RESUMEN – TRABAJO DE GRADO

AUTORES	**JESÚS ALBERTO CAMARGO PEREZ** **CHRISTIAN JHOAN MEJIA TORRADO**
FACULTAD	**INGENIERÍA**
PLAN DE ESTUDIOS	**INGENIERÍA DE SISTEMAS**
DIRECTOR	**PHD. TORCOROMA VELASQUEZ PEREZ**
TÍTULO DE LA TESIS	**DIAGNOSTICO DE LA SEGURIDAD DE LA INFORMACIÓN PARA LA DIVISIÓN DE INVESTIGACIÓN Y EXTENSIÓN DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA, BASADO EN LA NORMA ISO/IEC 27002:2013**

RESUMEN

(70 palabras aproximadamente)

ESTE PROYECTO TIENE COMO OBJETIVO LA REALIZACION DE UN DIAGNOSTICO DE LA SEGURIDAD DE LA INFORMACION DE LA DIVISION DE INVESTIGACION Y EXTENSION DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA TENIENDO EN CUENTA LAS NORMAS ISO/IEC 27002:2013. SE REALIZA AUDITORIA DE SISTEMAS PARA LA VERIFICACION DEL DIAGNOSTICO Y SE ELABORA UN DICTAMEN PARA REALIZAR MEJORAS EN EL FUTURO DE LA DEPENDENCIA.

CARACTERÍSTICAS

PÁGINAS: 85	PLANOS:	ILUSTRACIONES:	CD-ROM:1

DIANOSTICO DE LA SEGURIDAD DE LA INFORMACIÓN PARA LA DIVISIÓN DE INVESTIGACIÓN Y EXTENSIÓN DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA, BASADO EN LA NORMA ISO/IEC 27001:2013

AUTORES:

CAMARGO PÉREZ JESUS ALBERTO

TORRADO MEJIA CHRISTIAN JHOAN

Proyecto desarrollado como requisito para optar el título de Especialista en Auditoria de Sistemas

Director:

PhD. TORCOROMA VELÁSQUEZ PÉREZ

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

FACULTAD DE INGENIERIAS

ESPECIALIZACIÓN EN AUDITORIA DE SISTEMAS

Ocaña, Colombia Diciembre de 2018

Índice

Lista de Figuras

Lista de tablas

Capítulo 1. Diagnóstico de la Seguridad de la Información para la División de Investigación y Extensión de la Universidad Francisco de Paula Santander Ocaña, Basado en la Norma ISO/IEC 27001:2013

1.1 Planteamiento del problema

La actualidad empresarial abarca una gran cantidad de circunstancias, desde el ámbito administrativo, contable y financiero, pero el que mantiene un soporte fundamental en cómo se desarrolla una organización es la tecnología y la información.

Lemieux (2016) afirma:

> La era digital ha experimentado un cambio enorme en la forma en que creamos, comunicamos y mantenemos la información grabada. En los últimos veinte años, las nuevas tecnologías de la información y la comunicación (TIC) apoyados con Internet, nos han dado el correo electrónico, el contenido web, las redes sociales y la nube.

Con lo anterior se puede apreciar el nivel de desarrollo que determina la tecnología en el medio empresarial por lo tanto hay que administrar correctamente, ya que esta permite interactuar con el activo más importante, la información.

Para los autores Sokolov, Alimov, Golubeva, Burlov, & Vikhrov (2018):

> el sello distintivo de los negocios modernos es su gran dependencia de sistemas de información. La creciente complejidad y distribución de la infraestructura de información

significa que las empresas se están convirtiendo más vulnerables a la actividad maliciosa, error humano, técnico fallas, malware, etc., que a su vez requiere el uso activo de una cantidad de subsistemas de seguridad de la información.

"Sin embargo, se encuentra expuesta a riesgos en su seguridad; por tal motivo, las empresas actuales se preocupan por mitigarlos y evitar que pongan en peligro su normal funcionamiento" (Valencia & Orozco, 2017).

Así mismo también ha cambiado la manera de pensar de los atacantes, quienes en la búsqueda de vulnerabilidades intentan infiltrarse con el objetivo de hacer el mayor daño posible, según Santiago Chinchilla (2009): "Tanto para hacker como Crackers, años atrás la característica común apuntaba al dominio de un gran conocimiento sobre tecnología, aunque el diferencial entre ellos sigue siendo el beneficio propio o de un tercero y el reto mismo respectivamente".

El uso de las tecnologías de la información y su masificación las han convertido en blanco de ataques y vías para los mismos; los riesgos asociados a estas se intensifican y transforman y por ello se hace necesario crear y adaptar constantemente los medios y métodos utilizados para conservar la seguridad de la información que las organizaciones quieren proteger (Castro & Bayona, 2016).

A nivel internacional en la universidad de Oulu (Finlandia) se realizó un estudio acerca de la relación que tienen los empleados de las organizaciones con respecto a la seguridad de la información. Se desarrolló un nuevo modelo que explica que la amenaza clave para la seguridad

de la información proviene de los empleados que no cumplen con las políticas de seguridad de la información y se validó con una muestra de 669 respuestas de cuatro empresas en Finlandia. (Siponen, Pahnila, & Mahmood, 2014).

En España se realizó un estudio metodológico y técnico sobre la auditoría de la información en los hoteles del territorio donde se analizaron los datos de más de sesenta empresas hoteleras con el fin de encontrar los aspectos tecnológicos en los que tenían falencias y se definieron como las auditorías apoyaban la evolución del comercio por medio de la gestión tecnológica. (Infante, Martínez, & García, 2016).

A nivel nacional en la Universidad de Cartagena Colombia se propuso un modelo básico de seguridad lógica bajo el marco Plan-Do-Check-Act PDCA según Martelo, Tovar, & Maza (2018) se desarrolló un modelo de apoyo al proceso de creación y registro de políticas de seguridad a nivel lógico, el cual permite a la organización la creación, aplicación y apropiación de la seguridad informática como una de las claves principales de su negocio, sin descuidar las metas del mismo; así mismo permite un seguimiento, a través de auditorías, del cumplimiento de cada uno de los controles existentes en la organización, implementados a partir de las políticas presentes en dicha empresa.

También se ha indagado en los temas del riesgo y la seguridad de la información en las empresas, como lo plantea Cruz Garzón de la Universidad Piloto de Colombia, en su recopilación de aspectos de análisis, gestión de riesgos, seguridad y protección de la información en las organizaciones en Colombia, donde le da la importancia gerencial que necesitan las

empresas para que su seguridad tenga el manejo adecuado profundizando en aspectos como la gestión de riesgo, y el seguimiento de políticas que tengan en cuenta las características principales de confidencialidad, integridad y disponibilidad. (Cruz, 2015).

A nivel local se realizó un sistema de gestión de la seguridad de la información en la secretaría de hacienda del municipio de Río de Oro Cesar según Vega & Acosta la Secretaría de Hacienda de Río de Oro Cesar, no contaba con una adecuada Gestión del Sistema de Seguridad de la Información, lo que se evidencia en un incipiente sistema de gestión de riesgos, en una escasa gestión de la seguridad de la información de las áreas involucradas y en la poca conciencia en el tratamiento de la seguridad de la información por parte de los funcionarios de la dependencia. (Vega & Acosta, 2017).

En cuanto a ciberseguridad es importante darse cuenta de que la preparación del campo de batalla del mañana está sucediendo ahora, lo que resulta en puertas traseras en el diseño y la producción de hoy. Por lo tanto, mejorar la seguridad a lo largo de la línea de suministro se requiere rápidamente y puede ser empujada por, por ejemplo, el uso de tecnologías Blockchain. (Koch & Golling, 2018).

En el área de la seguridad de la información son diversos los temas que se desprenden de esta ciberseguridad, ciberdefensa etc., el mundo globalizado en el que estamos hoy nos invita a reflexionar y pensar en forma crítica sobre esta problemática que no es ajena a cualquier organización mientras esta haga uso del activo más importante la información.

Debido a la falta de capacitación en aspectos tecnológicos y la ausencia de procedimientos o políticas en cuanto a seguridad de la información en la División de Investigación y Extensión genera que el activo más importante de la organización, la información, presente deficiencias en cuanto a su integridad, disponibilidad y confidencialidad.

La seguridad de la información es importante en la medida en que las organizaciones y las personas desean contar con seguridad a nivel de tecnologías de la información, hoy en día los proveedores responden con productos y servicios más seguros, la industria y los consumidores reconocen la necesidad de brindar la seguridad necesaria en cuanto a información.

1.2 Formulación del problema

¿Diagnosticar el estado de la seguridad de la información de la dependencia de la División de Investigación y Extensión permitirá identificar los riesgos con mayor grado que pueden afectar la continuidad del negocio?

1.3 Objetivos

1.3.1 General

Diagnosticar la seguridad de la información para la División de Investigación y Extensión en la universidad Francisco de Paula Santander Ocaña

1.3.2 Específicos.

- Estudiar y analizar la ISO 27001 según la estructura aplicable a la División de Investigación y Extensión.
- Diagnosticar el estado actual de los sistemas de información en la División de Investigación y Extensión.
- Realizar las recomendaciones pertinentes para el aseguramiento de la seguridad de la información en la División de Investigación y Extensión.

1.4 Justificación

El uso de la tecnología en los procesos de negocio no solo trae beneficios a las organizaciones y a los usuarios, sino que muchas veces implica riesgos para la información digital, debido a la presencia de vulnerabilidades en el software y hardware computacional, muchas veces resultado de la falta de madurez de algunos productos a nivel de ciberseguridad.

De manera que la interconexión a la red de redes no solo se expande al mercado corporativo, sino que también expone a los activos de información de organizaciones a una gran cantidad de amenazas. (Santiago Chinchilla & Sánchez Allende, 2017).

En la actualidad la mayoría de las organizaciones almacenan y transmiten información a través de sus diferentes activos informáticos ya sean computadores, tabletas etc. La información en formato digital cada día juega un papel más relevante en la toma de decisiones para alcanzar los objetivos organizacionales, sin embargo, está sujeta a amenazas constantes de tipo natural o humanos y para las organizaciones es esencial protegerla tomando medidas preventivas para resguardarla, mediante actividades y procesos sistemáticos que permitan mantener su confidencialidad, integridad y disponibilidad.

La constante incorporación de sistemas de información en los procesos operacionales y de gestión dentro de las organizaciones, ha provocado que éstas se vuelvan cada más dependiente de ellos, por lo que una falla o vulneración de estos sistemas puede provocar graves perjuicios en la continuidad operacional de las organizaciones. (Dieguez, Cares, & Cachero, 2017).

Por tal motivo surge la necesidad de proponer un sistema de seguridad de la información que permita ejercer los principios de confidencialidad, integridad y disponibilidad de la data almacenada y gestionada en la división de investigación y extensión.

Según (Valencia & Orozco, 2017), para llevar a cabo un sistema de gestión de seguridad de la información es importante tener en cuenta una serie de elementos como lo son los objetivos

estratégicos de la organización, los requisitos normativos o de terceros relacionados con la seguridad de la información, los sistemas de gestión existentes.

Mantener la confidencialidad, la integridad, la disponibilidad y la usabilidad autorizada de la información cobra especial relevancia y plantea la necesidad de disponer de profesionales idóneos y capaces de asegurar, gestionar y mantener la seguridad de los datos en sus sistemas ante amenazas presentes y futuras.

En la División de Investigación y Extensión la gestión de los sistemas de información resultan ser un elemento muy importante, en la medida en que la dependencia se encarga de llevar a cabo los procesos relacionados con la gestión de proyectos, convocatorias, investigadores y eventos, lo que conlleva a la administración de información sumamente sensible.

La seguridad de la información es una disciplina asociada tradicionalmente a la gestión de TIC, cuyo propósito es mantener niveles aceptables de riesgo de la información organizacional y de los dispositivos tecnológicos que permiten su recolección, procesamiento, acceso, intercambio, almacenamiento, transformación y adecuada presentación. Ha sido definida por la norma ISO/IEC 27000 como la preservación de la confidencialidad, integridad y disponibilidad de la información. (ISO/IEC, 2014). (Valencia & Orozco, 2017).

En la provincia de Ocaña se realizó una propuesta de aplicación en las empresas de la norma ISO 27001. Esta es una actividad pendiente por ejecutar, la cual propone conocer las

fortalezas y debilidades a las que pudieran estar sometidos los activos de información que están en las diferentes empresas, con el fin de sugerir estrategias que minimicen la ocurrencia de posibles amenazas que en la mayoría de los casos explotan las vulnerabilidades organizacionales. (Ascanio, Trillos, & Bautista, 2015).

De acuerdo a lo expuesto por Velásquez Pérez, Pérez, & Messino Sossa, (2016) para obtener un modelo adecuado a cada empresa es necesario conocer con detalle cada uno de sus procesos y cuáles son los que tienen prioridad para la continuidad del negocio en cada nivel de gobernanza; según los resultados arrojados por las diferentes auditorias de sistemas realizadas en la región, se toman tres estándares los cuales son alineados para trabajar a la par cubriendo de extremo a extremo la organización con un Sistema de Gestión de Seguridad de la Información que será adaptable a todo nuevo criterio o reto al que se enfrenten, tomando como referentes COBIT 5.0, ISO 27001:2013 e ITIL.

El diagnostico de la seguridad de la información para División de Investigación y Extensión brindará el aseguramiento del activo más importante de la organización, minimizando los riesgos a las posibles acciones externas o internas a las que se pueden exponer estas, es importante restringir el acceso de la información a personas no autorizadas y de esta manera conservar su integridad mediante el cambio de claves de acceso de forma periódica y la validación de estas en cuanto a seguridad.

1.5 Delimitación

Geográfica. Esta investigación o estudio se realizará en la división de investigación y extensión de la Universidad Francisco de Paula Santander Ocaña.

Temporal. El proyecto se realizará dentro de un periodo de 4 meses a partir de la fecha de aprobación del proyecto.

Conceptual. Para el desarrollo del proyecto es necesario tener en cuenta conceptos como: Seguridad de la información y sistema de gestión de seguridad de la información (SGSI).

Operativa. Para dar cumplimiento al proyecto se realizará un diagnóstico de los sistemas de información teniendo en cuenta sus aspectos técnicos y operativos. También se definirá el alcance del sistema de seguridad de la información con respecto al diagnóstico anterior, dejando por último la realización de la documentación del mismo.

Capítulo 2. Marco Referencial

2.1 Marco Histórico

Desde hace muchas décadas la información ha jugado uno de los papeles más relevantes, tanto que han marcado hito en la historia de la humanidad, según (Pellicer, 2013), cuando se declaró la Segunda Guerra Mundial en 1939, Turing se desplazó a trabajar a tiempo completo en la Oficina de Codificación del Gobierno y en la Escuela de Cifrado en Bletchley Park. Sus brillantes ideas descifrando códigos y desarrollando máquinas para ayudar a descifrar códigos salvaron muchas vidas durante la Segunda Guerra Mundial, tal vez acortada en un par de años por el descifrado de códigos alemanes de la máquina Enigma.

Las guerras que se han dado han sido el origen o el punto de partida de los avances tecnológicos, cabe aclarar que en ellas en donde se presenta la mayor inversion, las carreras armamentistas se convirtieron en el genesis de mayoria de tecnologia con las cuales contamos en el presente.

La mayor parte de las veces, la seguridad será necesariamente algo relativo o dependiente de que se cumplan ciertas condiciones o protocolos la historia de la seguridad de la información puede ser tan antigua como la humanidad misma, no así la historia de la seguridad de la información contenida en archivos digitales o computadorizados, es decir, lo que llamamos seguridad informática. (Arguello, 2010).

Algunas fechas y entidades importantes en el desarrollo de la seguridad de la información son:

En junio de 1942, un problema criptográfico japonés tuvo como consecuencia la destrucción de sus 4 mayores portaaviones y supuso el fin del dominio japonés del Pacífico. ¡Bueno, esto es cosa de los militares y además ya forma parte del pasado!

En 1983 nace la Internet, aunque el concepto original se remonta los años 60 cuando el Ministerio de Defensa de Estados Unidos estableció una red interestatal, de modo que toda la defensa del país dependiera de la misma red y compartiera los recursos de ésta. Así nació ARPANet (Advanced Projects Agency Net, llamada también DARPANet, por Defensa), con tres requisitos fundamentales:

La red debía estar protegida en caso de que un desastre natural o una guerra, especialmente un ataque nuclear, afectase al país, de modo no debilitase a la totalidad de la red, aunque una parte estuviera dañada.

La red, al igual que no debía ser afectada por la eliminación de una parte, debía permitir la incorporación de nuevos elementos con facilidad.

La red debería usar un lenguaje (códigos informáticos), un protocolo, que pudiera ser entendido por cualquier ordenador, independientemente del sistema empleado.

A ARPANet se le unen, todavía en Estados Unidos, otras instituciones, como Universidades, centros gubernamentales, organizaciones privadas, etc. A principios de los 80 se unen otros países.

Así en 1983 nace lo que hoy conocemos como Internet o la red de redes, ya con un gran número de usuarios y ordenadores enlazados o con la capacidad de enlazarse.

El 2 de noviembre de 1988 un joven llamado Robert Morris escribió un pequeño programa capaz de, usando algunas vulnerabilidades de UNIX, transmitirse de unos sistemas a otros a gran velocidad infectándolos a su paso. En unas horas miles de equipos tenían sus CPUs al 100% sin solución de continuidad. Se trataba del primer Gusano (Worm) de la historia. ¡Es cosa de "los locos del UNIX" y también es ya pasado, con un AntiVirus esto se habría evitado!, pero hoy tenemos antivirus y esto todavía sucede…

En junio de 2005 un hacker logró un listado de 40 millones de tarjetas de crédito. Servired, Visa y 4B tuvieron que localizar y avisar urgentemente a más de 50.000 clientes en España del riesgo que corrían

El 17 de junio de 2010, VirusBlokAda emitió una alerta por todo el mundo que desató una carrera internacional para rastrear lo que se conoce como Stuxnet: el más sofisticado malware de ordenadores que se haya encontrado y que deja entrever una nueva generación de amenazas cibernéticas. A diferencia del malware convencional, que hace daño sólo al mundo virtual de las

computadoras y redes, el objetivo de este software es controlar las bombas, válvulas, generadores y otras máquinas industriales.

"Fue la primera vez que se había analizado una amenaza que podría causar daños en el mundo real, que podría, de hecho, provocar que una máquina de rompa, y ser capaz de provocar una explosión", dice Liam O Murchu, jefe de seguridad de Symantec, en Mountain View, California, la empresa de seguridad informática más grande del mundo.

Stuxnet aportó la prueba palpable de que determinados grupos o naciones podrían lanzar un ataque cibernético contra las infraestructuras vitales de una sociedad, como el agua y la energía. "Probablemente ahora estamos entrando en la era cibernética de una nueva clase de armas", indicaba Mikko Hypponen, jefe de investigación de F-Secure, una empresa de antivirus con sede en Helsinki.

Peor aún, el episodio de Stuxnet ha puesto de relieve cuán inadecuadas son las defensas actuales de la sociedad, y cómo quedan atrás frente a la ciencia cibernética.

Históricamente la seguridad no ha sido nunca vista como una parte más de las tecnologías de la información, sino como algo propio de pequeños círculos de amistades, curiosos o gurús. En las universidades no existían (en muchas aún hoy no existen) asignaturas relacionadas con la seguridad. En el mundo empresarial aun hoy existe esta tendencia en muchos casos.

Existen varias razones por las que a todos los niveles no se le ha dado a suficiente importancia:

1. El riesgo y las consecuencias de ignorarlo eran mínimos
2. Siempre ha sido incomoda: mucho esfuerzo -> poco resultado
3. Los posibles ataques requerían muy altos niveles de Los posibles ataques requerían muy altos niveles de conocimiento.
4. El acceso al conocimiento y a las redes era muy limitado
5. Las empresas por lo general no invierten en seguridad hasta que sufren alguna violación.

Luego nacen los “hackers” o piratas informáticos, cuyo trabajo se centra en descubrir las vulnerabilidades de los sistemas de información computadorizados y violar la seguridad de los mismos con diferentes fines tales como, fraudes financieros, espionaje o simplemente causar daño.

Antecedentes. Con el fin de dar cumplimiento a los objetivos a continuación se describe una serie antecedentes que servirán de apoyo para tener una mejor comprensión en cada uno de estos temas y alcances significativos evidenciados en otro u otros proyectos similares. Los sistemas de Gestión de la Seguridad de la información surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y la sensibilidad de la información que favorecen el desarrollo y el buen funcionamiento de la empresa, 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:

A nivel internacional en la universidad de Oulu (Finlandia) se realizó un estudio acerca de la relación que tienen los empleados de las organizaciones con respecto a la seguridad de la información. La amenaza clave para la seguridad de la información proviene de los empleados que no cumplen con las políticas de seguridad de la información. Desarrollamos un nuevo modelo basado en la teoría múltiple que explicaba la adherencia de los empleados a las políticas de seguridad. El paradigma combina elementos de la Teoría de la Motivación de la Protección, la Teoría de la Acción Razonada y la Teoría de la Evaluación Cognitiva. Validamos el modelo utilizando una muestra de 669 respuestas de cuatro empresas en Finlandia. (Siponen, Pahnila, & Mahmood, 2014).

A nivel nacional en la Universidad de Cartagena Colombia se propuso un modelo básico de seguridad lógica bajo el marco Plan-Do-Check-Act PDCA según (Martelo, Tovar, & Maza, 2018) se desarrolló un modelo de apoyo al proceso de creación y registro de políticas de seguridad a nivel lógico, el cual permite a la organización la creación, aplicación y apropiación de la seguridad informática como una de las claves principales de su negocio, sin descuidar las metas del mismo; así mismo permite un seguimiento, a través de auditorías, del cumplimiento de cada uno de los controles existentes en la organización, implementados a partir de las políticas presentes en dicha empresa.

La seguridad lógica para la protección de la información es vital, porque permite: restringir el acceso a programas y archivos mediante claves y/o encriptación; asignar las limitaciones correspondientes a cada usuario del sistema informático, esto significa, no dar privilegios extra a un usuario, sino solo los que necesita para realizar su trabajo; asegurarse de que los archivos y programas que se emplean son los correctos y se usan correctamente, por ejemplo, el mal uso de una aplicación puede ocasionar agujeros en la seguridad de un sistema informático; control de los flujos de entrada/salida de la información, esto incluye que la información enviada llegue al destino deseado, pero no cuenta con un modelo con el cual se guíen para la creación de un sistema de seguridad informático a nivel lógico, lo que no permite medir el nivel de protección que tiene una organización. (Martelo, Tovar, & Maza, 2018).

A nivel local se realizó un sistema de gestión de la seguridad de la información en la secretaría de hacienda del municipio de Río de Oro Cesar según Vega, Peñaranda, & Acosta (2017) la Secretaría de Hacienda de Río de Oro Cesar, no contaba con una adecuada Gestión del Sistema de Seguridad de la Información, lo que se evidencia en un incipiente sistema de gestión de riesgos, en una escasa gestión de la seguridad de la información de las áreas involucradas y en la poca conciencia en el tratamiento de la seguridad de la información por parte de los funcionarios de la dependencia.

2.2 Marco Contextual

El proyecto se llevará a cabo en la Universidad Francisco de Paula Santander Ocaña creada en 1974 por el Acuerdo No. 003 aprobado por el Consejo Superior de la Universidad Francisco

de Paula Santander Cúcuta, en la actualidad la universidad está ubicada en la vía Acolsure en el municipio de Ocaña Departamento Norte de Santander y consta de las siguientes facultades: La Facultad de Ciencias Agrarias y del Ambiente creada En 1995 según el acuerdo 084, la Facultad de Ciencias Administrativas y Económicas creada según el acuerdo 008 en el 2003, la Facultad de Ingenierías creada en el 2006 según el acuerdo 007 y por último La Facultad de Educación, Artes y Humanidades creada en el 2006 según Acuerdo 063. (UFPSO, s.f.)

La Investigación y la Extensión son dos pilares fundamentales de toda institución de educación superior. La dependencia tiene como propósito fortalecer los Observatorios, Grupos, Semilleros y Centros, creados por la universidad para el desarrollo y divulgación del conocimiento a través de proyectos innovadores que genere impacto en la región.

En la re-estructuración del proceso se definen las unidades de Investigación, Extensión, Publicaciones y Transferencia Tecnológica; estas con el fin de aportar a la cultura investigativa, contribuir con la calidad y visibilidad de los productos generados.

2.3 Marco Conceptual

Activo. En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO, 2014).

Amenazas. Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO, 2014).

Riesgo. Posibilidad de que se ejecute un hecho que produzca ciertos efectos, cuyo impacto produce incertidumbre frente a los eventos y situaciones que puedan afectar los beneficios de una actividad. (Ballesteros, s.f.).

Auditoría. Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO, 2014).

Ciberseguridad. Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (ISO, 2014).

Control. Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo. (ISO, 2014).

Sistema de Gestión de Seguridad de la Información SGSI. Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos

objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO, 2014).

Gestión. Realización de diligencias que permiten la ejecución de una operación comercial o de cualquier ámbito**.** (Pérez y Merino, 2012).

Seguridad. Forma de controlar los peligros y condiciones que amenacen con producir daños ya sea de tipo físico, psicológico o material con la finalidad de conservar el bienestar de los individuos y la comunidad. (INSPQ, 2018).

Información. Conjunto de elementos que dan significado a las cosas, para la informática la información hace referencia a datos organizados y procesados que forman mensajes, instrucciones, operaciones, funciones y cualquier tipo de actividad que se relacione con un ordenador. (DefinicionABC, 2008).

Informática. Se refiere al uso de la información, mediante la utilización de máquinas, viendo a las nuevas tecnologías como alternativa para la resolución de problemas, haciendo uso de programas, diseño, fundamentos teóricos – científicos y diversas técnicas. La informática permite que el ser humano potencializar sus capacidades comunicativas, de pensamiento y memoria**. (**DefinicionABC, 2008).

Seguridad de la información. Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO, 2014).

Estándares. Documentación que contiene un conjunto de reglas, guías o características con la finalidad de ser utilizadas repetidamente, para proveer, el conocimiento y fundamento que la organización necesita para alcanzar el éxito; dicha documentación ha sido estudiada y aprobada por un cuerpo reconocido. (PMI, 2018),

ISO 27001/2013. Es la nueva versión de la norma ISO 27001, la cual posee cambios significativos en cuanto a su estructura, evaluación y tratamientos de los riesgos. (Álvarez, 2016).

2.4 Marco Teórico

Las bases teóricas comprenden un conjunto de conceptos y proposiciones que constituyen un punto de vista o enfoque determinado, dirigido a explicar el fenómeno o problema planteado.

Teniendo en cuenta la evolución de las nuevas tecnologías de la información y las grandes amenazas a la que se ven expuestas se debe poner en marcha procesos que garanticen la seguridad de la información, es necesario que las organizaciones cuenten con un modelo o Sistema de Gestión de Seguridad que esté basado en los estándares reconocido a nivel mundial, la intención de diseñar un SGSI propio de la institución es establecer políticas de seguridad que se alineen a las necesidades de la organización y así lograr manejar adecuadamente cada uno de los riesgos que pueda comprometer la confidencialidad, integridad, disponibilidad y seguridad de la información.

Para lograr una adecuada gestión de la información es indispensable que las organizaciones establezcan una metodología estructurada, clara y rigurosa para la valoración y tratamiento de los riesgos de seguridad, es por ello que se tiene como referente teórico la familia de normas ISO/IEC 27000.

Tabla 1.

Normas ISO/IEC 27000

NORMAS ISO/IEC 27000	
ISO/IEC 27000	Posee la visión general de los SGSI con los términos y cada una de las definiciones que son utilizadas en las distintas normas de la ISO 27000
ISO/IEC 27001.	Norma principal de la serie, que contiene los requisitos del SGSI.
SO/IEC 27002	Guía de buenas prácticas que describe los objetivos de control y controles recomendados en cuanto a la SI.
SO/IEC 27003	Guía de implementación del SGSI e información relacionada con el uso del modelo PDCA (Planificar, Hacer, Verificar, Actuar) y, los requerimientos de sus distintas fases.
SO/IEC 27004	Contiene la especificación de las métricas y técnicas que se pueden aplicar para evaluar la eficacia de un SGSI y los controles relacionados
SO/IEC 27005	Propone las directrices de gestión de riesgos del Sistema de Información. Se apoya en los conceptos propuestos en la norma ISO/IEC 27001, además su finalidad es ser apoyo en la aplicación satisfactoria de la SI basada en un enfoque de gestión de riesgos.
SO/IEC 27006	Especifica los requerimientos necesarios para obtener la acreditación de entidades de auditoria y certificación de SGSI.
SO/IEC 27035	Guía sobre la gestión de incidentes de SI, dividida en tres partes que son: Principios de gestión de incidentes, guía para la elaboración de un plan de respuesta de incidentes y guía de operaciones en la respuesta de incidentes.

Nota: La tabla muestra algunas normas que conforman la familia ISO/IEC. Fuente: ISO 27000.

A continuación, se mencionan otras teorías en las que se basa la presente investigación:

Teoría de la confiabilidad. Su finalidad se centra en las probabilidades de que el sistema logre cumplir de manera satisfactoria las funciones que son la razón por la que fue creado, de

forma general la confiabilidad es usada para lograr medir el comportamiento de los sistemas para así, lograr optimizar los procesos. (García, 2006).

Con lo dicho anteriormente, podemos deducir que la confiabilidad permite que un componente o sistema sea capaz de ejecutar la tarea por la que fue desarrollado sin fallos y bajo las condiciones establecidas.

En la presente investigación se aplicará la teoría de la confiabilidad para optimizar el sistema de gestión de seguridad de la información propuesto, para así optimizarlo y garantizar que cumpla cada uno de los objetivos propuestos.

Teoría de Protección de motivación. Propone, que la intención de protección depende de 4 factores que son: La percepción de la gravedad de la amenaza de un evento, la posibilidad percibida de la vulnerabilidad, la eficacia de la conducta preventiva recomendada y la percepción de auto eficiencia. En ésta teoría, la conducta precavida se efectúa a partir de la combinación de la amenaza (teniendo en cuenta que tanto daño puede causar) y, la susceptibilidad que hace referencia al nivel de riesgo. (Altamirano y Bayona).

La teoría de la protección de motivación, se enfoca en estudiar, comprender y predecir el comportamiento del ser humano, en términos de fallos de seguridad éste comportamiento es crucial para el cumplimiento de políticas, siendo un eslabón débil de la cadena de seguridad, donde dicha teoría permite analizar las violaciones de las políticas de seguridad de los sistemas de información, originadas por la conducta humana.

2.5 Marco Legal

Siempre que se desea implementar un Sistema de Gestión, toda organización debe obligatoriamente cumplir con todas las leyes, normas, decretos, etc. que sean aplicables en el desarrollo de sus actividades. De manera general se puede mencionar el tema de seguridad social, cumplir con la biblioteca, permisos, licencias de construcción, etc. pero en lo que se refiere específicamente a seguridad de la información, estas son las Leyes vigentes al día de hoy:

> **ISO 27001.** La norma ISO 27001 fue publicada en octubre de 2005, esencialmente la sustitución de la antigua norma BS7799-2. Es la especificación para un SGSI, un Sistema de Gestión de Seguridad de la Información. Sí BS7799 era un estándar de larga data, publicado por primera vez en los años noventa como un código de prácticas. Como este maduró, una segunda parte surgió para cubrir los sistemas de gestión. Es esto en contra de la cual se concede la certificación. Hoy en día más de mil certificados están en su lugar, en todo el mundo. (Castro & Ciacedo, 2013).

Certificación del Sistema de Gestión de Seguridad de la Información con ISO/IEC 27001 – ICONTEC. El Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC), es el Organismo Nacional de Normalización de Colombia. Entre sus labores se destaca la creación de normas técnicas y la certificación de normas de calidad para empresas y actividades profesionales. ICONTEC es el representante de la Organización Internacional para la Estandarización (ISO), en Colombia. (NTC-ISO/IEC, 2006).

El estándar para la seguridad de la información ISO/IEC 27001 especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (NTC-ISO/IEC, 2006) Abarca:

- Organización de la seguridad de la información.
- Política de seguridad.
- Gestión de activos.
- Control de acceso.
- Seguridad de los recursos humanos.
- Cumplimiento.
- Seguridad física y del entorno.
- Adquisición, desarrollo y mantenimiento de los sistemas de información.
- Gestión de las comunicaciones y operaciones.
- Gestión de la continuidad del negocio.
- Gestión de incidentes de seguridad de la información. (ICONTEC, 2014).

Ley 23 De 1982 Sobre derechos de autor. Los autores de obras literarias, científicas y artísticas gozarán de protección para sus obras en la forma prescrita por la presente Ley y en cuanto fuere compatible con ella, por el derecho común. También protege esta Ley a los intérpretes o ejecutantes, a los productores de programas y a los organismos de radiodifusión, en sus derechos conexos a los del autor. (Ley 23 de 1982, 2014).

Ley 44 de 1993. Por la cual se reglamenta el Registro Nacional del Derecho de Autor y se regula el Depósito Legal.

Ley N° 44 de 1993 (5 de febrero) modifica y adiciona la Ley N° 23 de 1982 y se modifica la Ley N° 29 de 1944. Mediante la adición de disposiciones y medidas especiales para el Registro Nacional del Derecho de Autor, las sociedades de gestión colectiva de derechos de autor y derechos conexos, sanciones y otros derechos. (Ley 44 de 1993, 2014).

El Registro Nacional del Derecho de Autor es competencia de la Unidad Administrativa Especial - Dirección Nacional del Derecho de Autor, con carácter único para todo el territorio nacional.

Ley 719 de 2001. DECRETO 1721 DE 2002 (agosto 6) "Por el cual se reglamenta la Ley 719 de 2001, que modificó las Leyes 23 de 1982 y 44 de 1993". EL PRESIDENTE DE LA REPÚBLICA DE COLOMBIA, en ejercicio de sus facultades constitucionales, en especial las conferidas por el Artículo 189 numeral 11 de la Constitución Política de Colombia, DECRETA: Derecho exclusivo. El autor de una obra musical, o su derechohabiente, tiene el derecho exclusivo de realizar, autorizar o prohibir cualquier comunicación al público de su obra por medios alámbricos o inalámbricos, comprendida su puesta a disposición del público, de tal forma que los miembros del público puedan

acceder a éstas desde el lugar y en el momento que cada uno de ellos elija. (Ley 719 de 2001, 2014).

Ley 527 De 1999. Por medio de la cual 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. (Archivo General, 1999).

Ámbito de aplicación. La presente ley será aplicable a todo tipo de información en forma de mensaje de datos, salvo en los siguientes casos:

- En las obligaciones contraídas por el Estado colombiano en virtud de convenios o tratados internacionales;
- En las advertencias escritas que por disposición legal deban ir necesariamente impresas en cierto tipo de productos en razón al riesgo que implica su comercialización, uso o consumo. (Ley 527 De 1999, 2014).

Ley Estatutaria 1266 Del 31 De diciembre De 2008. Decreto N° 2952 de 2010 por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008, EL PRESIDENTE DE LA REPÚBLICA DE COLOMBIA. En ejercicio de sus facultades constitucionales y legales, en especial, las conferidas por el numeral 11 del artículo 189 de la Constitución Política y en desarrollo de lo previsto en los artículos 12 y 13 de la Ley 1266 de 2008.

Que el 31 de diciembre de 2008 se expidió la Ley Estatutaria N° 1266 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.

Ley 1273 Del 5 De enero De 2009. "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". (Ley 1273 5 de enero de 2009).

El 5 de enero de 2009 se decretó la Ley 1273 de 2009, la cual añade dos nuevos capítulos al Código Penal Colombiano: Capitulo Primero: De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos; Capitulo Segundo: De los atentados informáticos y otras infracciones.

Como se puede ver, esta Ley está muy ligada a la ISO 27000, lo cual coloca al País a l vanguardia en legislación de seguridad de la información, abriendo así la posibilidad de nuevas entradas con este tema.

Ley estatutaria 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. La presente 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; así como el derecho a la información consagrado en el artículo 20 de la misma. (Secretaria Senado, 2012).

Capítulo 3. Diseño Metodológico

3.1 Tipo de Investigación

De acuerdo a las características del proyecto que se llevara a cabo, se empleara el tipo de investigación descriptiva-cualitativa, con aportes de herramientas utilizadas en la investigación cuantitativa. La investigación descriptiva brinda una metodología apropiada para recolectar información básica para llevar a cabo el proyecto, ya que la misma describe de modo sistemático las características de una población, situación o área de interés.

En esta etapa se elaborarán los instrumentos de recolección de la información que permitió llevar a cabo el Diseño del Sistema de Gestión de la Seguridad de la Información para la división de investigación, con el fin de analizarla, detallarla e interpretarla, para el desarrollo y cumplimiento de los objetivos.

La línea de investigación se enmarcará en el Gobierno de TI, y los conceptos utilizados se relacionaron con temas como: tecnología de la información, seguridad de la información, gestión de la seguridad de la información, gestión de riesgos y sistema de gestión de seguridad de la información.

El diseño del Sistema de Gestión de Seguridad de la Información, se llevará a cabo en (3) fases:

Primera Fase: Diagnostico de la Gestión de la Seguridad de la Información, en la división de investigación. Tomando como base la norma ISO/IEC 27002:2013.

- ✓ Investigación documental de manuales, políticas, decretos, normas.

- ✓ Investigación de campo haciendo uso de encuestas y visitas a las instalaciones con el personal vinculados a los procesos.
- ✓ Procesamiento, análisis y evaluación de los hallazgos encontrados. Dictamen de la evaluación.

Segunda Fase: Diagnóstico de los riesgos de seguridad de la información en la división de investigación.

- ✓ Análisis de riesgos.
- ✓ Identificación de Amenazas
- ✓ Identificación de las Vulnerabilidades.
- ✓ Identificación y Valoración del Riesgo.
- ✓ Análisis y Evaluación del Riesgo.

Cuarta Fase:

- ✓ Documentación de buenas prácticas.
- ✓ Guía de buenas prácticas de la Seguridad de la Información.

Metodología. Este proyecto va dirigido al equipo de trabajo de la División de Investigación de la Universidad Francisco de Paula Santander Ocaña, con el objetivo de proponer un sistema de gestión de la seguridad de la información

3.2 Población y Muestra

Población.

En cuanto a la población objeto de estudio se tomaron en cuenta todos los funcionarios que laboran en la dependencia, y tienen directa relación con la información que se maneja al interior de la División de investigación.

Muestra.

Debido a que la población es limitada, se trabajó como muestra toda la población que conforma la División de investigación y Extensión.

3.3 Técnicas e Instrumentos de Recolección de la Información

Para el desarrollo del proyecto se utilizará la encuesta como técnica de recolección de la Información, aplicando cuestionarios y realizando entrevistas directas a los funcionarios de la División de investigación.

3.4 Procesamiento y análisis de los resultados

La información que se obtenga de las encuestas se registrará y analizará cuantitativamente utilizando tablas y gráficos estadísticos para organizar los datos y así examinar las respuestas dadas por los encuestados

Capítulo 4. Diagnóstico de la dependencia

4.1 Modelo de objetivos

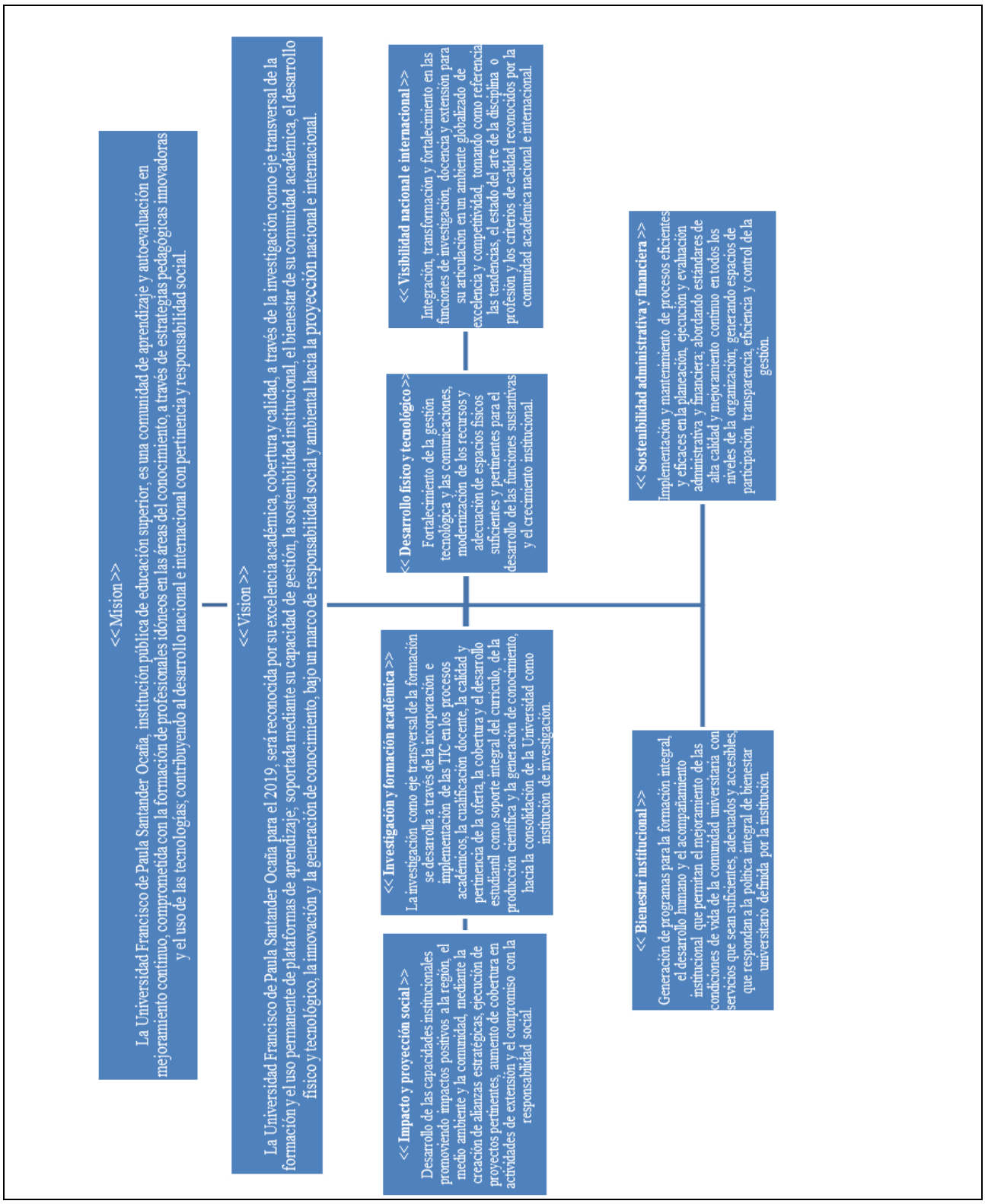

Figura 1: Modelo de objetivos

4.2 Organigrama

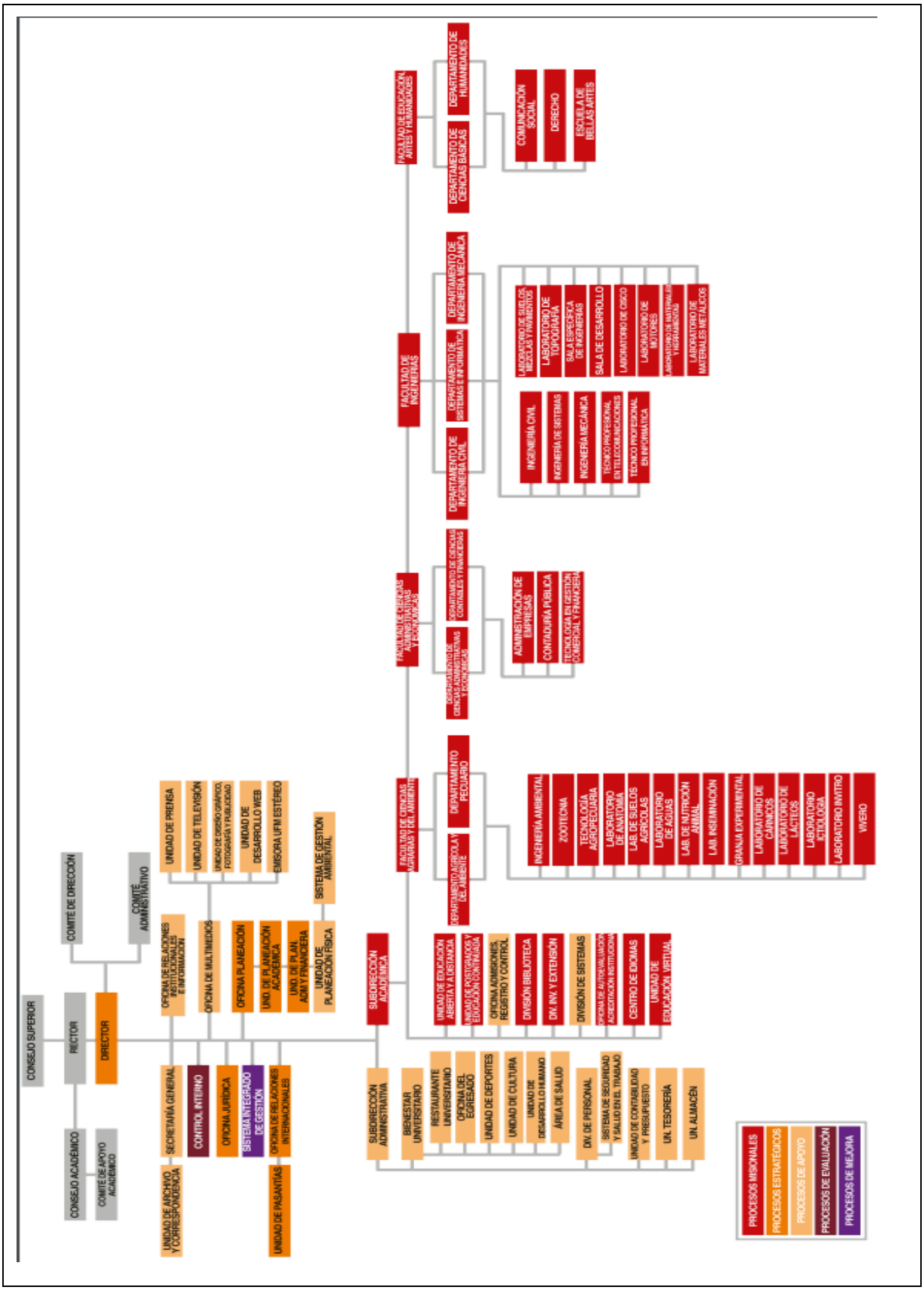

Figura 2: Organigrama de la Universidad Francisco de Paula Santander Ocaña

4.3 Cadena de valor

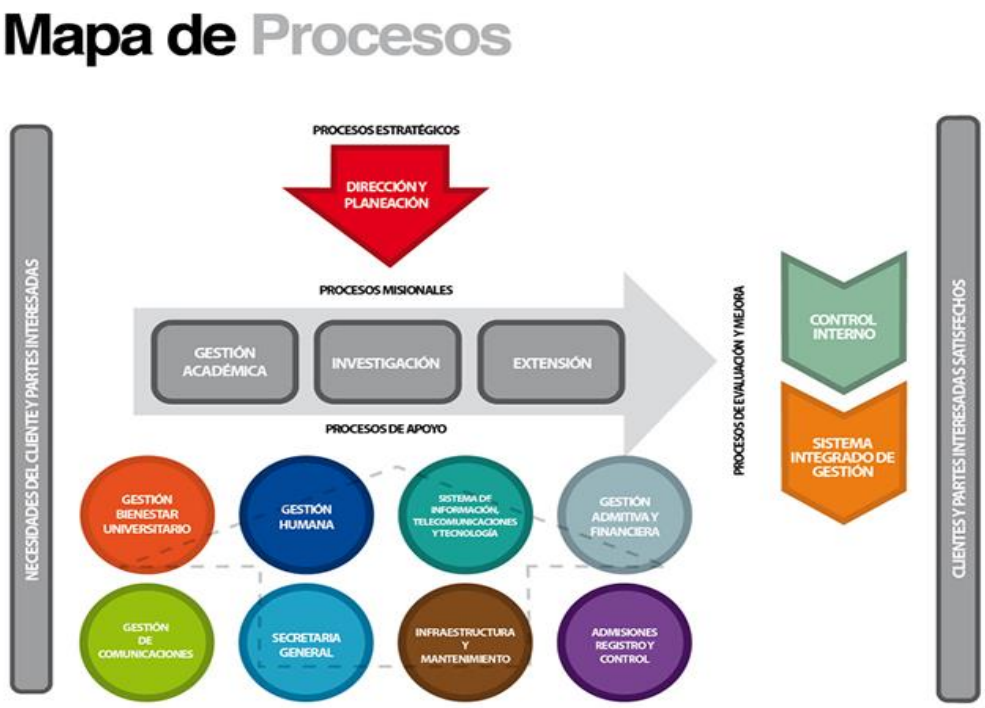

Figura 3: Mapa de Procesos de la Univerisdad Francisco de Paula Santander Ocaña. Fuente: Sitio web ufpso.edu.co

4.4 Descripción de procesos División de Investigación y Extensión

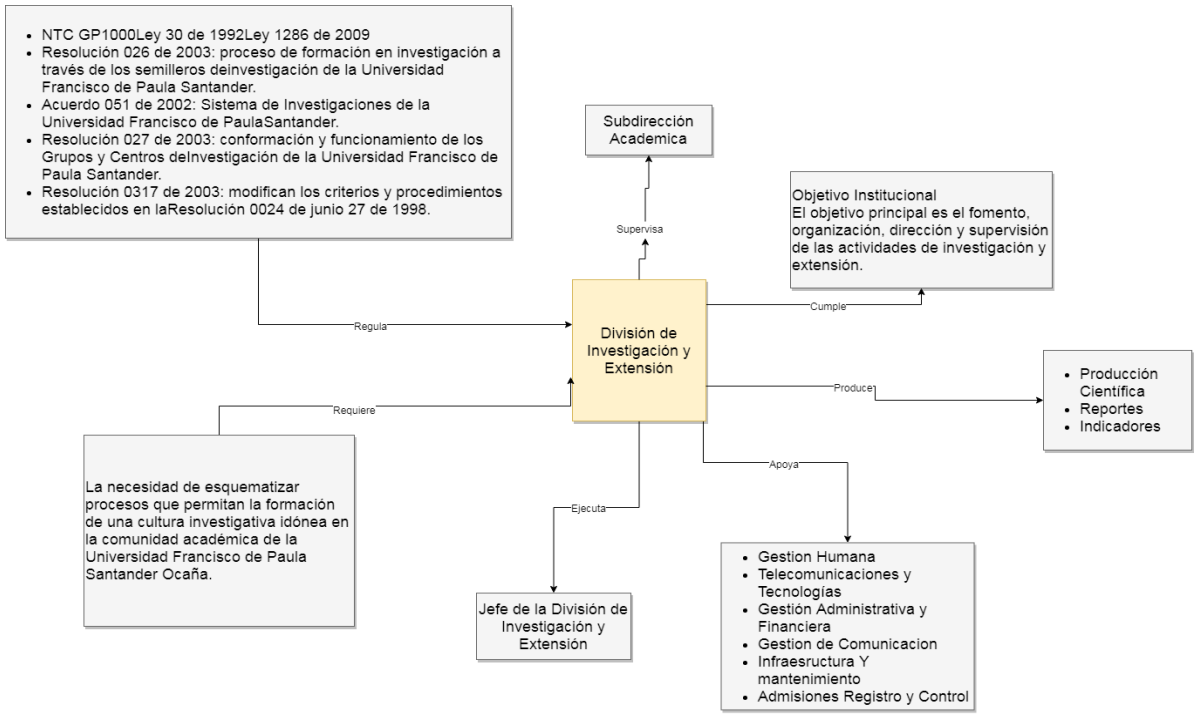

Figura 4: Descripción de procesos División de Investigación y Extensión

4.5 Descripción de procesos División de Investigación

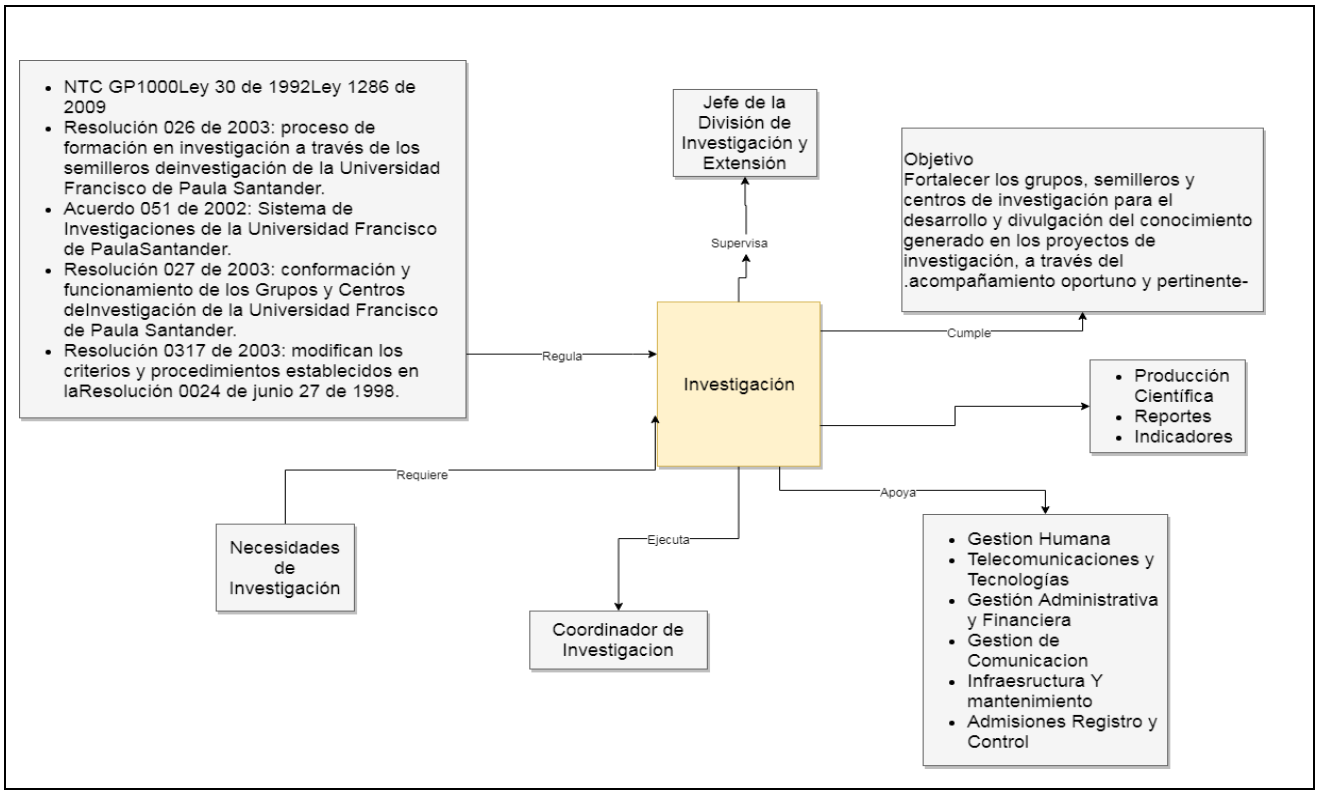

Figura 5: Descripción de procesos División de Investigación

Capítulo 5. Resultados

5.1 Diagnóstico de la seguridad de la información de los procesos incluidos para la División de investigación y Extensión

El dominio 13 Gestión De Los Incidentes De La Seguridad De La Información se utilizó en una encuesta a los funcionarios de la dependencia de la División de Investigación y Extensión para la evaluar la Seguridad de la Información, los funcionarios que fueron encuestados fueron:

- Secretaria
- Coordinador de transferencia tecnológica
- Coordinadora de publicaciones
- Profesional Universitario de la División de Investigación y Extensión

En la primera pregunta la dependencia de la división de investigación y extension manejan los módulos: SID, SGH

Figura 6. Pregunta 2, Del resultado obtenido de la pregunta se puede observar que de todos los encuestados el 50% informan casi de manera inmediata cuando se presenta algún inconveniente en los módulos o sistemas de información que ello usan

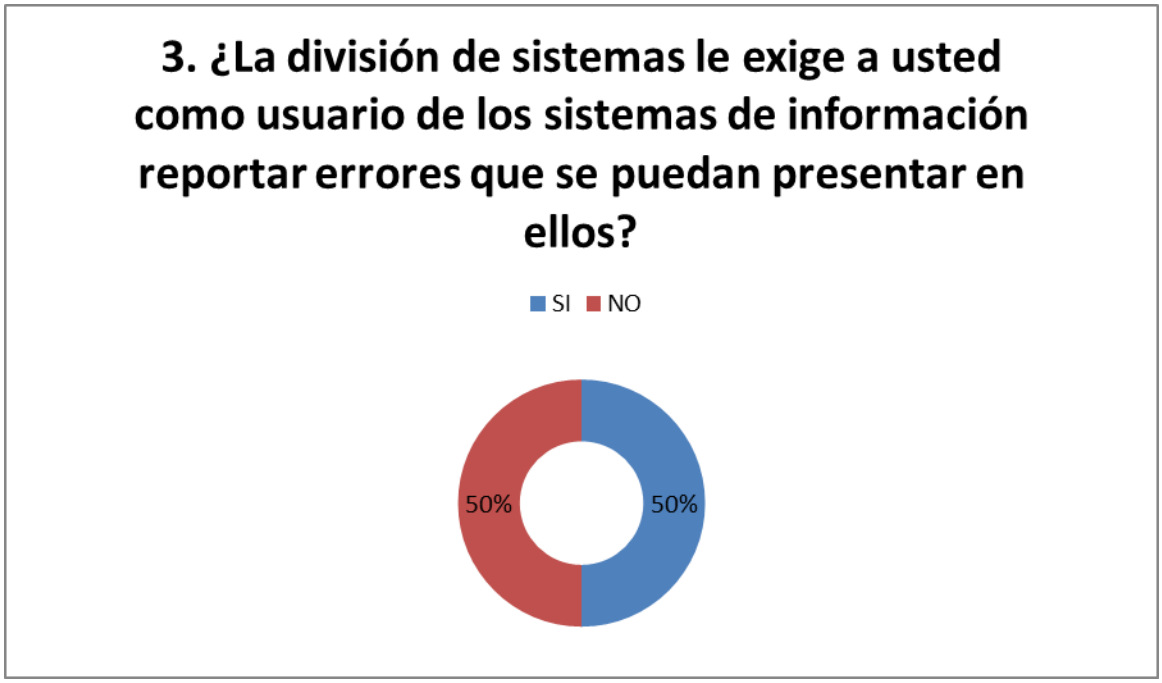

Figura 7: Pregunta , Del resultado de la pregunta se observa que el 50% de los encuestados fueron capacitados o la división de sistemas les exige como usuarios de los módulos o sistemas de información informar fallos en los mismos

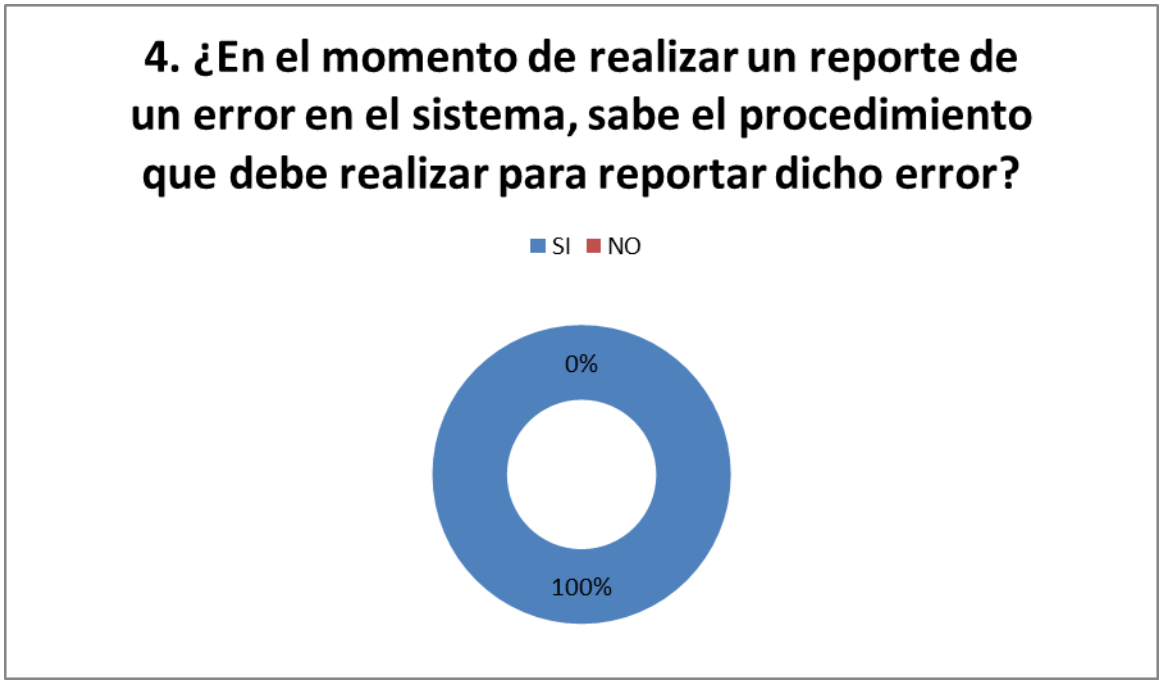

Figura 8. Pregunta 4, De la gráfica se observa que el 100% de los encuestados saben que procedimiento deben seguir para hacer un reporte de errores que se pueda presentar en sus módulos

Figura 9: Pregunta 5, e la gráfica se puede ver que el 83% de los funcionarios saben a quién deben dirigirse en caso de alguna emergencia presentado en sus módulos, pero uno de ellos pide asesoría a la enfermera

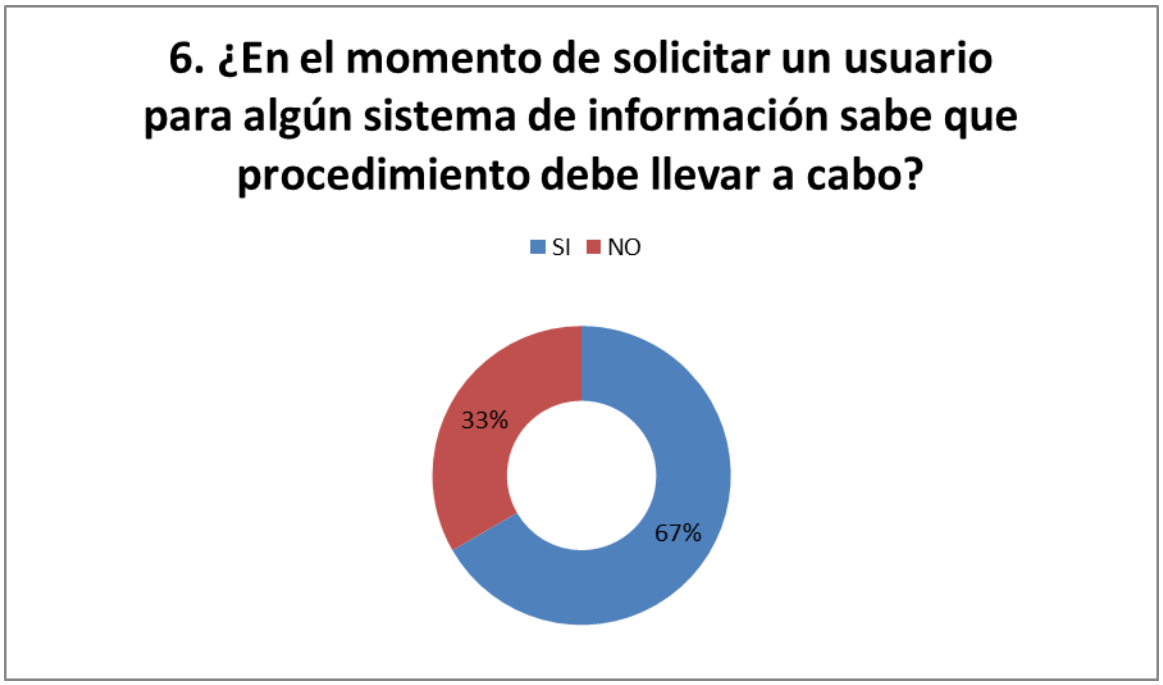

Figura 10. Pregunta 6, De la pregunta observamos que el 67% funcionarios saben que procedimiento deben llevar a cabo para solicitar un usuario para alguno modulo que necesiten usar

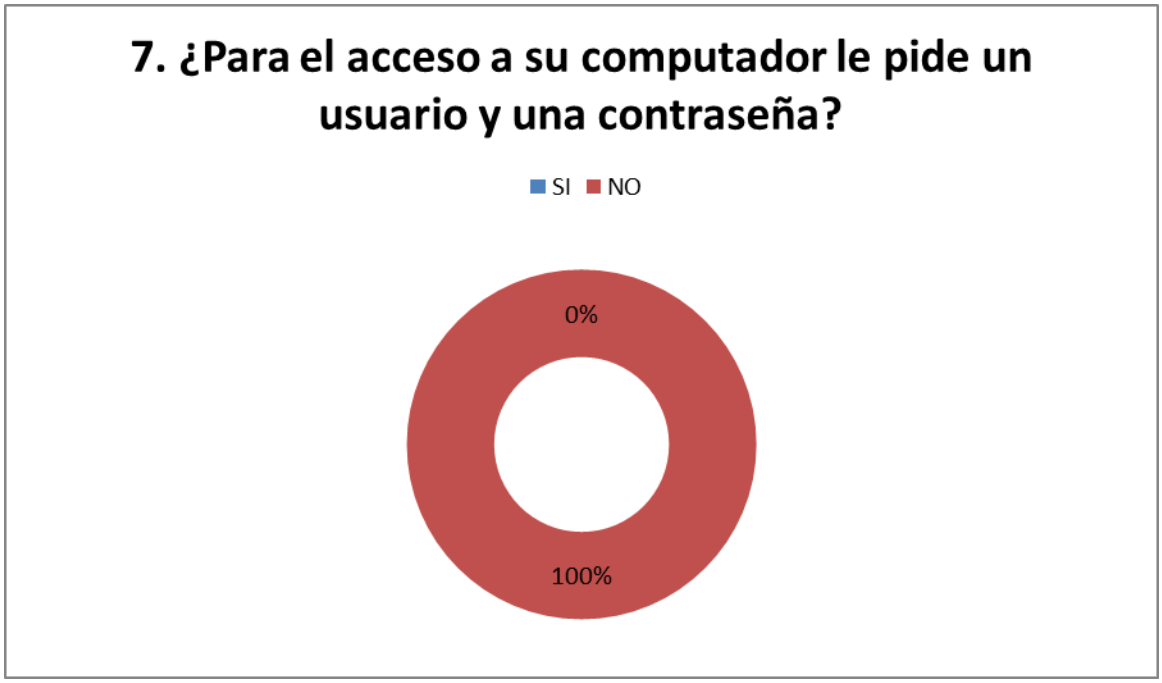

Figura 11. Pregunta 7, De la gráfica se puede observar que el 10% de los funcionarios de la dependencia tienen un usuario y una contraseña establecidos para acceder al computador

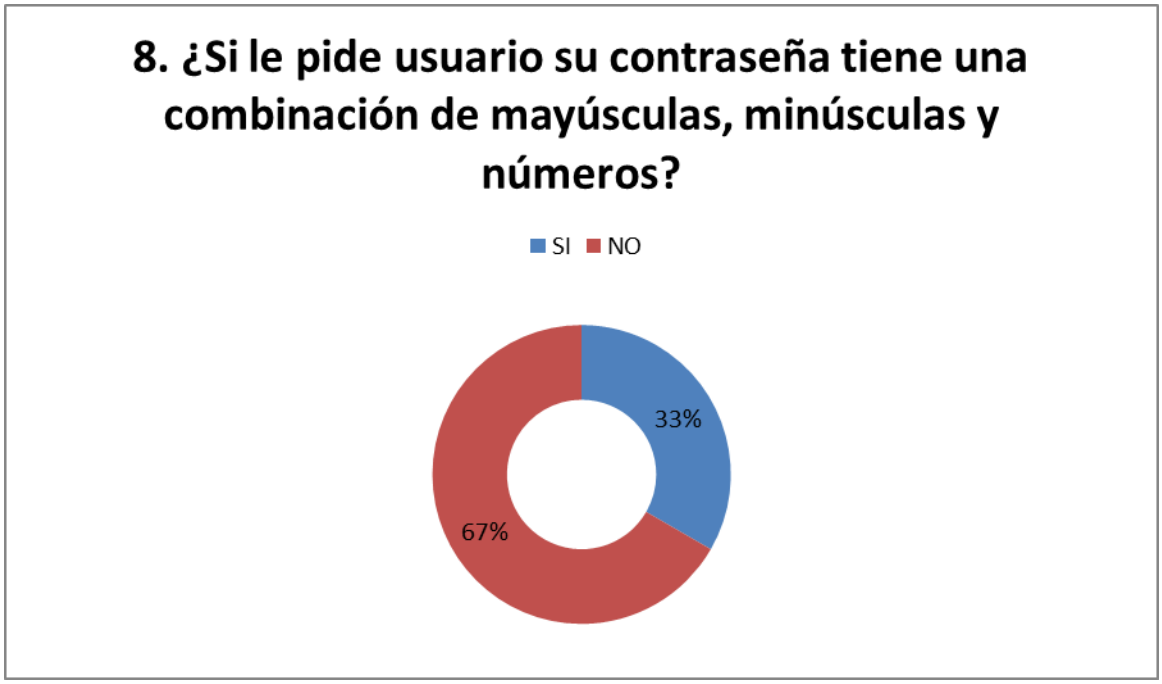

Figura 12. Pregunta 8, Se puede observar que el 67% de los funcionarios que les piden clave de acceso para el computador tienen una contraseña alfanumérica, con un resultado de aprobación medio y un índice por mejorar medio.

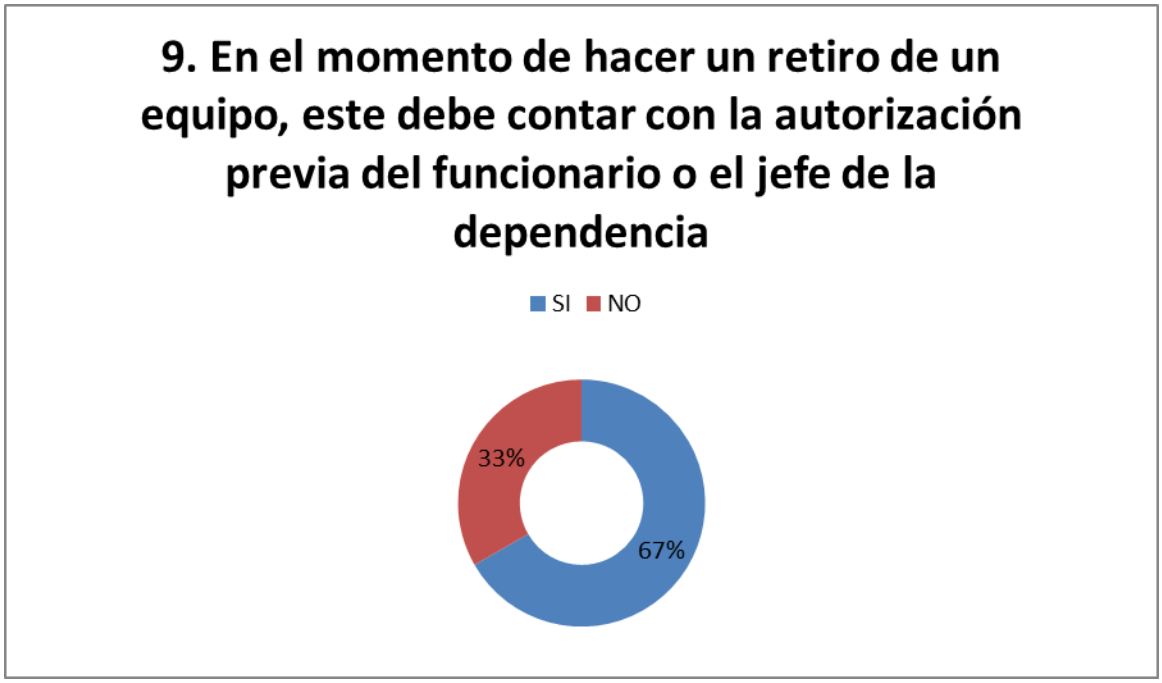

Figura 13. Pregunta 9, Del resultado de la pregunta se aprecia el 67% de los funcionarios tienen claro que para el retiro de un equipo de la oficina esta debe tener primero la autorización del jefe de la dependencia

5.2 Listas de chequeo

ANEXO		ESTADO
A5	**POLÍTICAS DE LA SEGURIDAD DE LA INFORMACION**	
A5.1	Orientación de la dirección para la gestión de la seguridad de la información	
Objetivo: Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes		
A5.1.1	Políticas para la seguridad de la información	No aplica
A5.1.2	Revisión de las políticas para la seguridad de la información.	No aplica
A6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION**	
A6.1	Organización interna	
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.		
A6.1.1	Roles y responsabilidades para la seguridad de la información	No aplica

A6.1.2	Separación de deberes	No aplica
A6.1.3	Contacto con las autoridades	No aplica
A6.1.4	Contacto con grupos de interés especial	No aplica
A6.1.5	Seguridad de la información en la gestión de proyectos.	No aplica
A6.2	Dispositivos móviles y teletrabajo	
Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles		
A6.2.1	Política para dispositivos móviles	No aplica
A6.2.2	Teletrabajo	No aplica
A7	**SEGURIDAD DE LOS RECURSOS HUMANOS**	
A7.1	Antes de asumir el empleo	
Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.		
A7.1.1	Selección	No aplica
A7.1.2	Términos y condiciones del empleo	No aplica
A7.2	Durante la ejecución del empleo	
Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.		
A7.2.1	Responsabilidades de la dirección	No aplica

A7.2.2	Toma de conciencia, educación y formación en la seguridad de la información.	No aplica
A7.2.3	Proceso disciplinario	No aplica
A7.3	Terminación y cambio de empleo	
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo		
A7.3.1	Terminación o cambio de responsabilidades de empleo	No aplica
A8	**GESTION DE ACTIVOS**	
A8.1	Responsabilidad por los activos	
Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección adecuadas.		
A8.1.1	Inventario de activos	No aplica
A8.1.2	Propiedad de los activos	No aplica
A8.1.3	Uso aceptable de los activos	No aplica
A8.1.4	Devolución de activos	No aplica
A8.2	Clasificación de la información	
Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.		
A8.2.1	Clasificación de la información	No aplica
A8.2.2	Etiquetado de la información	No aplica

A8.2.3	Manejo de activos	No aplica
A8.3	Manejo de medios	
Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios		
A8.3.1	Gestión de medio removibles	No aplica
A8.3.2	Disposición de los medios	No aplica
A8.3.3	Transferencia de medios físicos	No aplica
A9	**CONTROL DE ACCESO**	
A9.1	Requisitos del negocio para el control de acceso	
Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.		
A9.1.1	Política de control de acceso	No cumple
A9.1.2	Acceso a redes y a servicios en red	No aplica
A9.2	Gestión de acceso de usuarios	
Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.		
A9.2.1	Registro y cancelación del registro de usuarios	No cumple
A9.2.2	Suministro de acceso de usuarios	No cumple
A9.2.3	Gestión de derechos de acceso privilegiado	No cumple
A9.2.4	Gestión de información de autenticación secreta de usuarios	No cumple
A9.2.5	Revisión de los derechos de acceso de usuarios	No cumple
A9.2.6	Retiro o ajuste de los derechos de acceso	No cumple
A9.3	Responsabilidades de los usuarios	

Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.		
A9.3.1	Uso de información de autenticación secreta	No cumple
A9.4	Control de acceso a sistemas y aplicaciones	
Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.		
A9.4.1	Restricción de acceso a la información	No cumple
A9.4.2	Procedimiento de ingreso seguro	No cumple
A9.4.3	Sistema de gestión de contraseñas	No cumple
A9.4.4	Uso de programas utilitarios privilegiados	No cumple
A9.4.5	Control de acceso a códigos fuente de programas	No aplica
A10	**CRIPTOGRAFIA**	
A10.1	Controles criptográficos	
Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o la integridad de la información		
A10.1.1	Política sobre el uso de controles criptográficos	No aplica
A10.1.2	Gestión de llaves	No aplica
A11	**SEGURIDAD FISICA Y DEL ENTORNO**	
A11.1	Áreas seguras	
Objetivo: Prevenir el acceso físico no autorizado, el daño e la interferencia a la información y a las instalaciones de procesamiento de información de la organización.		
A11.1.1	Perímetro de seguridad física	No cumple
A11.1.2	Controles de acceso físicos	No cumple

A11.1.3	Seguridad de oficinas, recintos e instalaciones.	No cumple
A11.1.4	Protección contra amenazas externas y ambientales.	No cumple
A11.1.5	Trabajo en áreas seguras.	No cumple
A11.1.6	Áreas de carga, despacho y acceso público	No cumple
A11.2	Equipos	
Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.		
A11.2.1	Ubicación y protección de los equipos	No cumple
A11.2.2	Servicios de suministro	No cumple
A11.2.3	Seguridad en el cableado.	No cumple
A11.2.4	Mantenimiento de los equipos.	No cumple
A11.2.5	Retiro de activos	Cumple parcialmente
A11.2.6	Seguridad de equipos y activos fuera de las instalaciones	No cumple
A11.2.7	Disposición segura o reutilización de equipos	Cumple parcialmente
A11.2.8	Equipos de usuario desatendido	Cumple parcialmente
A11.2.9	Política de escritorio limpio y pantalla limpia	Cumple parcialmente
A12	**SEGURIDAD DE LAS OPERACIONES**	

A12.1	Procedimientos operacionales y responsabilidades	
Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.		
A12.1.1	Procedimientos de operación documentados	No cumple
A12.1.2	Gestión de cambios	No cumple
A12.1.3	Gestión de capacidad	No aplica
A12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	No aplica
A12.2	Protección contra códigos maliciosos	
Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.		
A12.2.1	Controles contra códigos maliciosos	No aplica
A12.3	Copias de respaldo	
Objetivo: Proteger contra la perdida de datos		
A12.3.1	Respaldo de la información	No aplica
A12.4	Registro y seguimiento	
Objetivo: Registrar eventos y generar evidencia		
A12.4.1	Registro de eventos	No cumple
A12.4.2	Protección de la información de registro	Cumple parcialmente
A12.4.3	Registros del administrador y del operador	No aplica
A12.4.4	Sincronización de relojes	No aplica
A12.5	Control de software operacional	
Objetivo: Asegurarse de la integridad de los sistemas operacionales		
A12.5.1	Instalación de software en sistemas operativos	No aplica
A12.6	Gestión de la vulnerabilidad técnica	

Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas		
A12.6.1	Gestión de las vulnerabilidades técnicas	No aplica
A12.6.2	Restricciones sobre la instalación de software	No aplica
A12.7	Consideraciones sobre auditorias de sistemas de información	
Objetivo: Minimizar el impacto de las actividades de auditoria sobre los sistemas operativos		
A12.7.1	Controles de auditorías de sistemas de información	No aplica
A13	**SEGURIDAD DE LAS COMUNICACIONES**	
A13.1	Gestión de la seguridad de las redes	
Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.		
A13.1.1	Controles de redes	No aplica
A13.1.2	Seguridad de los servicios de red	No aplica
A13.1.3	Separación en las redes	No aplica
A13.2	Transferencia de información	
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.		
A13.2.1	Políticas y procedimientos de transferencia de información	No cumple
A13.2.2	Acuerdos sobre transferencia de información	No cumple
A13.2.3	Mensajería Electronica	No cumple
A13.2.4	Acuerdos de confidencialidad o de no divulgación	No aplica
A14	**Adquisición, desarrollo y mantenimiento de sistemas**	
A14.1	Requisitos de seguridad de los sistemas de información	

Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes .		
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	No aplica
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	No aplica
A.14.1.3	Protección de transaccciones de los servicios de las aplicaciones.	No aplica
A14.2	Seguridad en los procesos de Desarrollo y de Soporte	
Objetivo: Asegurar que la seguridad de la información este diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.		
A.14.2.1	Política de desarrollo seguro	No aplica
A.14.2.2	Procedimientos de control de cambios en sistemas	No aplica
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	No aplica
A.14.2.4	Restricciones en los cambios a los paquetes de software	No aplica
A.14.2.5	Principio de Construcción de los Sistemas Seguros.	No aplica
A.14.2.6	Ambiente de desarrollo seguro	No aplica
A.14.2.7	Desarrollo contratado externamente	No aplica

A.14.2.8	Pruebas de seguridad de sistemas	No aplica
A.14.2.9	Prueba de aceptación de sistemas	No aplica
A14.3	Datos de prueba	
Objetivo: Asegurar la protección de los datos usados para pruebas.		
A.14.3.1	Protección de datos de prueba	No aplica
A15	**RELACIONES CON LOS PROVEEDORES**	
A15.1	Seguridad de la información en las relaciones con los proveedores.	
Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.		
A15.1.1	Política de seguridad de la información para las relaciones con proveedores	No aplica
A15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	No aplica
A15.1.3	Cadena de suministro de tecnología de información y comunicación	No aplica
A15.2	Gestión de la prestación de servicios de proveedores	
Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores		
A15.2.1	Seguimiento y revisión de los servicios de los proveedores	No aplica
A15.2.2	Gestión del cambio en los servicios de los proveedores	No aplica
A16	**GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION**	
A16.1	Gestión de incidentes y mejoras en la seguridad de la información	
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.		

A16.1.1	Responsabilidades y procedimientos	No aplica
A16.1.2	Reporte de eventos de seguridad de la información	No aplica
A16.1.3	Reporte de debilidades de seguridad de la información	No aplica
A16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	No aplica
A16.1.5	Respuesta a incidentes de seguridad de la información	No aplica
A16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	No aplica
A16.1.7	Recolección de evidencia	No aplica
A17	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO**	
A17.1	Continuidad de Seguridad de la información	
Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.		
A17.1.1	Planificación de la continuidad de la seguridad de la información	No aplica
A17.1.2	Implementación de la continuidad de la seguridad de la información	No aplica
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	No aplica
A17.2	Redundancias	
Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.		

A17.2.1	Disponibilidad de instalaciones de procesamiento de información	No aplica
A18	**CUMPLIMIENTO**	
A18.1	Cumplimiento de requisitos legales y contractuales	
Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.		
A18.1.1	Identificación de la legislación aplicable.	No aplica
A18.1.2	Derechos propiedad intelectual (DPI)	No aplica
A18.1.3	Protección de registros	No aplica
A18.1.4	Privacidad y protección de información de datos personales	No aplica
A18.1.5	Reglamentación de controles criptográficos.	No aplica
A18.2	Revisiones de seguridad de la información	
Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.		
A18.2.1	Revisión independiente de la seguridad de la información	No aplica
A18.2.2	Cumplimiento con las políticas y normas de seguridad	No aplica

A18.2.3	Revisión del cumplimiento técnico	No aplica

Figura 14. Listas de chequeo de la Norma ISO 27001:2013

Avances por dominio de control

POR DOMINIO DE CONTROL						
NOMBRE DOMINIOS DE CONTROL	CONTROLES QUE APLICAN	PESO CONTROLES IMPLEMENTADOS Y PARCIALMENTE IMPLEMENTADOS	IMPLEMENTADOS	PARCIALMENTE	NO CUMPLE	NO APLICA
DOMINIO 5 - POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	0	0	0	0	0	2
DOMINIO 6 - ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	0	0	0	0	0	7
DOMINIO 7 - SEGURIDAD DE LOS RECURSOS HUMANOS	0	0	0	0	0	6
DOMINIO 8 - GESTIÓN DE ACTIVOS	0	0	0	0	0	10
DOMINIO 9 - CONTROL DE ACCESO	12	0	0	0	12	2
DOMINIO 10 - CRIPTOGRAFÍA	0	0	0	0	0	2
DOMINIO 11 - SEGURIDAD FÍSICA Y DEL ENTORNO	15	2	0	4	11	0
DOMINIO 12 - SEGURIDAD DE LAS OPERACIONES	4	0,5	0	1	3	10
DOMINIO 13 - SEGURIDAD DE LAS COMUNICACIONES	3	0	0	0	3	4
DOMINIO 14 - ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE	0	0	0	0	0	13
DOMINIO 15 - RELACIÓN CON LOS PROVEEDORES	0	0	0	0	0	5
DOMINIO 16 - GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	0	0	0	0	0	7
DOMINIO 17 - ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO	0	0	0	0	0	4
DOMINIO 18 - SEGURIDAD DE LAS COMUNICACIONES	0	0	0	0	0	8
	34					

Figura 15. Avances por dominio de control

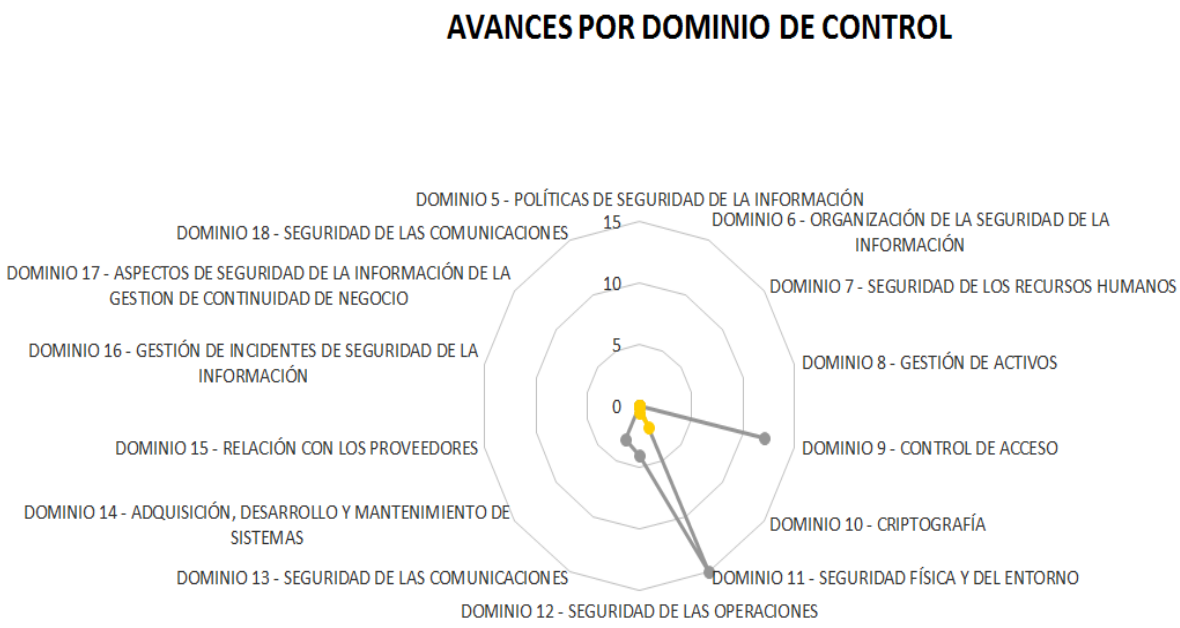

Figura 16. Se evidencia que luego de haber realizado la lista de chequeo el Dominio 9. Control de Acceso y el Dominio 11 seguridad física y del entorno, son dos elementos a los que se les debe prestar mayor atención, por los riesgo y amenazas inherentes a estos.

Controles para la seguridad de la información

Gestión de activos

- Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.
- Los activos mantenidos en el inventario deben tener un propietario.
- Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.

- Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.
- La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
- Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.
- Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.

Control de acceso

- Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.
- Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.
- Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado
- La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.
- Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.

- Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.
- Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.

- El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.
- Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.
- Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.
- Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.

Seguridad física y del entorno

Áreas Seguras

- Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.
- Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.
- Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones.

- Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
- Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.
- Se deben controlar los puntos de acceso tales como las áreas de despacho y carga y otros puntos por donde pueden entrar personas no autorizadas y, si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.

Equipos

- Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.
- Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.
- El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.
- Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
- Los equipos, información o software no se deben retirar de su sitio sin autorización previa
- Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.
- Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición

o reúso.

- Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.
- Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.

Seguridad de las operaciones

- Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.
- Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
- Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
- Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.

Seguridad de las comunicaciones

- Se debe contar con políticas, procedimientos y controles de transferencia información formales para proteger la transferencia de información mediante el uso de
- todo tipo de instalaciones de comunicaciones.

- Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.
- Se debe proteger adecuadamente la información incluida en la mensajería electrónica.

Gestión de incidentes de seguridad de la información

- Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
- Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.
- Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.
- Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.
- Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.
- El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o impacto de incidentes futuros.
- La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.

Informe de auditoria

PhD. Torcoroma Velásquez Pérez

Jefe de División de Investigación y Extensión

Universidad Francisco de Paula Santander Ocaña

En uso de su aprobación para la realización de la auditoria en la División de Investigación y Extensión, para evaluar los aspectos de la seguridad de la información de la dependencia.

1. Objetivo De La Auditoria

- Evaluar la seguridad física de la dependencia de la División de Investigación y extensión
- Evaluar la seguridad de la información

2. Alcance de la auditoria

La auditoría se llevará a cabo a la Seguridad Física, y de la Información de la dependencia de la División de investigación y Extensión de la Universidad Francisco de Paula Santander Ocaña, desde el 01 de octubre del 2018 al 28 de febrero de 2019.

3. Hallazgos Potenciales

- Inexistencia de software de protección contra virus y malware
- Falta de claves de acceso a los equipos de la dependencia
- Falta de copias de seguridad internas
- No cuentan con regulador de energía ni UPS

- No cuentan con firewall activado algunos equipos

- Algunos funcionarios no se encuentran capacitados para reporte de errores presentado en los módulos o sistemas de información

- Falta de elementos de seguridad en caso de emergencia

- Ambiente de escritorio no despejado

4. Conclusiones

Como resultado de la Auditoría realizada a la dependencia de la División de investigación y Extensión de la Universidad Francisco de Paula Santander Ocaña, por el período comprendido entre el 01 de octubre del 2018 al 28 de febrero de 2019, podemos manifestar que hemos cumplido con evaluar cada uno de los objetivos contenidos en el programa de auditoria.

5. Recomendaciones

- Instalar antivirus a todos los equipos de la dependencia con sus respectivas licencias

- Activar el firewall a todos los equipos de la dependencia

- Crear una política interna de respaldos de información para documentos internos

- Solicitar Capacitación a los empleados sobre la importancia de claves de acceso a los equipos para seguridad de la información

- Solicitar Capacitación a los empleados sobre la importancia del reporte de errores presentados en los módulos o sistemas de información usados por ellos

- Adquisición de una UPS y reguladores de energía para los equipos en caso de descarga eléctrica o falla de luz

- Adquisición de elementos de seguridad faltantes en la dependencia (detectores de humo)

- Capacitar a los empleados de la importancia de tener un ambiente de escritorio despejado

Conclusiones

Con el desarrollo del presente trabajo de grado, realizado en la División de Investigación y Extensión de la Universidad Francisco de Paula Santander Ocaña inicialmente se hizo un estudio y análisis de la ISO 27001, luego del análisis hecho se decidió tomar la ISO 27002 como referencia.

Se logró realizar un diagnóstico que permitiría comprender el estado actual de la dependencia en cuanto a las tecnologías de la información, lo que conllevo a evidenciar las debilidades y amenazas existentes en ella.

De acuerdo a los fallos encontrados en la dependencia de la División de Investigación y Extensión se realizaron los controles pertinentes con el objetivo de evitar amenazas a futuro.

Recomendaciones

Se hace necesaria la implementación de las políticas aquí expuestas con el objetivo de poder ir en búsqueda de la mejora continua dentro de la organización

Referencias

Altamirano, J. y Bayona, S. (2017). Políticas de Seguridad de la Información: Revisión Sistemática de las Teorías que Explican su Cumplimiento. *Revista Ibérica de Sistemas e Tecnologías de Información, 1*(25). Recuperado de http://www.scielo.mec.pt/scielo .php?script=sci_arttext&pid=S1646-98952017000500009

Álvarez Z. (2016). ISO/IEC 27001:2013 – sistemas de Gestión de seguridad de la Información. *Universidad Piloto de Colombia.* Recuperado de http://polux.unipiloto.edu.co:8080 /00003427.pdf

Arguello, G. (2010). Historia de la seguridad de la informacion.

Ascanio, J. G., Trillos, R. A., & Bautista, D. W. (2015). *Implantation of a safety management system information under the ISO 27001: risk analysis information.*

Ballesteros, A. (s.f.). Riesgo, Amenaza y Vulnerabilidad. Bogotá, Colombia: Seguridad de instalaciones. Recuperado de http://epn.gov.co/elearning/distinguidos/SEGURIDAD/13_ riesgo_amenaza_y_vulnerabilidad.html

Castro, A. R., & Bayona, Z. O. (2016). Technology risk management based on ISO 31000.

Castro, F. Ciacedo C. (2013). La norma iso 27001. Recuperado de http://es.slideshare.net/Karlos19s/la-norma-iso-27001-2- 28689086

Cruz Garzón, J. J. (2015). Aspectos de Analisis Gestión de Riesgos, Seguridad y Protección de la información en las Organizaciones de Colombia.

Definición ABC. (2008). Definición de Información. Sao Paulo, Brasil: DefiniciónABC tú diccionario hecho fácil. Recuperado de https://www.definicionabc.com/tecnologia /informacion.php

Definición ABC. (2008). Definición de Informática. Sao Paulo, Brasil: DefiniciónABC tú diccionario hecho fácil. Recuperado de https://www.definicionabc.com/tecnologia /informatica.php

Dieguez, M., Cares, C., & Cachero, C. (2017). Methodology for the information security controls selection.

García, L. (2006). Introducción a la teoría de la confiabilidad y su aplicación en el diseño y mantenimiento de equipos industriales de un proceso de renovación (Tesis de pregrado) Universidad nacional de Colombia, Medellín

Infante Moro, A., Infante Moro, J. C., Martinez Lopez, F. J., & García Ordaz, M. (2016). LA AUDITORÍA INFORMÁTICA EN ESPAÑA: EL CASO DE LOS HOTELES.

INSPQ. (2018). Definición del concepto de seguridad. Québec, Canada: INSPQ Competencias e información especializada en salud pública. Recuperado de https://www.inspq.qc.ca/es/centro-collaborador-oms-de-quebec-para-la-promocion-de-la-seguridad-y-prevencion-de-traumatismos/definicion-del-concepto-de-seguridad

ISO. (2014). ISO 27000.ES. Recuperado de: http://www.iso27000.es/glosario.html

ISO27000. (2005). El portal de ISO 27001 en español. ISO27000.ES. Recuperado de http://americalatina.pmi.org/latam/pmbokguideandstandards/whatisastandar.aspx

ISO 27001. (2015). La norma ISO 27001 versión 2013. SGSI log especializado en Sistemas de Gestión de Seguridad de la Información. Recuperado de https://www.pmg-ssi.com/2015/10/la-norma-iso-27001-version-2013/

Koch, R., & Golling, M. (2018). The Cyber Decade:Cyber Defence at aX-ing Point.

Lemieux, V. (2016). *Blockchain.*

Ley 23 de 1982. (2014). Derecho de autor y propiedad intelectual ley. Recuperado de http:// http://legislacion.vlex.com.co/vid/ley-derechos- autor-71608275

Ley 44 de 1993. (2014). Derecho de autor. Recuperado de http:// http://www.derechodeautor.gov.co/documents

Ley 527 De 1999. (2014). Recuperado de http://www.alcaldiabogota.gov.co/sisjur/normas /Norma1.jsp?i=4276

Ley 719 de 2001. (2014). Recuperado de http://www.alcaldiabogota.gov.co /sisjur/normas/Norma1.jsp?i=5533-ftp://ftp.camara.gov.co/

Ley 1273 5 de enero de 2009. (s.f.). Recuperado de http://www.mintic.gov.co/portal/604/articles- 3705_documento.pdf

Martelo, R. J., Tovar, L. C., & Maza, D. A. (2018). Modelo Básico de Seguridad Lógica. Caso de Estudio: el.

PELLICER, M. L. (2013). HOMENAJE A TURING: DE LAS MÁQUINAS DE TURING A PROBLEMAS CRIPTOGRÁFICOS.

Perez, J. y Merino, M. (2008). Concepto de gestión. Definicion.de. Recuperado de https://definicion.de/gestion/

PMI. (2018). ¿Qué es un estándar? Newtown Square, USA: PMI. Recuperado de http://americalatina.pmi.org/latam/pmbokguideandstandards/whatisastandar.aspx

Rodríguez, M. Diseño de proyectos y desarrollo de tesis en ciencias administrativas, Organizacionales y sociales. (2010) Culiacán Sinaloa, México: Universidad autónoma de Sinaloa.

Sabino, C. y Reyes, J. (1999). *El proyecto de investigación.* Caraca, Venezuela: Editorial Episteme.

Santiago Chinchilla, E. J. (2009). Penetration test on the support of risk evaluation on information security.

Santiago Chinchilla, E. J., & Sánchez Allende, J. (2017). RIESGOS DE CIBERSEGURIDAD EN LAS EMPRESAS.

Seif, Y., & Beni, N. N. (2018). Identifying the effective components of information security management in information technology of iranian offshore oil company.

Siponen, M., Pahnila, S., & Mahmood, A. (2014). Employees' Adherence to Information. 217-224.

Sokolov, S. S., Alimov, O. M., Golubeva, M. G., Burlov, V. G., & Vikhrov, N. M. (2018). The Automating Process of Information Security.

Valencia, & Orozco. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *Revista lbérica de Sistemas y Tecnologías de Informa ción*.

VEGA, M. L., PEÑARANDA, A. D., & ACOSTA, R. S. (2017). DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA LA SECRETARIA DE.

Velásquez Pérez, T., Pérez, Y. M., & Messino Sossa, A. (2016). APLICACIÓN DE SISTEMAS DE GESTION DE SEGURIDAD DE LA INFORMACION.

Apéndice A: Programa de auditoria

JC AUDITORES	**PROGRAMA DE AUDITORIA**			
Empresa: Universidad Francisco de Paula Santander Ocaña – División de Investigación y Extensión				**Fecha: 01-09-2018**
Fase	**Actividad**	**Horas Estimadas**	**Hora Total**	**Encargados**
1	Visita Preliminar • Recopilación de la información organizacional: Estructura orgánica, misión y visión de la dependencia, Recurso humano. • Reunión con el jefe de la División de Investigación y Extensión	6 Hrs 2 Hrs	8 Hrs	
2	Desarrollo de la auditoria • Entrevista con el jefe • Encuesta a funcionarios de la dependencia • Inventario de Hardware • Inventario de Software • Aplicación de listas de chequeo (Seguridad de la información) • Aplicación de pruebas de cumplimiento	2 Hrs 16 Hrs 20 Hrs 20 Hrs 71 Hrs 71 Hrs	200 Hrs	

3	Revisión y pre informe • Revisión de la información obtenida del desarrollo de la auditoria • Diagnóstico de la empresa(Situaciones encontradas, Desviaciones encontradas) • Elaboración del borrador del Diagnostico • Presentación del borrador al Jefe de la División de Investigación y Extensión	60 Hrs 100 Hrs 120 Hrs 20 Hrs	300 Hrs	
4	Informe • Elaboración y presentación del diagnóstico final	52 Hrs	52 Hrs	

Apéndice B: Guía de auditoria

GUÍA DE AUDITORIA				
Empresa: Universidad Francisco de Paula Santander Ocaña				**05/07/2018**
Área: División de Investigación y Extensión				
Ref.	**Actividad o función a evaluar**	**Procedimiento de auditoria**	**Herramientas que serán utilizadas**	**Observación**
1	Evaluar la seguridad en el acceso de los usuarios a los equipos de la dependencia	Solicitar a los funcionaros correspondientes ingresar y digitar sus credenciales de acceso	Observación Pruebas Entrevista	El equipo no debe permitir el ingreso a personas no autorizadas
2	Verificar la existencia de antivirus	Solicitar el acceso a los equipos de la dependencia para verificar la existencia de antivirus adecuados Verificar la licencia de los mismos así como sus actualizaciones correspondientes	Observación Pruebas Entrevista	Los equipos de cómputo deben tener obligatoriamente instalado su respectivo antivirus para protección de la información.
3	Verificar la existencia de manuales de usuario en los sistemas de información usados por la dependencia de la División de Investigación y Extensión	Solicitar a algunos funcionarios que aceda a los sistemas de información que usan, y verificar algún enlace que muestre el manual de usuario. Solicitar a la división de sistemas los manuales de usuario de aquellos sistemas de información que no lo contengan en su sistema.	Observación Pruebas Entrevista	Cada sistema de información debe tener su respectivo manual de usuario
4	Verificar la existencia de un plan de contingencia	Solicitar a la oficina de salud ocupacional los planes de	Observación Pruebas	La universidad debe contar con sus respectivos

	en la Universidad Francisco de Paula Santander Ocaña	contingencia de la universidad. Verificar que los planes de contingencia cubran todos los aspectos de la División de Investigación y Extensión		planes de contingencia en caso de emergencias.

Apéndice C: Dominios excluidos

NOMBRE DOMINIOS DE CONTROL	OBSERVACIÓN
DOMINIO 5 - POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	La dirección junto con la división de sistemas son los que encargados de la revisión y aprobación de las políticas de seguridad de la información, aplica para todo el dominio.
DOMINIO 6 - ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	La dirección junto con la división de sistemas son los que encargados de la aplicación de la seguridad de la información de la universidad incluyendo las partes internas y externas, aplica para todo el dominio.
DOMINIO 7 - SEGURIDAD DE LOS RECURSOS HUMANOS	La oficina de personal, la dirección y la oficina salud ocupacional se encarga de la aplicabilidad del dominio, incluyendo antes, durante y después de la contratación laboral. Aplica para todo el dominio.
DOMINIO 8 - GESTIÓN DE ACTIVOS	La oficina de almacén junto con la división de sistemas son los encargados de gestión de los activos de cada una de las dependencias de la universidad, incluyendo la seguridad de la información como el valor, requisitos legales, sensibilidad, etc. Aplica para todo el dominio.
DOMINIO 9 - CONTROL DE ACCESO	
DOMINIO 10 - CRIPTOGRAFÍA	La división de sistemas es el responsable
DOMINIO 11 - SEGURIDAD FÍSICA Y DEL ENTORNO	
DOMINIO 12 - SEGURIDAD DE LAS OPERACIONES	
DOMINIO 13 - SEGURIDAD DE LAS COMUNICACIONES	
DOMINIO 14 - ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	La división de sistemas junto con la oficina de almacén son los encargados de la aplicabilidad de este dominio, aplica para todo el dominio
DOMINIO 15 - RELACIÓN CON LOS PROVEEDORES	La oficina de almacén junto con la división de sistemas son los encargados de gestión
DOMINIO 16 - GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	La oficina de división de sistemas son los encargados de gestión
DOMINIO 17 - ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO	

Apéndice D: Dictamen de auditoria

De acuerdo con los resultados obtenidos de la evaluación, se encontró las siguientes situaciones:

Las medidas de seguridad que tienen los equipos de cómputo de la dependencia de la División de Investigación y Extensión Universitario no son del todo seguras debido a que estos no cuentan con un software de protección contra virus y malware, donde se observó que de todos los equipos de la dependencia ninguno cuenta con software de protección, lo que provoca que los equipos sean infectados ocasionando perdida y manipulación de la información.

Además, se verifico que de los equipos de la dependencia ninguno cuentan con claves de acceso a los computadores, lo que origina acceso indebido de personas ajenas a la dependencia, como también de manipulación y robo de información.

En las medidas internas de control de la dependencia los equipos no tienen un plan de respaldo de copias de seguridad para los documentos manejados internamente, lo que ocasiona que, en caso de daño del equipo, daño del disco local C y robo de información, los documentos se pierdan y no se tenga una manera de poder recuperar esta información, trayendo problemas a la dependencia de la División de Investigación y Extensión.

En las medidas de seguridad tecnológica ninguno de los equipos de la dependencia cuenta con reguladores de energía, ni una UPS (Sistema de Alimentación Interrumpida) que protejan los equipos en caso de una descarga eléctrica o desconexión de la energía eléctrica, lo que ocasiona que la información no guardada se pierda, además de quemarse los equipos y el rendimiento de trabajo del funcionario hacia sus usuarios.

En medidas de seguridad en caso de presentarse un problema con los sistemas de información o módulos usados por los funcionarios, muchos funcionarios no fueron capacitados o la división de sistemas no les exige como trabajadores de la universidad reportar los errores que se puedan presentar en estos sistemas o módulos, lo que conlleva a problemas de seguridad.

Por último, la dependencia no cuenta con un plan de continuidad del negocio, lo que ocasiona demoras o agilidad en los procesos que se trabajan a diario y se tienen programados de manera semestral.

De antemano estaré atento a cualquier inquietud que tenga con respecto al presente dictamen.

Atentamente,

JESUS CAMARGO PEREZ
Auditor Líder
JC Auditores

Apéndice E: Encuesta dirigida a funcionarios de la Universidad Francisco de Paula Santander Ocaña, dependencia División de Investigación y Extensión

Objetivo:

Diagnosticar La Seguridad De La Información A La Dependencia De División de Investigación Y Extensión De La Universidad Francisco De Paula Santander Ocaña

1. Que sistemas de información o módulos usa:

_____

_____

_____

2. ¿Cuándo sucede un fallo en los sistemas de información usados por usted, estos deben ser informados al instante por algún canal de reporte de errores?

Si: _____ No: _____

3. ¿La división de sistemas le exige a usted como usuario de los sistemas de información reportar errores que se puedan presentar en ellos?

Si: _____ No: _____

4. ¿En el momento de realizar un reporte de un error en el sistema, sabe el procedimiento que debe realizar para reportar dicho error

Si: _____ No: _____

5. ¿A parte del reporte del error usted sabe a quién acudir?

Si: _____ No: _____

A quien: _____

6. ¿En el momento de solicitar un usuario para algún sistema de información sabe que procedimiento debe llevar a cabo?

Si: _____ No: _____

7. ¿Para el acceso a su computador le pide un usuario y una contraseña?

Si: _____ No: _____

8. ¿Si le pide usuario su contraseña tiene una combinación de mayúsculas, minúsculas y números?

Si: _____ No: _____

9. En el momento de hacer un retiro de un equipo, este debe contar con la autorización previa del funcionario o el jefe de la dependencia

Si: _____ No: _____

Apéndice F: Entrevista dirigida al jefe de la Dependencia División de Investigación y Extensión de la Universidad Francisco de Paula Santander Ocaña

Objetivo:

Diagnosticar La Seguridad De La Información a La Dependencia División de Investigación y Extensión De La Universidad Francisco De Paula Santander Ocaña

1. ¿La dependencia de la Dependencia División de Investigación y Extensión cuenta con políticas de seguridad física para las oficinas, recintos e instalaciones?
2. ¿La dependencia cuenta con políticas para trabajo en áreas seguras?
3. ¿Cada cuánto se realiza mantenimiento a los equipos e infraestructura tecnológica, quienes lo realizan, y que proceso se lleva a cabo?
4. ¿En el momento de cambio o baja de equipo la información de los medios de almacenamiento son eliminados de manera segura, para evitar manipulaciones de la información o recuperación de la misma?
5. ¿En el momento de hacer un retiro de un equipo, este debe contar con la autorización previa del funcionario o el jefe de la dependencia?
6. ¿Existen procedimientos para el manejo y almacenamiento de información para la protección de dicha información contra divulgación no autorizada o uso inadecuado?
7. ¿La División de Investigación y Extensión cuenta con un plan de continuidad del negocio donde incluya requisitos de seguridad de la información?
8. ¿Se identifican los eventos que pueden ocasionar interrupciones a los procesos de la División de Investigación y Extensión y se mide su impacto? ¿Cómo se identifican los eventos?
9. ¿Cuándo sucede una interrupción la dependencia cuenta con un plan para recuperar las operaciones y asegurar la disponibilidad de la información?
10. ¿En los planes de continuidad del negocio se mantiene una única estructura para poder identificar prioridades para pruebas y mantenimiento?
11. ¿Los planes se someten a pruebas y revisión para asegurar su actualización y su eficiencia?