No existe política de seguridad de la información, además, no se da cumplimiento a la normatividad nacional para la gestión de archivos, y por último, no se cuenta con copias de respaldo de la información, ni se tienen procedimientos para obtenerlas.

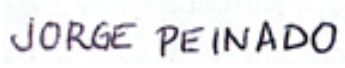
Es importante notar que el proceso de Secretaría General cuenta con su respectiva documentación en cuanto a procedimientos, procesos y formato, de acuerdo al enfoque por procesos que ha logrado la UFPS Ocaña.

A continuación se muestra la tabla de hallazgos encontrados durante la auditoría, teniendo como criterio algunos dominios de la norma ISO/IEC 27001, como se indica más delante.

Atentamente,



ÁLVARO JAVIER DURÁN SANJUÁN
Auditor



JORGE LUIS PEINADO RODRÍGUEZ
Auditor