	UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA			
Universidad Francisco de Paula Santander Ocaña - Colombia Vigilada Mineducación	Documento: FORMATO HOJA DE RESUMEN PARA TRABAJO DE GRADO	Código: F-AC-DBL-007	Fecha: 10-04-2012	Revisión: A
	Dependencia: DIVISIÓN DE BIBLIOTECA	Aprobado: SUBDIRECTOR ACADEMICO		Pág.: i(110)

RESUMEN – TRABAJO DE GRADO

AUTORES	**ANYELO JULIAN PAEZ PACHECO, ALBA LUZ SANCHEZ PERILLA**
FACULTAD	**FACULTAD DE INGENIERIAS**
PLAN DE ESTUDIOS	**AUDITORIA DE SISTEMAS**
DIRECTOR	**EDUAR BAYONA IBAÑEZ**
TÍTULO DE LA TESIS	**DIAGNOSTICO DE LA SEGURIDAD DE LA INFORMACIÓN A LA DEPENDENCIA DE BIENESTAR UNIVERSITARIO DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA APLICANDO LA NORMA ISO 27001**

RESUMEN

(70 palabras aproximadamente)

ESTE DOCUMENTO CONTIENE INFORMACIÓN PARA EL DESARROLLO DE UNA AUDITORIA DE SEGURIDAD DE LA INFORMACIÓN APLICANDO LA NORMA ISO 27001, EL CUAL SIRVE COMO GUÍA PARA REALIZAR AUDITORÍAS DE SISTEMAS. LA AUDITORÍA FUE APLICADA A LA DEPENDENCIA DE BIENESTAR UNIVERSITARIO PARA EVALUAR LA SEGURIDAD DE LA INFORMACIÓN, DONDE SE REALIZÓ UN ESTUDIO DE LA NORMA PARA ESCOGER LOS DOMINIOS A APLICAR, SE DIAGNOSTICÓ LA DEPENDENCIA Y SE GENERÓ EL INFORME FINAL DE AUDITORIA.

CARACTERÍSTICAS			
PÁGINAS: 110	PLANOS:	ILUSTRACIONES:	CD-ROM: 1

DIAGNOSTICO DE LA SEGURIDAD DE LA INFORMACIÓN A LA DEPENDENCIA DE BIENESTAR UNIVERSITARIO DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA APLICANDO LA NORMA ISO 27001.

AUTORES:

ALBA LUZ SANCHEZ PERILLA 850231

ANYELO JULIAN PAEZ PACHECO 850223

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

DIVISIÓN DE POSTGRADOS

ESPECIALIZACIÓN EN AUDITORIA DE SISTEMAS

Ocaña, Colombia Agosto de 2018

Contenido

Tablas

Figuras

Capítulo 1.Diagnostico de la Seguridad de la Información a la Dependencia de Bienestar Universitario de la Universidad Francisco de Paula Santander Ocaña Aplicando la Norma ISO 27001.

1.1 Planteamiento del Problema:

En la actualidad las empresas soportan en su actividad económica tecnología, información y comunicación, por más pequeña que esta sea, necesitan un sistema de información y algunas infraestructura informáticas en red, por lo que esto conlleva medida de protección que garanticen el desarrollo, sostenibilidad, confidencialidad, integridad, disponibilidad y usabilidad autorizada de la información, de la actividad del negocio. (Bertolìn, 2008)

> La adecuada gestión de la seguridad de la información es de vital importancia para la supervivencia de una organización (Bertolìn, 2008, p. 2)

Es por eso que la dependencia de Bienestar Universitario de la Universidad Francisco de Paula Santander Ocaña (UFPSO) es una dependencia que se encarga del bienestar de la comunidad universitaria en diferentes actividades como cultura, deportes, psicología, enfermería, entre otros, manejando información importante de sus usuarios para el desarrollo de las mismas, información que puede ser vulnerada por cualquier actividad malintencionada o actividad que origine algún riesgo para la dependencia, tales como ataques de hackers, robo de información, sabotaje, vandalismo, desastres naturales, entre otras.

Por lo que si en algún caso hay pérdida de la información puede afectar la imagen y pérdida de confianza de los usuarios de la Universidad, lo que origina evaluar cómo está su seguridad respecto a la información, que medidas tienen implementadas, y de qué manera reducir riesgos.

1.2 Formulación del problema

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

1.3 Objetivos

1.3.1 Objetivo General:

Diagnosticar la seguridad de la información en la dependencia de bienestar universitario de la Universidad Francisco De Paula Santander Ocaña aplicando la norma ISO 27001.

1.3.2Objetivos Específicos

- Estudiar los dominios de la norma ISO 27001 según la estructura aplicable a la dependencia de Bienestar Universitario.
- Diagnosticar el estado de la seguridad de la información en la dependencia de Bienestar Universitario.
- Identificar los riesgos asociados a la seguridad de la información en la dependencia de Bienestar Universitario.

- Realizar recomendaciones para el aseguramiento de la seguridad de la información en la dependencia de Bienestar Universitario.

1.4 Justificación:

La tecnología se ha convertido hoy en día en un pilar fundamental en toda organización ya que maneja información de su actividad económica, tales como datos de sus usuarios, proveedores, actividad financiera, y demás datos que son relevantes en toda empresa y que debe estar segura de alguna manera, tanto de manera digital como de manera física, lo que surge la necesidad de aplicar medidas de protección, y controles de seguridad de la información que resulta considerablemente más económicos y eficaces si se incorporan en la etapa de especificación, requerimiento y diseño, la hora de definir un sistema de información existe un amplio abanico de definiciones una de ellas es la propuesta por Andreu, Ricart(1991), mencionando lo dicho por otro autor en la cual lo tomo:

> Conjunto formal de procesos que, operando sobre una colección de datos estructurada de acuerdo a las necesidades de la empresa, recopila, elabora y distribuyen selectivamente la información necesaria para la operación de dicha empresa y para las actividades de dirección y control correspondientes, apoyando, al menos en parte, los procesos de toma de decisiones necesarios para desempeñar funciones de negocio de la empresa de acuerdo con su estrategia. (Trasobares).

Tomando en cuenta que la metodología existente para la seguridad de la información la universidad se apoya en la norma ISO 27001 que contiene las herramientas y solución tecnologías que le ayuden a cumplir el objetivo final de la universidad, dándole un nivel más de seguridad a la información que maneja, por tal motivo se pretende realizar un estudio de la norma ISO 27001, revisar si dicha norma se aplica de forma correcta en la dependencia de Bienestar Universitario, y

en caso de encontrar inconsistencias dar las respectivas recomendaciones de mejoramiento para su mejor implementación.

1.5 Delimitaciones

1.5.1 Geográfica:

Este proyecto se desarrollara en las instalaciones de la Universidad Francisco de Paula Santander Ocaña en la dependencia de Bienestar Universitario, vía Acolsure sede algodonal, Ocaña - Norte de Santander.

Se aplicara en la Dependencia de Bienestar Universitario, que consta de 9 oficinas con un total de 13 funcionarios trabajando para la comunidad, distribuidos entre Jefe de Bienestar, secretaria, psicólogas, trabajadora social, coordinador de deportes, enfermera, doctores, y coordinador pastoral juvenil.

1.5.2 Temporal:

Para la realización del diagnóstico de la seguridad de la información se llevara a cabo en un periodo de cuatro (4) meses a partir de la aprobación del anteproyecto, ya que para su realización se requiere de investigación detallada.

Se desarrollara en 4 meses ya que el proyecto se realizara entre dos personas, por lo que las investigaciones que se realicen deben ser completas sobre la Dependencia para saber las

actividades que realiza y como estas se pueden ver comprometidas en sus seguridad, como la aplicabilidad de la auditoria llevan tiempo su desarrollo.

1.5.3 Conceptual:

Para el desarrollo de esta investigación se incluyen conceptos asociados con la norma ISO 27001 tales como seguridad física, comunicaciones, datos, información, controles, entre otros términos que ayudan a la realización del proyecto.

Se basara en la norma ISO 27001 por ser la norma que describe como se debe gestionar la seguridad de la información y puede ser implementado en cualquier tipo de organización, en donde se analiza y luego se procede a ser una gestión de riesgos de los procesos.

1.5.4 Operativa:

Como la investigación se aborda en el paradigma cuantitativo, se tomaran los instrumentos necesarios para la recolección de información que ayuden al desarrollo del proyecto.

Se usara este paradigma ya que se obtendrá datos orientados a la realidad que podrán ser comprobados, orientado a los resultados obtenidos, en donde se obtiene una perspectiva fuera de la dependencia para luego saber el estado de la seguridad de la información.

Capítulo 2. Marco Referencial

2.1 Marco Histórico

"La información se puede definir como el conjunto de datos que, transformados o modificados, tiene un valor para aquellos usuarios que hacen uso de ellos". (UPC, 2004, p. 206).

Durante los últimos años los sistemas de información constituyen uno de los principales ámbitos de estudio en el área de organización de empresas. El entorno donde las compañías desarrollan sus actividades se vuelve cada vez más complejo. La creciente globalización, el proceso de internacionalización de la empresa, el incremento de la competencia en los mercados de bienes y servicios, la rapidez en el desarrollo de las tecnologías de información, el aumento de la incertidumbre en el entorno y la reducción de los ciclos de vida de los productos originan que la información se convierta en un elemento clave para la gestión, así como para la supervivencia y crecimiento de la organización empresarial. Si los recursos básicos analizados hasta ahora eran tierra, trabajo y capital, ahora la información aparece como otro insumo fundamental a valorar en las empresas. (Trasobares).

A la hora de definir un sistema de información existe un amplio abanico de definiciones1. Tal vez la más precisa sea la propuesta por Andreu, Ricart y Valor (1991), en la cual un sistema de información queda definido como:

> Conjunto formal de procesos que, operando sobre una colección de datos estructurada de acuerdo a las necesidades de la empresa, recopila, elabora y distribuyen selectivamente la información necesaria para la operación de dicha empresa y para las actividades de dirección y control correspondientes, apoyando, al menos en parte, los procesos de toma de decisiones necesarios para desempeñar funciones de negocio de la empresa de acuerdo con su estrategia. (Trasobares).

Todo sistema de información utiliza como materia prima los datos, los cuales almacena, procesa y transforma para obtener como resultado final información, la cual será suministrada a los diferentes usuarios del sistema, existiendo además un proceso de retroalimentación "feedback", en la cual se ha de valorar si la información obtenida se adecua a lo esperado (Trasobares).

Junto con los datos, los otros dos componente básicos que constituyen un sistema de información son los usuarios (personal directivo, empleados y en general cualquier agente de la organización empresarial que utilice la información en su puesto de trabajo) y los equipos (informáticos, software, hardware y tecnologías de almacenamiento de la información y de las telecomunicaciones). (Ver figura 1). (Trasobares).

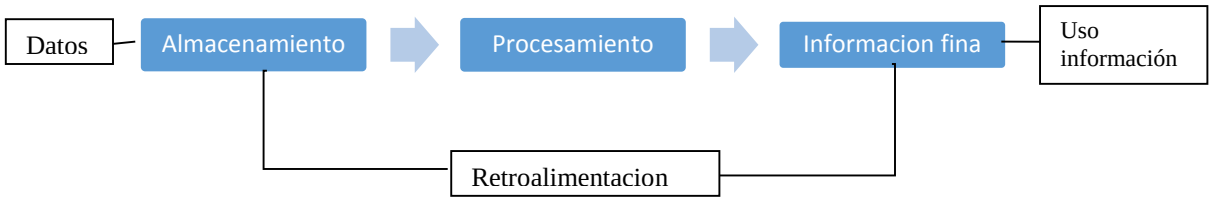


Figura 1. Sistema de información de la organización

En muchas ocasiones existe bastante confusión, pues al referirse a sistemas de información se piensa en un primer momento tanto los ordenadores como en los programas informáticos2. Una empresa puede adquirir nuevos ordenadores, instalar nuevos productos de telecomunicaciones, elaborar una página web, realizar comercio electrónico, pero ello no implica que exista en su organización un sistema de información. Un sistema de información abarca más que el aspecto meramente computacional, pues no sólo hemos de tener en cuenta estas herramientas, sino

también el modo de organizar dichas herramientas y de obtener la información necesaria para el correcto funcionamiento de la empresa. (Trasobares, p.1).

Una de las disciplinas de la ingeniera del software que más impulso está teniendo en los últimos tiempos es aquella que describe, desarrolla y utiliza técnicas software para la construcción de sistemas abiertos y distribuidos. Un ejemplo de esto son los sistemas de información distribuidos**.** (Iribarne, 2001, p. 1).

La disciplina de los sistemas de información distribuidos, como tal, ha empezado a ser reconocida ampliamente desde hace relativamente poco tiempo. Es un término que surge en la década de los 90, cuando los ingenieros, encargados de desarrollar y de mantener los grandes sistemas de información de la empresa, ven la necesidad de escalar y ampliar sus sistemas para dar cobertura ya no solo al personal interno de una sección, de un departamento o de una organización, sino también para dar servicio a otros miembros de la organización ubicados en diferentes localizaciones geográficas, y como no, a otros miembros externos a la organización. (Iribarne, 2001, p. 1).

Los sistemas de información distribuidos |en ocasiones también denominados sistemas informáticos distribuidos- surgen justo en la época donde comienza el \boom de Internet", y con ello, un cambio radical en las metodologías de desarrollo de los sistemas de información. En pocos años se pasa de una mentalidad centralizada, donde prevalecía la confidencialidad y sistemas de información basados en Intranet, a una mentalidad totalmente opuesta, descentralizada y basada en Internet. Evidentemente todo esto se ve influenciado por la caída

progresiva de los equipos hardware y materiales de comunicación, lo cual, como hemos dicho, permitirá que en pocos años surgiera una multitud nueva de tecnología alrededor de una única idea: mantener sistemas de información descentralizados, distribuidos y abiertos, generalmente, si no en su totalidad, una parte, funcionando sobre Web. (Iribarne, 2001, p. 1)

Como vemos, el término Sistema de Información Distribuido surge como confluencia interesada de dos disciplinas elementales. Por un lado la disciplina de los sistemas de información, como idea original de un sistema centralizado en sí, y por otro lado la disciplina de los sistemas distribuidos, como idea original de un sistema descentralizado. La disciplina de los sistemas de información históricamente ha estado relacionada con la disciplina que analiza, diseña, desarrolla, implanta y mantiene el sistema informático de una empresa Esto está relacionado con todos los procesos de ingeniera de software que los profesionales del software utilizan para el desarrollo de sistemas informáticos. (Iribarne, 2001, p. 1).

La disciplina de los sistemas distribuidos históricamente ha estado relacionada con el paradigma de la programación distribuida, como algoritmos distribuidos, modelos para la implementación abstracta de memoria compartida distribuida, sistemas de archivos y sistemas de gestión de bases de datos distribuidos, comunicación y paso de mensajes entre procesos concurrentes, sincronización, seguridad, y tolerancia a fallos, entre otros factores. (Iribarne, 2001, p. 1).

El proceso de desarrollo de sistemas informáticos de empresa ha ido cambiando gradualmente en pocos años para pasar de un modelo centralizado y rígido hacia un modelo descentralizado,

abierto y distribuido. El sistema informático o sistema de información de una empresa |a nivel de recursos software, hardware y humanos, solía estar localizado en un mismo espacio geográfico, en un departamento o una sección de la empresa. Desde aquí, el equipo humano de profesionales, que tradicionalmente estaba compuesto por las categorías de analistas y programadores de sistemas, elaboraba las aplicaciones del sistema de información haciendo uso de conocimientos y prácticas tradicionales del proceso de ingeniería del software. (Iribarne, 2001, p. 1)**.**

A mediados de los años 80 empiezan a converger diversos factores en el mundo de la informática que serían el detonante de un cambio en el proceso de ingeniería de los sistemas de información. Por un lado comienza la explosión de los PCs, que irrumpe con fuerza dentro de la empresa, básicamente en los centros de cálculo. Aunque la mayor parte de la lógica de negocio[1] aun residía en grandes estaciones de trabajo o en mainframes, la masiva presencia de equipos de bajo coste (PCs, comparados con los grandes sistemas) permitirá a los ingenieros desarrollar grandes aplicaciones desglosadas en módulos software que podían estar ubicados en distintos ordenadores, dando lugar ahora a nuevo enfoque en el desarrollo de sistemas de información. (Iribarne, 2001, p. 2)**.**

Inicialmente, estos bloques software funcionaban como elementos de computo independientes dentro del sistema, pero pronto, los ingenieros vieron la necesidad de disponer nuevas técnicas para la comunicación y transferencia de datos entre estos elementos de computo. Precisamente por esta fecha, ajeno a estas necesidades, empezaban a consolidarse fuertes líneas de investigación en computación paralela y programación concurrente, motivada en un principio por la masiva presencia de sistemas operativos tipo Unix en sistemas multiprocesador. (Iribarne, 2001, p. 2).

Estas líneas de investigación en programación paralela y concurrente, junto con las necesidades de comunicación entre procesos en ambientes de cómputo independientes, dieron lugar a primeros esfuerzos en la elaboración de nueva tecnología para la programación distribuida de aplicaciones. Precisamente, uno de los primeros resultados fue el desarrollo de la técnica RPC (Remote Procedure Call), origen de gran parte de la tecnología middleware actual. Esta técnica permite que los desarrolladores de software puedan diseñar sus aplicaciones mediante módulos comunicantes, como si fuesen un conjunto de procesos cooperativos independientes. (Iribarne, 2001, p. 2).

Esta nueva técnica empezó a utilizarse de forma masiva en la empresa para el desarrollo de grandes sistemas de información. Pero esto provocó principalmente dos problemas. Por un lado, se empezó a echar en falta un modelo distribuido estándar que sirviera de guia para los ingenieros en la elaboración de sus aplicaciones distribuidas. Debido a la rápida utilización de la técnica RPC, se empezó a dar forma a todo un entorno de computación distribuida sin la elaboración de un marco teórico que lo sustentase. (Iribarne, 2001, p. 2)**.**

Esto dio lugar a la aparición del primer modelo de distribución en 1994, conocido con el nombre de DCE (Distributed Computation Environment,). Este modelo fue desarrollado por OSF (Open Systems Foundation), una organización formada por IBM, DEC y Hewlett-Packard. El modelo establecía las pautas y normas que los ingenieros de sistemas de información debían seguir para desarrollar sus sistemas. Entre otras características, el modelo DCE destaco por ser un modelo cliente/servidor basado en el lenguaje C y que inicialmente funcionaba para

plataformas Unix. Posteriormente el modelo se extendió para soportar diversos sistemas operativos, como VMS, Windows y OS/2, entre otros. (Iribarne, 2001, p. 2)**.**

Por otro lado, esta nueva mentalidad de construir aplicaciones divididas en partes comunicantes y residentes en distintos ambientes de computo fue un gran paso en el campo programación distribuida. Evidentemente, las antiguas aplicaciones del sistema no dejaron de funcionar, pero los ingenieros vieron pronto la necesidad de integrar las partes existentes del sistema con las nuevas diseñadas. (Iribarne, 2001, p. 2).

Esto dio paso a la aparición de nuevos conceptos, como legacy systems o sistemas heredados, que hace referencia a la integración de partes software existente con las del sistema actual. Otro concepto es el de wrapper, que son porciones de códigos especialmente diseñados para encapsular y dar funcionalidad a otras partes del sistema ya existentes; o el concepto glue, que son porciones de código cuyo efecto es similar al de un \pegamento" y que sirve para unir distintas partes envueltas y funcionando con wrappers. (Iribarne, 2001, p. 2)**.**

Pero el concepto más importante que ha cambiado y sigue cambiando los procesos de ingeniera y reingeniería, es el concepto de componente. Inicialmente este concepto surge ante la necesidad de reutilizar partes o módulos software existente que podían ser utilizadas para la generación de nuevas extensiones de las aplicaciones, o incluso para la generación de completas aplicaciones. Pero esto suponía un gran esfuerzo, pues había que localizar estas partes reutilizables y almacenarlas en repositorios o librerías de código especiales que más tarde podían ser consultadas en fase de diseño. (Iribarne, 2001, p. 3).

Este es uno de los puntos clave más importantes dentro de los Sistemas de Información distribuidos (SID), pues empiezan a diferenciarse dos estilos de desarrollo de software, utilizados después en los procesos de ingeniería para la construcción de SID|. Por un lado está el desarrollo de software basado en reutilización, donde las aplicaciones se construyen a partir de otras partes software ya existente y accesible en repositorios conocidos. Por otro lado está el desarrollo de software para reutilización, donde se ponen en práctica procesos de ingeniería para la elaboración de eficientes partes software que luego pueden ser utilizadas para la construcción de aplicaciones (en el otro estilo de desarrollo de software). A estas partes software se las conoce como componentes software, y han dado lugar a los paradigmas de programación de componentes top-down (para reutilizar) y bottom-up (basado en reutilización). (Iribarne, 2001, p.3).

Pero el uso generalizado de los componentes en procesos de ingeniería de software realmente empieza a tomar presencia y sentido con la aparición de nuevos modelos de distribución, como CORBA, DCOM o EJB, modelos que actualmente se están utilizando para el desarrollo de aplicaciones distribuidas. Su predecesor, el modelo DCE, empieza a ser visto por los ingenieros de sistemas como un modelo difícil y costoso de llevar a la práctica. (Iribarne, 2001, p. 3).

Por este motivo, la Object Management Organization (OMG) empezó a desarrollar un modelo para la distribución y localización dinámica de objetos en tiempo de ejecución, el modelo CORBA (Common Object Request Broker Architecture). Por otro lado, Sun Microsystems (tecnologia Unix) y Microsoft (tecnologia Windows) elaboran modelos, conocidos como EJB (Enterprise Java Beans) y DCOM (Distributed Component Object Model), respectivamente. (Iribarne, 2001, p. 3).

Sin embargo, la presencia de distintos modelos de objetos distribuidos dentro de la empresa, cada vez más influenciada por intereses de la industria |intereses de soluciones Sun frente a intereses de soluciones Microsoft|, y la fuerte evolución de nuevas tecnologías (XML, SOAP, Servlets, seguridad, entre otros), está haciendo que los ingenieros de sistemas tengan que hacer grandes procesos de ingeniería de requisitos para seleccionar aquellas tecnologías adecuadas para el desarrollo de sus sistemas. Incluso, en la mayoría de los casos, los ingenieros se ven obligados a utilizar e incorporar múltiples métodos y técnicas para dar soporte a distintos clientes |software y humanos, del sistema de información. (Iribarne, 2001, p. 3)**.**

Por tanto, los grandes sistemas de información de hoy día están basados en modelos cliente/servidor con arquitecturas multicapa y que hacen uso de una gran variedad de tecnologías. La tendencia actual, es que los sistemas de información de la empresa estén distribuidos y localizados en distintos lugares geográficos, comunicándose sus partes con modelos distribuidos CORBA, EJB y/o DCOM, haciendo uso de normas y técnicas de seguridad importantes, utilizando nuevas técnicas como XML para la representación intermedia de información entre componentes software, o SOAP para la localización y activación automática de servicios web, entre otras muchas nuevas tecnología. Esto _ultimo ha sido motivo para la consolidación del concepto abierto, que se utiliza cuando se habla de sistemas de información distribuidos y abiertos. (Iribarne, 2001, p. 3)**.**

El concepto abierto significa que el sistema de información distribuido debe ser heterogéneo y estar preparado en todo momento para sufrir cualquier modificación (proceso de mantenimiento

y actualización) sin que esto altere el funcionamiento normal de ninguna parte del sistema. Pero esto está dando paso a la necesidad real de estándares y sobre todo de una meta modelo de computación distribuida global que abarque cualquier modelo distribuido. (Iribarne, 2001, p. 4).

La tendencia en los procesos de ingeniería del software para el desarrollo de sistemas de información distribuidos, es elaborar sistemas de información cooperativos y colaborativos, compuesto por subsistemas, componentes y objetos especializados y coordinados para ofrecer servicios. En este sentido, están empezando a distinguirse distintas subdisciplinas de la ingeniería conocidas como \ingenierías basadas" o \ingenierías orientadas", como por ejemplo:

- Ingeniería del software basada en componentes,
- Ingeniería del software basada en aspectos,
- Ingeniería del conocimiento,
- Ingeniería de requisitos, entre otros. (Iribarne, 2001, p. 4)**.**

Esto está obligando a la necesidad de disponer nuevas categorías de profesionales especializados en estas ingeniera de la informática. Actualmente, los profesionales adquieren estos conocimientos desde cursos de formación internos que se imparten en la propia empresa o desde masters impartidos por organizaciones que se dedican exclusivamente al desarrollo y formación en nuevas tecnología. No es extraño, por tanto, que en pocos años podamos ofertar en la Universidad distintas ingeniera de informática, ante la fuerte demanda para los próximos años de estos profesionales desde las empresas. (Iribarne, 2001, p. 4).

Evolución de los sistemas de información

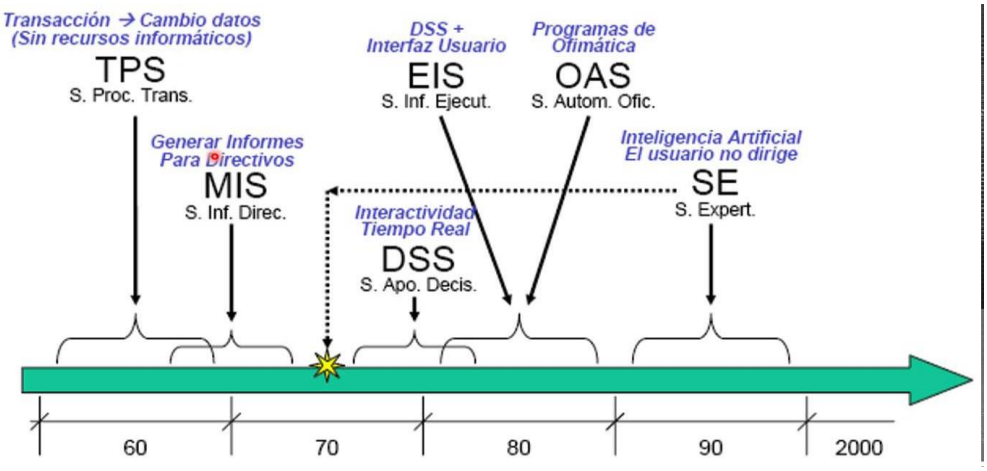


Figura 2. Evolución de los sistemas de información
Fuente**:** google.com

En la década de los setenta, Richard Nolan, un conocido autor y profesor de la Escuela de Negocios de Harvard, desarrolló una teoría que impactó el proceso de planeación de los recursos y las actividades de la informática.

Según Nolan, la función de la Informática en las organizaciones evoluciona a través de ciertas etapas de crecimiento, las cuales se explican a continuación: (Laudon & Laudon, 1996).

Etapa de inicio. Características más relevantes:

Comienza con la adquisición de la primera computadora.

- Se implantan nóminas o contabilidad.
- Sistemas depende de contabilidad.
- No hay preparación formal en el área de computación.
- Resistencia al cambio para aplicar nuevos sistemas. (Laudon & Laudon, 1996).

Etapa de contagio o expansión. Los aspectos sobresalientes que permiten diagnosticar rápido que una empresa se encuentra en esta etapa son:

- Implantación exitosa
- Se aplica en otras funciones de la empresa.
- Se realiza de manera desordenada y sin control.
- Especialista en el área de sistemas.
- Los gastos empiezan a crecer. (Laudon & Laudon, 1996).

Etapa de control o formalización. Para identificar a una empresa que transita por esta etapa es necesario considerar los siguientes elementos:

- Controlar el uso de recursos computacionales.
- Orientados a facilitar el control de las operaciones.
- El depto. de Sistemas tiene una posición Gerencial.
- Se orienta al control administrativo y la justificación económica.
- Desarrollo de estándares de trabajo.
- Se integra al personal en el depto. de Sistemas. (Laudon & Laudon, 1996).

Etapa de integración. Las características de esta etapa son las siguientes:

- La integración de los datos y de los sistemas surge como un resultado directo de la centralización del departamento de sistemas bajo una sola estructura administrativa.

- Las nuevas tecnologías relacionadas con base de datos, sistemas administradores de bases de datos y lenguajes de cuarta generación, hicieron posible la integración.
- El costo del equipo y del software disminuyó por lo cual estuvo al alcance de más usuarios.
- Los usuarios y el departamento de sistema iniciaron el desarrollo de nuevos sistemas, reemplazando los sistemas antiguos, en beneficio de la organización. (Laudon & Laudon, 1996).

Etapa de administración de datos. Entre las características que destacan en esta etapa están las siguientes:

- El departamento de Sistemas de Información reconoce que la información es un recurso muy valioso que debe estar accesible para todos los usuarios.
- Para poder cumplir con lo anterior resulta necesario administrar los datos en forma apropiada, es decir, almacenarlos y mantenerlos en forma adecuada para que los usuarios puedan utilizar y compartir este recurso.
- El usuario de la información adquiere la responsabilidad de la integridad de la misma y debe manejar niveles de acceso diferentes. (Laudon & Laudon, 1996).

Etapa de madurez. Entre los aspectos sobresalientes que indican que una empresa se encuentra en esta etapa, se incluyen los siguientes:

- Informática de la organización definida.
- Desarrollo de sistemas de manufactura.
- Aplicación de tecnología en la base de datos.

- Se perfeccionan los controles implantados.
- Planeación de los recursos de cómputo.
- Buena comunicación con la dirección general y los usuarios de la organización. (Laudon & Laudon, 1996).

Otra clasificación, según el entorno de aplicación

Entorno transaccional: Los sistemas de procesamiento de transacciones están formados por hardware informático y software que aloja una aplicación orientada a intercambios que ejecutan las transacciones habituales necesarias para realizar operaciones comerciales. Entre los ejemplos se incluyen sistemas que administran entradas de órdenes de ventas, reservas de billetes de avión, nóminas, registros de empleados, fabricación y transporte. (Laudon & Laudon, 1996).

Entorno decisional: Este es el entorno en el que tiene lugar la toma de decisiones; en una empresa, las decisiones se toman a todos los niveles y en todas las áreas (otra cosa es si esas decisiones son estructuradas o no), por lo que todos los SI de la organización deben estar preparados para asistir en esta tarea, aunque típicamente, son los DSS los que se encargan de esta función. Si el único SI de una compañía preparado para ayudar a la toma de decisiones es el DSS, éste debe estar adaptado a todos los niveles jerárquicos de la empresa. (Laudon & Laudon, 1996).

2.1.1 Antecedentes.

Sistema de información académica SIA: La definición de base de datos del sistema de información académico de la Universidad Francisco de Paula Santander (SIA) tuvo en cuenta aspectos de mucha importancia que influyeron directamente en el diseño final de la misma. (Cuesta & Garcia, 2002, p.33).

En el análisis hecho durante la primera etapa del proyecto, que se realizó en la Universidad Francisco de paula Santander Cúcuta, se estudió la influencia que podía tener el nuevo Sistema de Información Académica y la aplicación de la ley 30 del 28 de Diciembre de 1992, por la cual se reglamentan el servicio público de la educación superior en Colombia. La conclusión fue precisa en el sentido de que la universidad se vio en la necesidad de replantear sus políticas académicas y por lo tanto su estructura orgánica. (Cuesta & Garcia, 2002, p.33).

Como consecuencia de lo anterior, las autoridades académicas de la Universidad vieron en el proceso de departamentalización, una forma efectiva de mejorar las condiciones y estrategias académicas de la Universidad, la cual venía funcionando hasta este momento bajo la estructura de direcciones de escuela, como la unidad académica básica. (Cuesta & Garcia, 2002, p.33).

La departamentalización llevo consigo cambios en todo el orden del proceso académico. Por ejemplo, las asignaturas son agrupadas de acuerdo a un campo común de la ciencia. Por ello la administración del personal docente y de las asignaturas es responsabilidad de las direcciones de departamentos y no de las direcciones de escuela como anteriormente ocurría. Por lo anterior,

este fue uno de los aspectos más relevantes en el diseño de la base de datos del Sistema de Información Académico de la Universidad Francisco de Paula Santander (SIA). (Cuesta & Garcia, 2002, p.33).

¿Qué es el SIA? El Sistema de Información Académico SIA de la Universidad Francisco de Paula Santander es una aplicación elaborada para facilitar la administración de los diferentes procesos académicos que se llevan a cabo en la universidad. (Cuesta & Garcia, 2002, p.35).

La implementación del SIA en el proceso académico de la Universidad Francisco de Paula Santander seccional Ocaña, tiene como propósitos específicos:

- Alcanzar altos niveles de eficiencia y confiabilidad durante la ejecución de los procesos que conforman el sistema académico de la universidad.

Garantiza el correcto y oportuno mantenimiento, tanto cualitativa como cuantitativamente, de la información almacenada en la base de datos utilizado en el Sistema de Información Académico en mención. (Cuesta & Garcia, 2002, p.35).

Estructura del software: el software que compone el Sistema de Información Académico SIA de la Universidad Francisco de Paula Santander, está distribuido en seis módulos, los cuales contiene los programas encargados de llevar a cabo los diferentes procesos académicos de la universidad. (Cuesta & Garcia, 2002, p.36).

Cada módulo se encuentra directamente relacionado con algunas de las dependencias de la universidad que prestan sus servicios directamente al estudiantado o con algún proceso con el que el estudiante interactúa directamente. (Cuesta & Garcia, 2002, p.36).

El sistema de información académico SIA consta de los siguientes módulos:

- Matricula.
- Inclusiones y cancelaciones.
- Departamentos.
- Plan de estudios.
- Registro y control.
- Centro de cómputo. (Cuesta & Garcia, 2002, p.36).

2.2 Estado del Arte

Es importante mencionar los proyectos de grado que se han relacionado a través del desarrollo del Sistema de Información Académico SIA. Inicialmente se realizó el proyecto titulado Sistema de Información Académica SIA de la Universidad Francisco de Paula Santander, que tuvo su diseño e implementación utilizando el sistema manejador de base de datos **FoxPro** versión 2.5 para Windows 3.1 y que fue remplazado a la adquisición del **RDBMS ORACLE**, con la cual la universidad desarrollo e implemento el Sistema de Información Académico SIA que actualmente se utiliza en todos los procesos académicos. (Cuesta & Garcia, 2002, p.34).

Luego, se realizó el proyecto titulado Conversión de Datos de la División de Educación Abierta y a Distancia al Sistema de Información Académica SIA, el cual permitió analizar el comportamiento de los procesos académicos modalidad presencial y a distancia, logrando de esta forma la gestión académica de los estudiantes del programa a distancia de la Universidad Francisco de Paula Santander. (Cuesta & Garcia, 2002, p.34).

Posteriormente se han desarrollado dos proyectos más: el primero titulado Diseño e Implementación de un CGI para el proceso de matrícula académica de la Universidad Francisco de Paula Santander, el cual permite a los estudiantes a través de una página HTML realizar el proceso de matrícula académica; y el segundo, titulado Documentación del Sistema de Información Académica SIA y del Sistema de Información Financiera SIF de la Universidad Francisco de Paula Santander, el cual muestra los manuales de usuario y el sistema de ayudas interactivas de cada uno de los módulos del Sistema de Información Académico SIA y del sistema de Información Financiera SIF. (Cuesta & Garcia, 2002, p.34).

2.3 Marco Conceptual

Sistema de información: Un sistema de información es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad u objetivo. Dichos elementos formarán parte de alguna de las siguientes categorías:

- Personas
- Datos
- Actividades o técnicas de trabajo
- Recursos materiales en general (generalmente recursos informáticos y de comunicación, aunque no necesariamente).

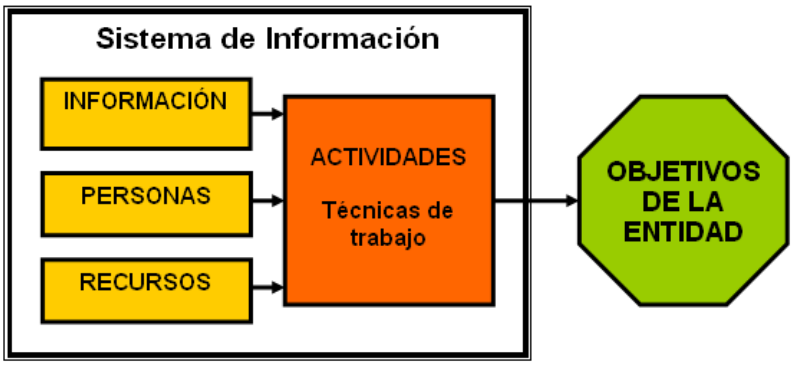


Figura 3. Sistema de información.
Fuente. (Laudon & Laudon, 1996).

Según el autor Laudon, profesor de Administración de Empresas, un sistema de información es un organismo que recolecta, procesa, almacena y distribuye información. Son indispensables para ayudar a los gerentes a mantener ordenada su compañía, a analizar todo lo que por ella pasa y a crear nuevos productos que coloquen en un buen lugar a la organización. Esta definición es una de las únicas que manifiesta la exigencia de que un sistema de información tenga

componentes, aunque no especifica cuáles deban ser, posiblemente porque intenta englobar todas las posibles variantes de este concepto. Cabe resaltar que el concepto de sistema de información suele ser utilizado como sinónimo de sistema de información informático, aunque no son lo mismo. Este último pertenece al campo de estudio de la tecnología de la información y puede formar parte de un sistema de información como recurso material. De todas formas, se dice que los sistemas de información tratan el desarrollo y la administración de la infraestructura tecnológica de una organización.

Hay tres actividades en un sistema de información que producen la información que esas organizaciones necesitan para tomar decisiones, controlar operaciones, analizar problemas y crear nuevos productos o servicios. Estas actividades son:

- **Entrada:** captura o recolecta datos en bruto tanto del interior de la organización como de su entorno externo.
- **Procesamiento:** convierte esa entrada de datos en una forma más significativa.
- **Salida:** transfiere la información procesada a la gente que la usará o a las actividades para las que se utilizará. (Laudon & Laudon, 1996).

Los sistemas de información también requieren retroalimentación, que es la salida que se devuelve al personal adecuado de la organización para ayudarle a evaluar o corregir la etapa de entrada.

Las actividades son las siguientes:

Figura 4. Transformación de datos.
Fuente. (Laudon & Laudon, 1996)

a) **Entrada de datos:** Proceso mediante el cual se captura y prepara datos para su posterior procesamiento. Las entradas pueden ser manuales o automáticas. Las manuales se realizan por el operador o el usuario, y las automáticas surgen de otros sistemas. (Laudon & Laudon, 1996).

b) Almacenamiento de datos: Proceso mediante el cual el sistema almacena de manera organizada los datos e información para su uso posterior.

Para hacer fácil su recuperación, los datos almacenados se organizan en:

- Campo: agrupación de caracteres que identifican a un sujeto, lugar u objeto, por ejemplo: nombre de un empleado.

- Registro: conjunto de campos interrelacionados, por ejemplo el registro nómina de un trabajador podría componerse por el nombre, ítem, departamento y sueldo.
- Archivo: conjunto de registros interrelacionados, por ejemplo el archivo planilla del mes enero del año 2001 podría estar compuesto por registros de la nómina de todos los trabajadores durante el mes de enero de 2001.
- Base de datos: conjunto integrado de registros interrelacionados. Por ejemplo, la base de datos de empleados de una organización, podría incluir archivos de las planillas de todos los meses, junto con otros archivos relacionados a registros de evaluación de desempeño de cada trabajador, asistencia a capacitaciones, etc. (Laudon & Laudon, 1996).

c) **Procesamiento de datos**: Es la capacidad de efectuar operaciones con los datos guardados en las unidades de memoria. Durante este procesamiento se evidencia lo siguiente:

1. Aumenta, manipula y organiza la forma de los datos.
2. Analiza y evalúa su contenido.
3. Selecciona la información para ser usada en la toma de decisiones, y constituye un componente clave en el sistema de información gerencial. (Laudon & Laudon, 1996).

d) Salida de información: Actividad que permite transmitir información útil y valiosa a los usuarios finales.

Además un sistema de información debe tener control del desempeño del sistema, es decir debe generar retroalimentación sobre las actividades de entrada, procesamiento, almacenamiento y salida de información. Esta retroalimentación debe evaluarse para determinar si el sistema cumple con los estándares de desempeño establecidos. (Laudon & Laudon, 1996).

Norma ISO 27001: ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2. (Advisera, 2012)

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001. (Advisera, 2012)

ISO 27001 se ha convertido en la principal norma a nivel mundial para la seguridad de la información y muchas empresas han certificado su cumplimiento. (Advisera, 2012)**.**

¿Cómo funciona la ISO 27001? El eje central de ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto lo hace investigando cuáles son los potenciales problemas que podrían afectar la información (es decir, la evaluación de riesgos) y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan (es decir, mitigación o tratamiento del riesgo). (Advisera, 2012)

Por lo tanto, la filosofía principal de la norma ISO 27001 se basa en la gestión de riesgos: investigar dónde están los riesgos y luego tratarlos sistemáticamente.

Figura 5. Estructura de ISO 27001.
Fuente: (Advisera, 2012).

Las medidas de seguridad (o controles) que se van a implementar se presentan, por lo general, bajo la forma de políticas, procedimientos e implementación técnica (por ejemplo, software y equipos). Sin embargo, en la mayoría de los casos, las empresas ya tienen todo el hardware y software pero utilizan de una forma no segura; por lo tanto, la mayor parte de la implementación de ISO 27001 estará relacionada con determinar las reglas organizacionales (por ejemplo, redacción de documentos) necesarias para prevenir violaciones de la seguridad.

Como este tipo de implementación demandará la gestión de múltiples políticas, procedimientos, personas, bienes, etc., ISO 27001 ha detallado cómo amalgamar todos estos elementos dentro del sistema de gestión de seguridad de la información (SGSI).

Por eso, la gestión de la seguridad de la información no se acota solamente a la seguridad de TI (por ejemplo, cortafuegos, anti-virus, etc.), sino que también tiene que ver con la gestión de procesos, de los recursos humanos, con la protección jurídica, la protección física, etc

2.4 Marco Legal

Ley 603 de 2000. Por medio de la cual se regula el tipo de software que usan las empresas, con el fin de proteger la propiedad intelectual y evitar el incremento de la piratería en el país. (Colombia, 2000)

Ley 1581 de 2012 y Decreto 1377 de 2013. La cual trata 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. (Bogota, 2013).

Ley 1273 Del 2009. El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 “Por medio del 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". (Ministerio de las TIC, 2009)Dicha ley decreta: (Colombia, 2009).

CAPITULO I: De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos:

Artículo 269A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático. (Colombia, 2009).

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático. (Colombia, 2009).

Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático. (Colombia, 2009).

Artículo 269D: Daño informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos. (Colombia, 2009).

Artículo 269E: Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos. (Colombia, 2009).

Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes. (Colombia, 2009).

Artículo 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes. (Colombia, 2009).

CAPITULO II: De los atentados informáticos y otras infracciones.

Artículo 269I: Hurto por medios informáticos y semejantes. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante. (Colombia, 2009).

Artículo 269J: Transferencia no consentida de Activos. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no 38 consentida de cualquier activo en perjuicio de un tercero. (Colombia, 2009).

Capítulo 3. Diseño Metodológico

3.1 Tipo de Investigación

En este proyecto se utilizará la investigación descriptiva que para Tamayo y Tamayo (2009) la define como la descripción, registro, análisis e interpretación de la naturaleza, y composición de un proceso o fenómenos, e investigación de diagnóstico, tipo cuantitativa, teniendo en cuenta lo planteado por Sampieri, " Es la representación de un conjunto de procesos secuenciales y probatorios", su objetivo consiste en conocer las situaciones, donde involucre la información que maneja bienestar universitario, a través de la descripción exacta de las actividades, objetos, procesos y las personas. Los investigadores no son solo tabuladores, sino que recogen los datos sobre la base de las herramientas a utilizar donde se encuentran, exponen y resume la información de manera cuidadosa y luego se analizan minuciosamente los resultados, a fin de extraer generalizaciones significativas que contribuyan al conocimiento y hallazgos de la aplicabilidad de la norma ISO 27001

3.2 Población

La población objeto de estudio que se tendrá en cuenta para la realización de esta investigación está conformado por todo el personal que labora en el Área de Bienestar Universitario, los cuales no superan los 13 profesionales, por lo tanto, la población es igual a la muestra. La población está dividida por Jefe de Bienestar 1, secretaria 1, psicólogos 3, oficina egresados 1, enfermería 2, trabajo social 1, médicos 2, asesoría espiritual 1, deportes 1.

3.3 Técnicas e Instrumentos de Recolección de Información

Entre las metodologías internas se tiene la observación, estudio de los archivos permanentes, entrevistas, listas de chequeo, cuestionarios, herramientas de evaluación y la realización de pruebas sustantivas.

Capítulo 4. Administración del Proyecto

4.1 Recursos

4.1.1 Proponentes SANCHEZ PERILLA, Alba Luz, y, PAEZ PACHECO, Anyelo Julián. Estudiantes de la Especialización en Auditoría de Sistemas de la Universidad Francisco de Paula Santander Ocaña.

4.1.2 Director BAYONA IBAÑEZ, Eduar. Magister en práctica docente.

4.2 Recursos Institucionales

Los recursos de carácter físico e institucional para el desarrollo del proyecto son: área de Bienestar Universitario de la Universidad Francisco de Paula Santander Ocaña, el servicio de biblioteca de la Universidad Francisco de Paula Santander Ocaña.

4.3 Recursos Financieros

4.3.1 Ingresos.

Los ingresos contemplados para la realización del proyecto son de $3'000.000 aportados por los autores del mismo.

4.3.2 Egresos.

Los gastos estimados para el desarrollo de la auditoria es de 3.000.000 distribuidos en la tabla 2 donde se pagaran los gastos al director del proyecto por las asesorías, como a el equipo auditor que se encargara de aplicar la auditoria y la tabla 3 se muestran los gastos varios que puede tener el proyecto.

Tabla 1 *Costos profesionales*

Responsable	Función	Valor por hora	Horas	Total
Eduar Bayona Ibañez	Director del Proyecto	12.000	14	168.000
Anyelo Julián Páez	Autor del Proyecto	8.000	60	480.000
Alba Luz Sánchez	Autor del Proyecto	8.000	60	480.000
			Total	1.128.000

Fuente: Autores del Proyecto

Tabla 2 *Gastos varios*

Concepto	Valor
Fotocopia e impresiones	350.000
Uso de computadores	200.000
Papelería	150.000
Transporte	500.000
Servicio de internet	200.000
Otros	472.000
Total	1.872.000

Fuente: Autores del Proyecto

Capítulo 5. Resultados

5.1 OBE1: Estudiar los dominios de la norma ISO 27001 según la estructura aplicable a la dependencia de Bienestar Universitario

Para la aplicación de la auditoria, primero se procedió a realizar un estudio de la norma ISO 27001 con todos sus dominios, en donde se analizó cada uno de estos dominios y se compararon con la actividad del negocio de la Dependencia de Bienestar Universitario, donde luego de haber hecho la comparación varios de estos dominios se excluyeron de la auditoria pues no pertenecían a la actividad del negocio de la dependencia (Ver Apéndice H).

Los dominios que se aplicaron en la auditoria fueron el A.9, A.10, A.11, A.13, A.14 especificados en la tabla 3, excluyendo los subdominios o controles que no se trabajaron.

Tabla 3. *Dominios aplicados*

Dominio	Descripción
A.9	SEGURIDAD FÍSICA Y DEL ENTORNO
A.10	GESTIÓN DE COMUNICACIONES Y OPERACIONES
A.11	CONTROL DE ACCESO
A.13	GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN
A.14	GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

Fuente: Autores del Proyecto

5.2 OBE2: Diagnosticar el estado de la seguridad de la información en la dependencia de Bienestar Universitario

Para realizar el análisis de los resultados obtenidos durante las encuestas y listas de chequeo se usara la tabla 4 de rangos de aprobación, para medir los porcentajes obtenidos y tener una mejor lectura.

Tabla 4 *Rangos de aprobación*

Rangos de aprobación		
Porcentaje	Aprobación	Índice de mejora
0% a 20%	Muy malo	Muy Alto
21% a 40%	Malo	Alto
41% a 60%	Regular	Medio
61% a 80%	Bueno	Bajo
81% a 90%	Muy Bueno	Muy bajo
91% a 100%	Excelente	N/A

Fuente: Autores del Proyecto

5.2.1 Encuestas

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 Bienestar para la evaluar la Seguridad de la Información, los funcionarios que fueron encuestados fueron.

Secretaria
Psicología
Enfermería
Trabajo Social
Coordinación de Bienestar
Oficina de Egresados
Médico General
Asesoría espiritual
Coordinación de deportes

Se tiene en cuenta que en las oficinas existen más equipos pero solo se revisaron los equipos y opinión de los funcionarios encargados de la oficina y se revisaron los equipos principales, la encuesta arrojo los siguientes resultados que se muestran a continuación:

En la primera pregunta la dependencia de bienestar maneja los módulos:

SID (Sistema de información documental), módulo de información de estudiantes, becas trabajo, monitorias, liquidaciones, módulo de sicología, módulo de enfermería, módulo de trabajo social, planes de estudio, módulo de egresados, módulo de medicina, módulo de asesoría espiritual, SIAA, SID, inclusión de electivas, módulo de bienestar universitario,

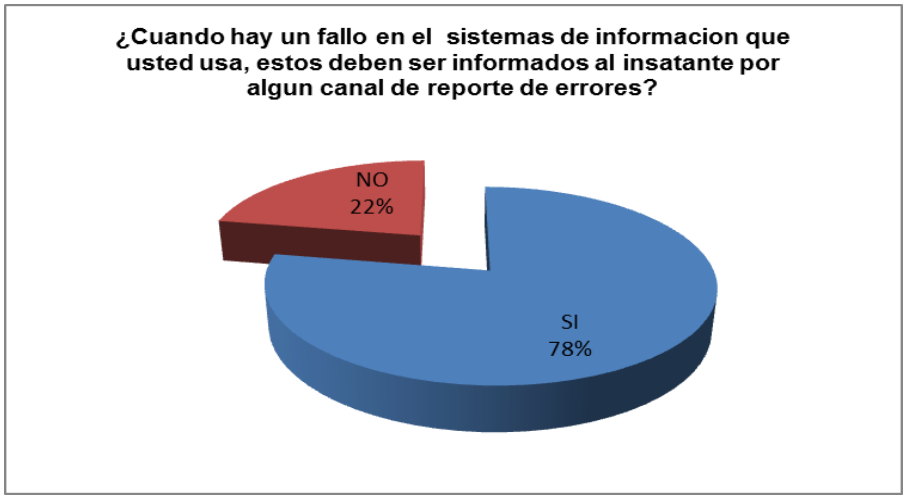


Figura 6. Porcentaje de Información sobre fallos en el sistema
Fuente: Autores del Proyecto

Del resultado obtenido de la pregunta se puede observar que de todos los encuestados el 78% informan casi de manera inmediata cuando se presenta algún inconveniente en los módulos o sistemas de información que ello usan, obteniendo un resultado de bueno obtenido de la tabla 4 en aprobación con un índice bajo por mejorar.

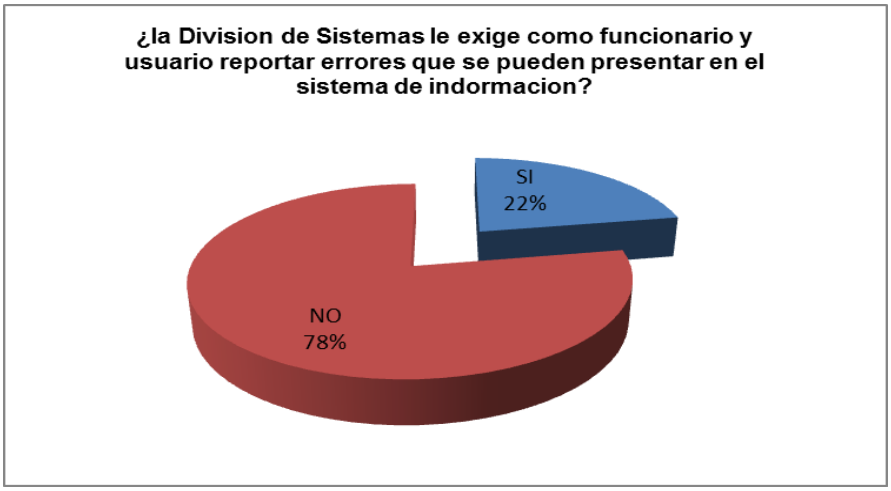


Figura 7. Porcentaje de reporte de errores
Fuente: Autores del Proyecto

Del resultado de la pregunta se observa que el 22% de los encuestados fueron capacitados o la división de sistemas les exige como usuarios de los módulos o sistemas de información informar

de fallos en los mismos, lo que muestra un resultado de malo en aprobación con un índice alto por mejorar.

Figura 8. Porcentaje para un procedimiento de reportes de errores
Fuente: Autores del Proyecto

De la gráfica se observa que el 56% de los encuestados saben que procedimiento deben seguir para hacer un reporte de errores que se pueda presentar en sus módulos, obteniendo un resultado de aprobación de Regular con un índice medio por mejorar.

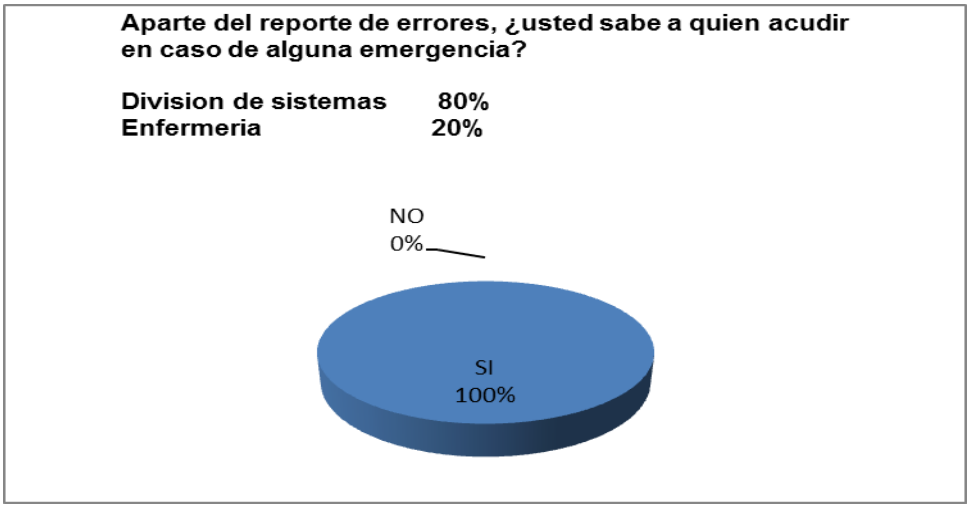


Figura 9. Porcentaje, a quien acude en caso de emergencia
Fuente: Autores del Proyecto

De la gráfica se puede ver que todos 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, obteniendo un resultado de aprobación de excelente.

Figura 10. Porcentaje, solicitud de usuario
Fuente: Autores del Proyecto

De la pregunta observamos que todos los funcionarios saben que procedimiento deben llevar a cabo para solicitar un usuario para alguno modulo que necesiten usar, con un resultado de aprobación de excelente.

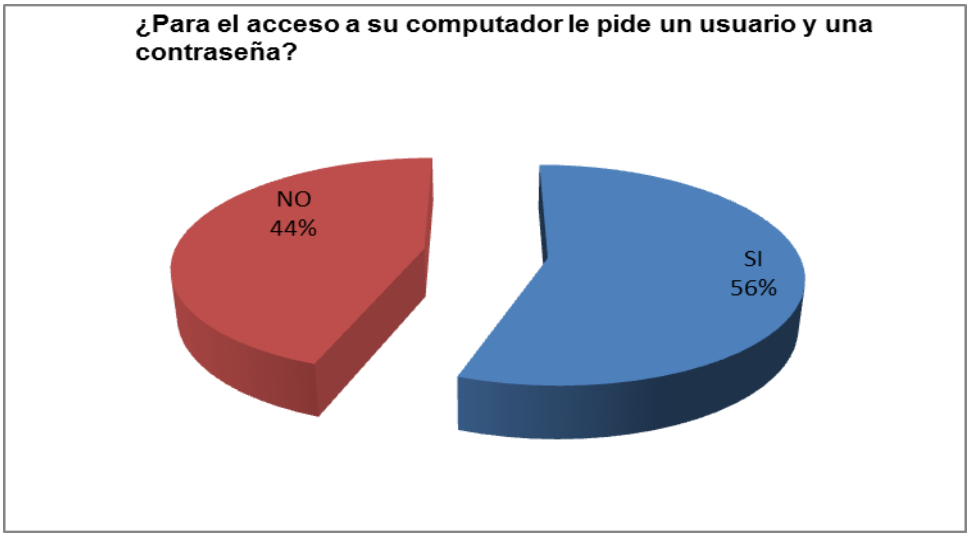


Figura 11. Porcentaje de usuario y contraseña
Fuente: Autores del Proyecto

De la gráfica se puede observar que el 56% de los funcionarios de la dependencia tienen un usuario y una contraseña establecidos para acceder al computador, con un resultado de aprobación de regular y un índice de mejora medio.

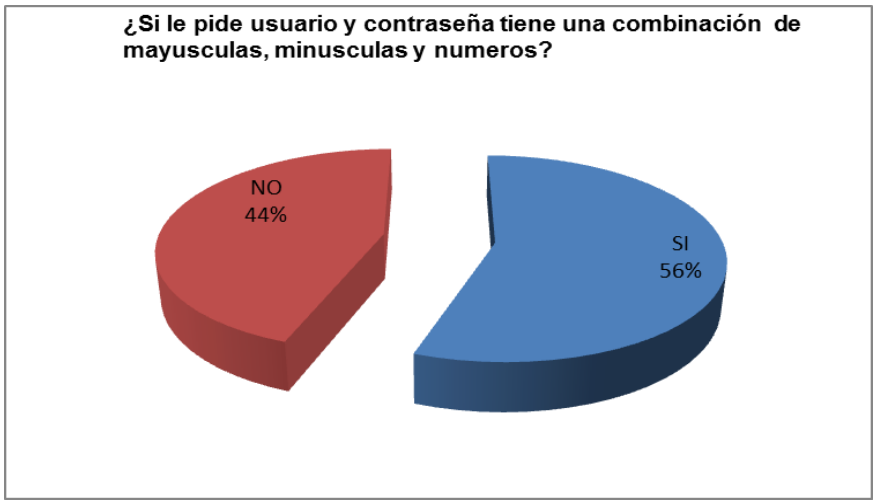


Figura 12. Porcentaje, Contraseñas
Fuente: Autores del Proyecto

Se puede observar que el 56% 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.

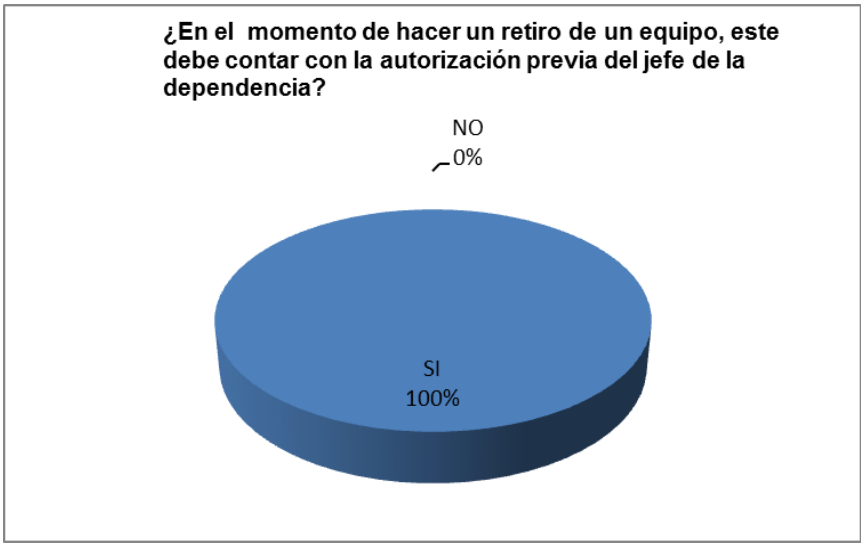


Figura 13. Porcentaje, de autorización de retiro de equipo
Fuente: Autores del Proyecto

Del resultado de la pregunta se aprecia el 100% 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, con un resultado de aprobación de excelente.

5.2.2 Listas de chequeo

A.9 Seguridad física y del entorno

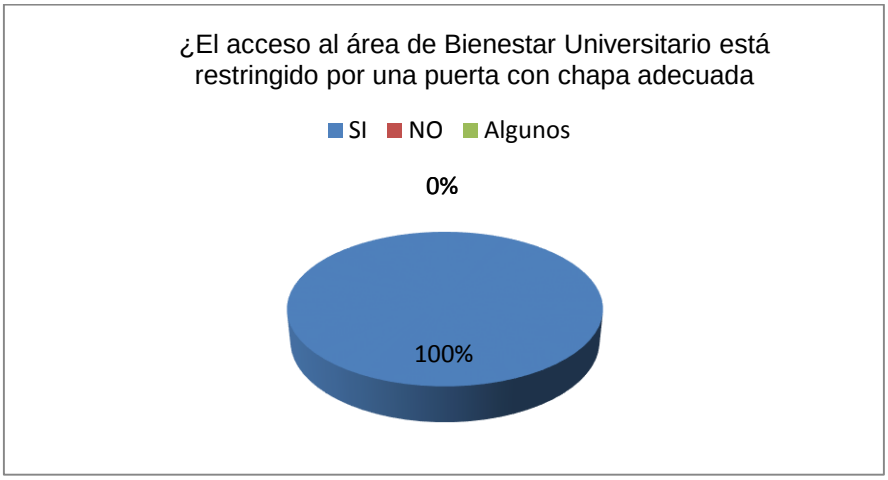


Figura 14. Porcentaje, acceso a la dependencia
Fuente: Autores del Proyecto

Las 2 entradas de la dependencia cuentan con las medidas de seguridad para mantener segura las instalaciones.

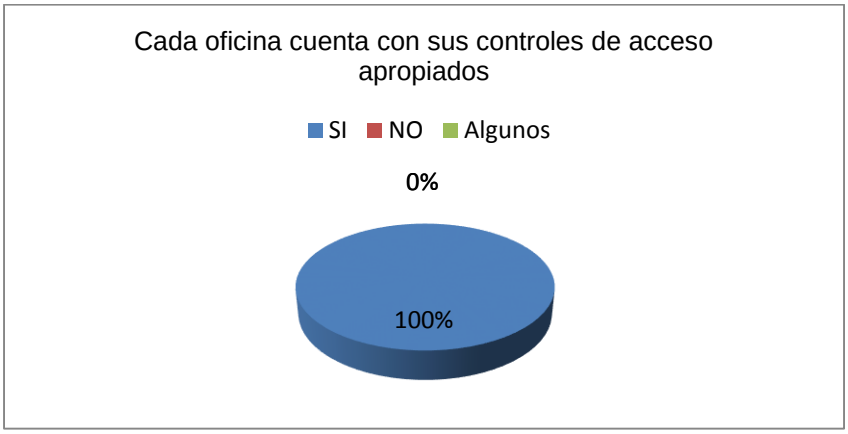


Figura 15. Porcentaje, controles de acceso
Fuente: Autores del Proyecto

El 100% de las oficinas de la dependencia cuentan con las medidas de seguridad de acceso óptimas.

Figura 16. Porcentaje, dispositivos adecuados contra emergencia
Fuente: Autores del Proyecto

La dependencia no cuenta con algunos dispositivos de seguridad necesarios para evitar problemas en caso de una emergencia que se pueda presentar.

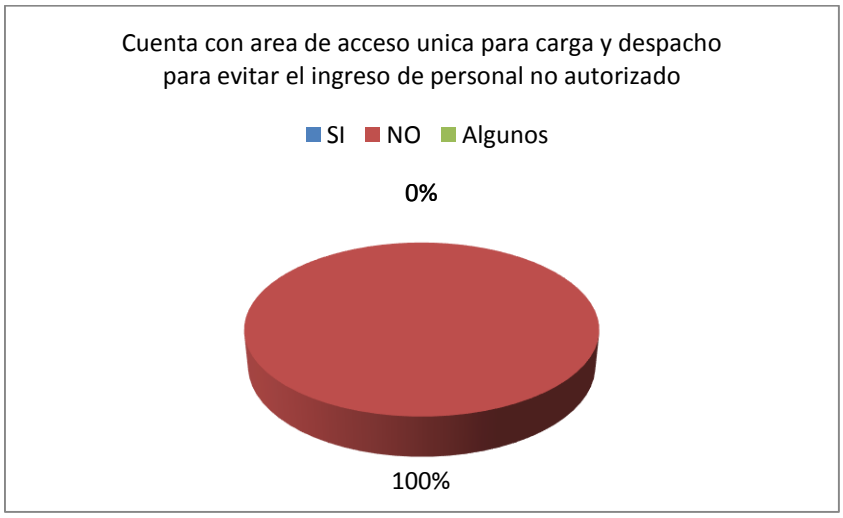


Figura 17. Porcentaje, acceso único para carga y descarga
Fuente: Autores del Proyecto

El dependencia de bienestar no cuenta con un acceso para cargue y descague lo que ocasiona un peligro tanto para los usuarios de la misma, como para el ingreso en areas restringidas.

A.9.2 Seguridad en los equipos

1:

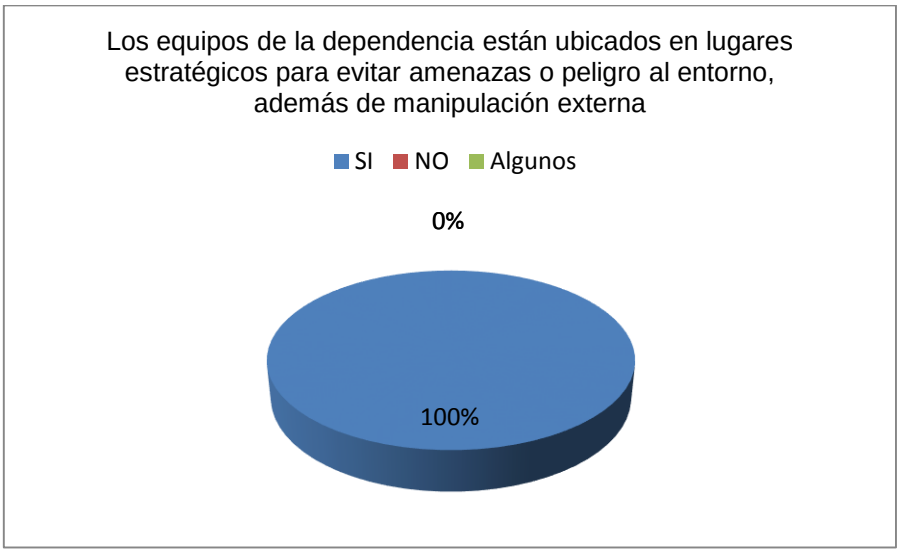


Figura 18. Porcentaje de seguridad de los equipos
Fuente: Autores del Proyecto

Todos los equipos de la dependencia se encuentran ubicados en lugares estratégicos para evitar el contacto directo con los usuarios que ingresan a las oficinas, evitando problemas de seguridad, con un resultado de aprobación de excelente.

2:

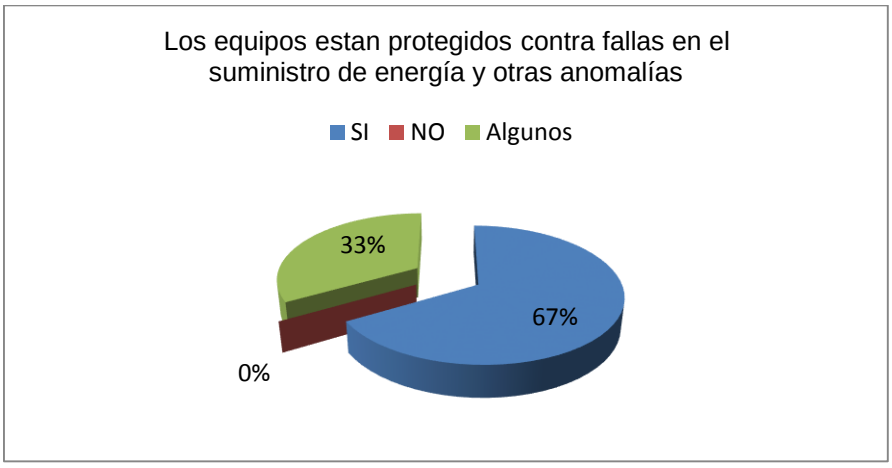


Figura 19. Porcentaje, protección de equipos
Fuente: Autores del Proyecto

Del resultado obtenido se observa que el 67% de los equipos de la dependencia se encuentran protegidos contra problemas del suministro eléctrico, obteniendo un resultado de aprobación de bueno y un índice de mejora bajo.

3:

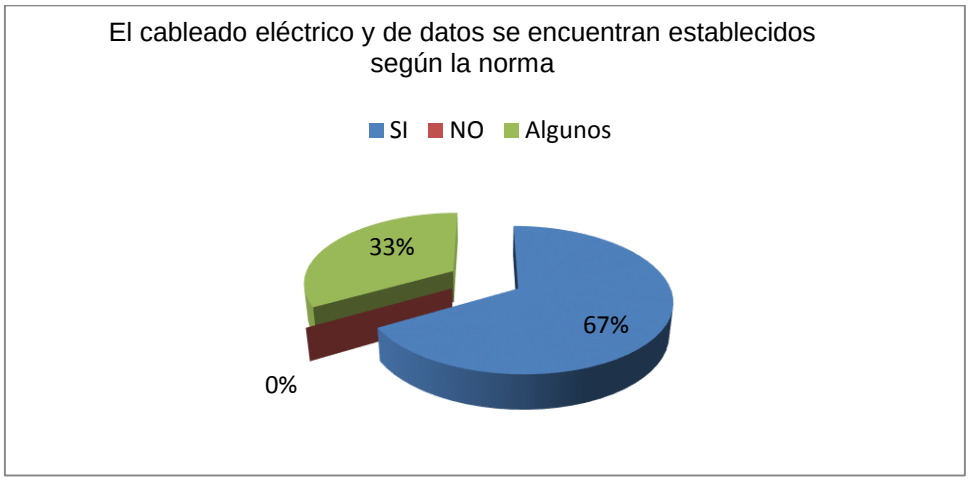


Figura 20. Porcentaje, estructura física
Fuente: Autores del Proyecto

De la gráfica se observa que el 67% de las oficinas de la dependencia, no presentan un fallo en el cableado eléctrico, obteniendo un resultado de aprobación de bueno con un índice de mejora bajo.

A.10 Gestión de comunicaciones y operaciones

A.10.4 Protección contra códigos maliciosos y móviles

1:

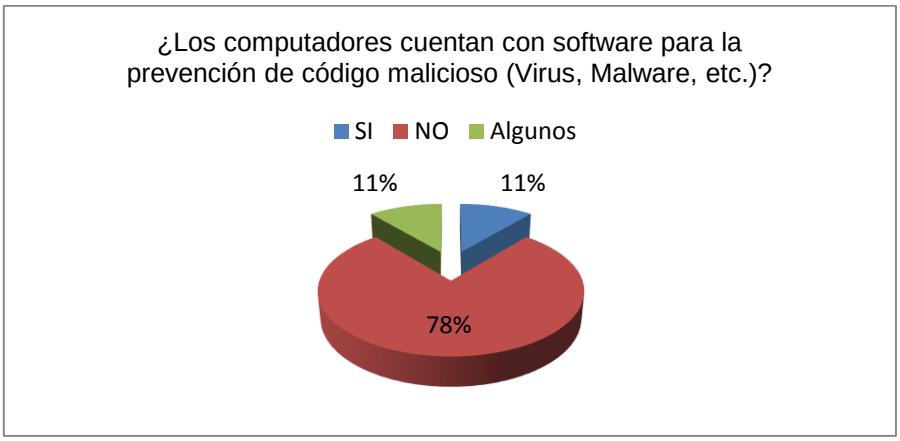


Figura 21. Porcentaje, software malicioso
Fuente: Autores del Proyecto

En la gráfica se observa que el 11% de los equipos de la dependencia cuentan con software para la prevención contra código malicioso, lo que ocasiona un fallo de seguridad muy alto, obteniendo un resultado de aprobación de muy malo con un índice de mejora muy alto.

A.10.5 Respaldo

2:

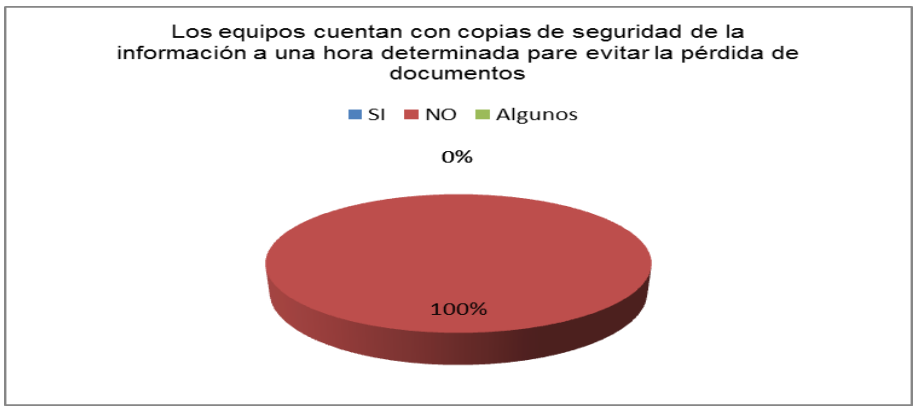


Figura 22. Porcentaje, copias de seguridad
Fuente: Autores del Proyecto

De los resultados obtenidos se observa que el 100% de los equipos de la dependencia están excluidos de copias de seguridad diarias, lo que origina un problema de seguridad grave, obteniendo un resultado de aprobación muy malo y un índice de mejora de muy alto.

A.10.6 Gestión de la seguridad de las redes

Gestión de la seguridad de las redes

1:

Figura 23. Porcentaje, redes
Fuente: Autores del Proyecto

De la gráfica se observa que el 100% de las redes de toda la dependencia se encuentra con las medidas de seguridad óptimas para evitar inconvenientes de seguridad, obteniendo un resultado de aprobación de excelente.

2:

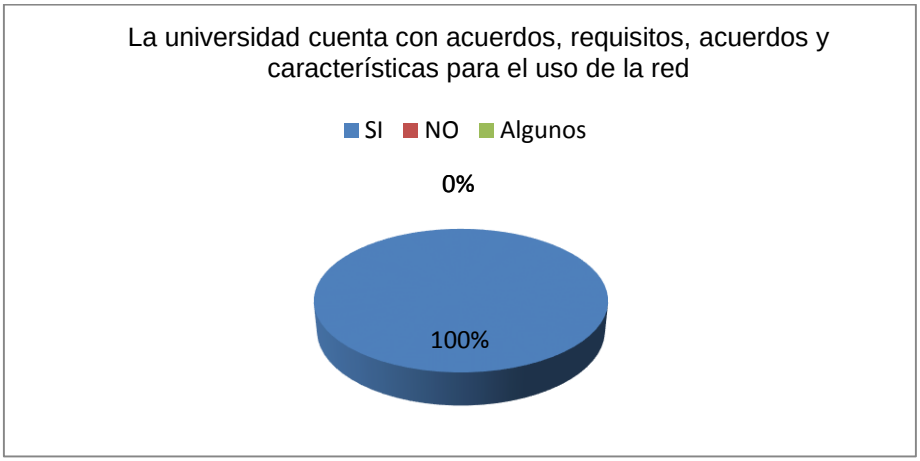


Figura 24. Porcentaje de acuerdos para el uso de la red
Fuente: Autores del Proyecto

La universidad tiene acuerdos que garantice que las redes de la universidad se usen de manera correcta evitando problemas de seguridad, obteniendo un resultado de aprobación de excelente.

A.10.7 Manejo de los medios (Solo se aplica a los funcionarios que manejan el modulo del sistema de información documental)

1.

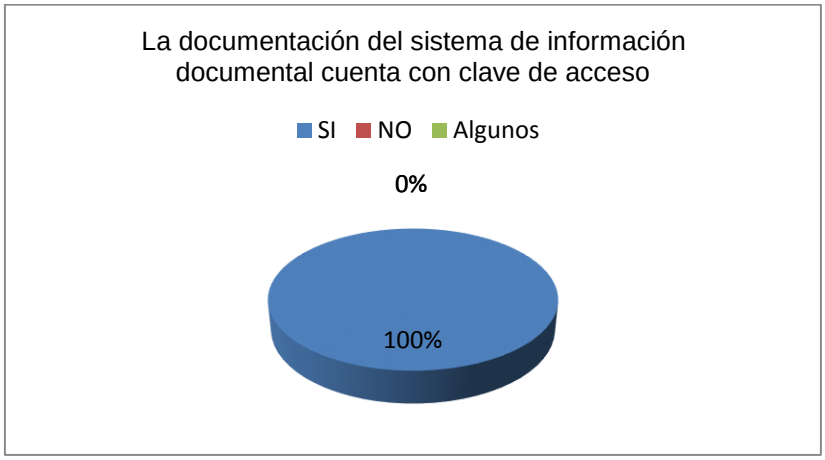


Figura 25. Porcentaje, documentación de claves de acceso
Fuente: Autores del Proyecto

Esta pregunta solo se le aplico a un solo funcionario quien tiene acceso a ese sistema de información, esta cuenta con las medidas de seguridad óptimas para evitar problemas, con un resultado de aprobación de excelente.

A.11 Control de acceso

A.11.3 Responsabilidades de los usuarios

1.

Figura 26. Porcentaje, protección de equipos
Fuente: Autores del Proyecto

De la gráfica se observa que el 100% de los equipos no cuentan con todas las medidas de seguridad necesarias para evitar problemas de seguridad, entre los que están claves de acceso, software antivirus

2.

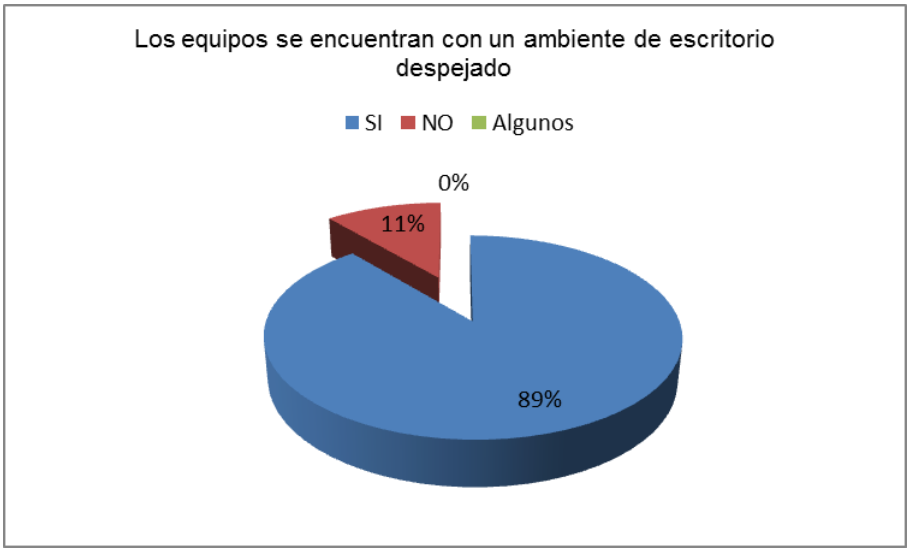


Figura 27. Porcentaje, ambiente de escritorio
Fuente: Autores del Proyecto

Más del 89% de los equipos de la dependencia cuentan con un ambiente de escritorio despejado, con un resultado de aprobación de muy bueno y un índice de mejora muy bajo.

3.

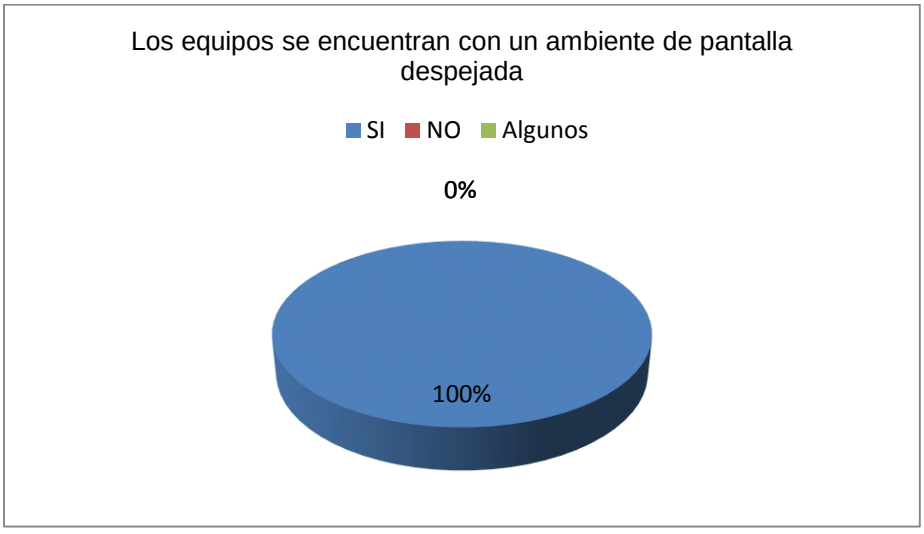


Figura 28. Porcentaje, ambiente de pantalla
Fuente: Autores del Proyecto

Todos los equipos de la dependencia se encuentran con un ambiente de pantalla despejada, lo que evita problemas de seguridad en las oficinas, con un resultado de aprobación de excelente.

A.11.4 Control de acceso a las redes

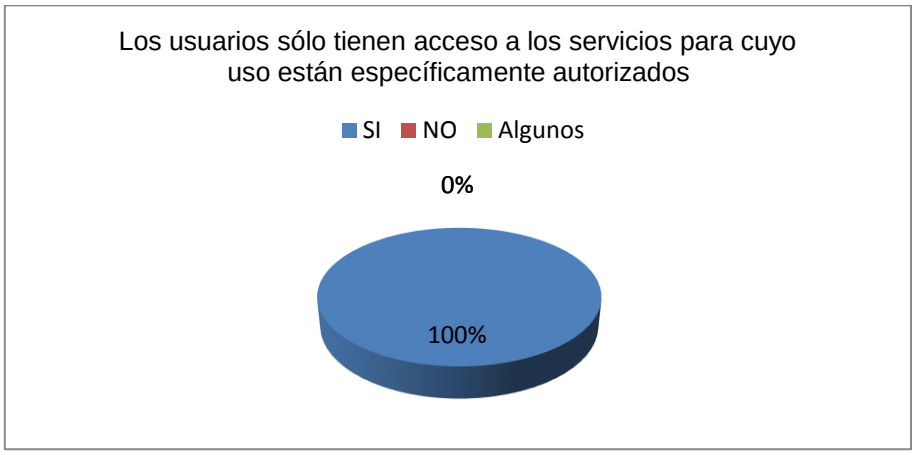


Figura 29. Porcentaje de acceso de usuarios
Fuente: Autores del Proyecto

Cada funcionario de la dependencia cuenta con su usuario y clave de acceso para acceder a los módulos que se les fueron asignados, con un resultado de aprobación de excelente.

A.11.5 Control de acceso al sistema operativo

1.

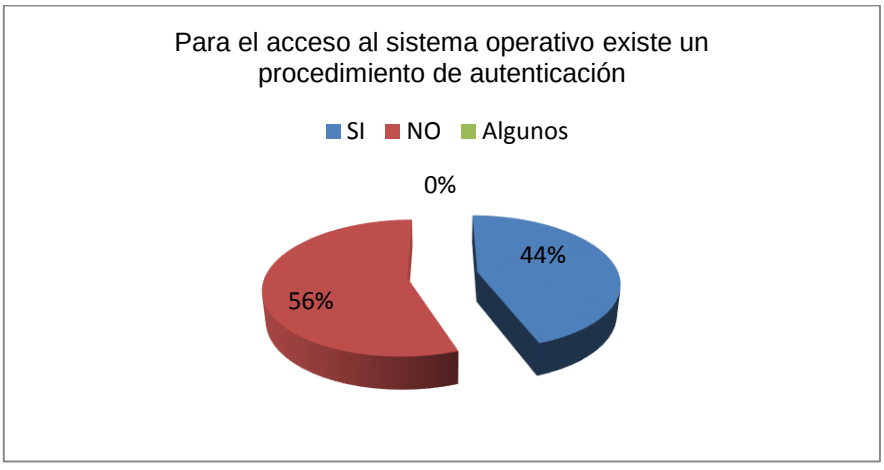


Figura 30. Porcentaje, acceso al sistema operativo
Fuente: Autores del Proyecto

Del resultado obtenido se observa que el 44% de los equipos de la dependencia tienen configurado un método de autenticación para acceder al sistema operativo, lo que ocasiona problemas de seguridad, con un resultado de aprobación de regular y un índice de mejora medio.

2.

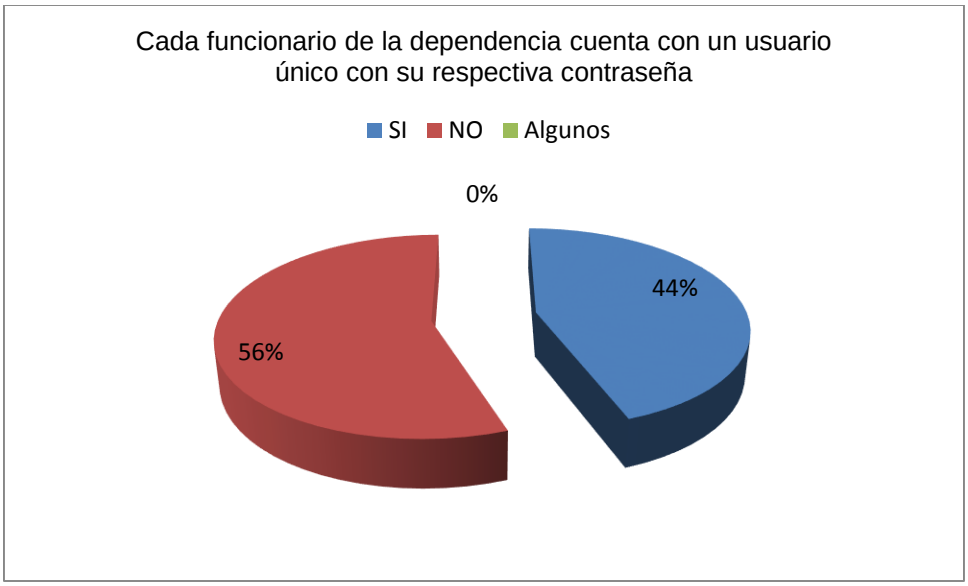


Figura 31. Porcentaje, clave única
Fuente: Autores del Proyecto

El 44% de los equipos de la dependencia tienen método de autenticación para acceder a sus equipos de trabajo, presentando fallas en la seguridad, con un resultado de aprobación de regular y un índice de mejora de medio.

3.

Figura 32. Porcentaje, violación de política de calidad
Fuente: Autores del Proyecto

Los equipos de la dependencia tienen instalado un programa que al apagar el computador este se regresa a su estado inicial, evitando que cualquier programa instalado durante el tiempo de trabajo sea desinstalado.

4.

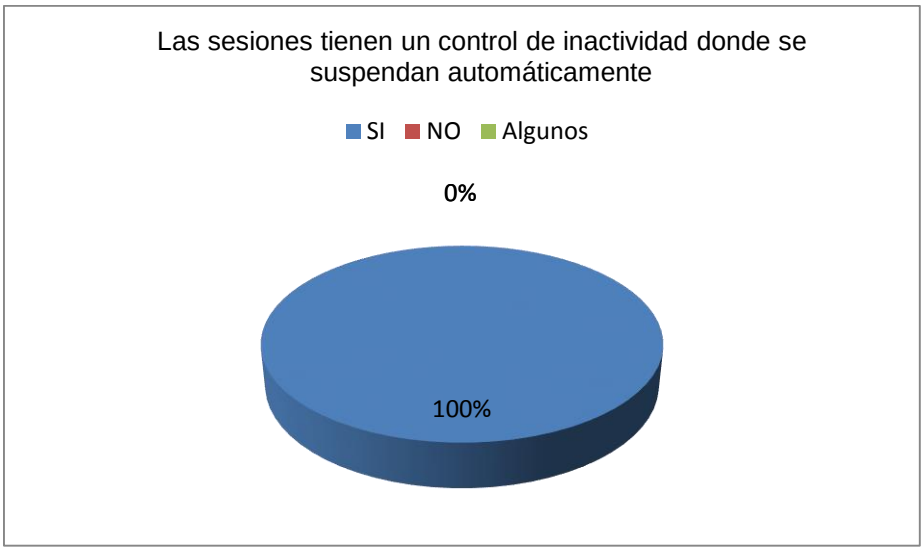


Figura 33. Porcentaje, suspensión automática del sistema
Fuente: Autores del Proyecto

El 100% de los equipos cuentan con un tiempo mínimo de suspensión en caso de inactividad, aunque algunos con un tiempo muy largo, con un resultado de aprobación de excelente.

5.

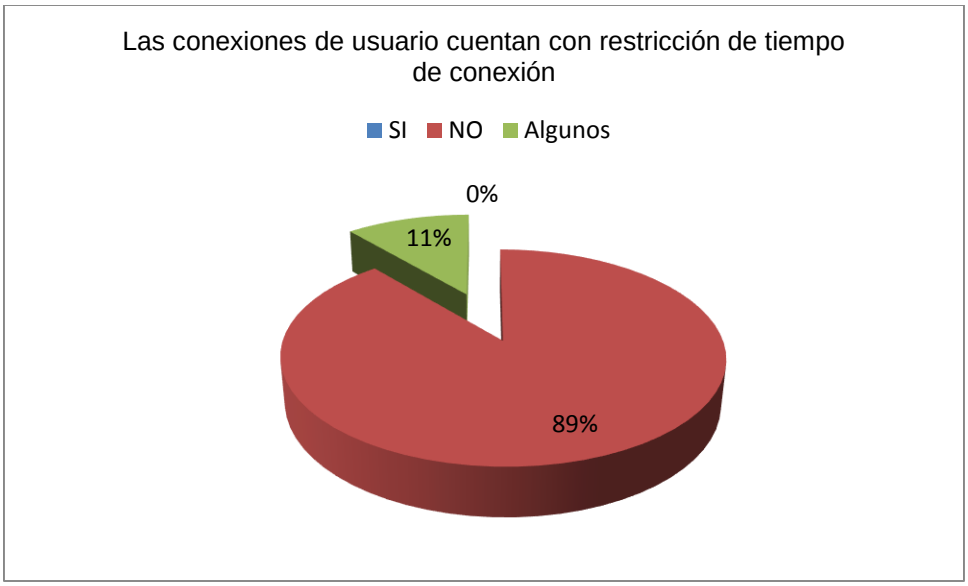


Figura 34. Porcentaje, conexión de usuarios
Fuente: Autores del Proyecto

El 89% de las conexiones de usuario no cuentan con un tiempo límite de conexión, lo que disminuye el nivel de seguridad

Nota: El Diagnostico del OBE2 se realizó la construcción de los instrumentos de recolección usando los dominios a aplicar de la Tabla 3, para luego proceder a su aplicación.

5.3 OBE3: Identificar los riesgos asociados a la seguridad de la información en la dependencia de Bienestar Universitario

5.3.1 A.9 Seguridad física y del entorno

5.3.1.1 A.9.1 Áreas seguras

Objetivo: Evitar el acceso físico no autorizado, el daño e interferencia a las instalaciones y a la información de la organización

Cumple parcialmente, la dependencia no cuenta con todas las medidas de seguridad necesarias para cuando se presente alguna emergencia (detectores de humo, desague, planta eléctrica), además no tienen una puerta de acceso para cargue y descargue (sillas, mesas, equipo de sonido, elementos deportivos), la misma puerta principal de la dependencia es la puerta de cargue y descargue lo que conlleva problemas de seguridad tanto para los usuarios de la dependencia, como para la misma.

5.3.1.2 A.9.2 Seguridad de los equipos

Objetivo: Evitar pérdida, daño, robo o puesta en peligro de los activos y la interrupción de las actividades de la organización.

Cumple parcialmente, el 33% de las oficinas de la dependencia poseen tomas de corriente que se encuentran abiertos lo que ocasiona riesgo para los usuarios y funcionarios de la dependencia, además de ser un causante de incendio, algunos cables de internet están sueltos, además no tienen UPS en caso de problemas de energía.

5.3.2 A.10 Gestión de comunicaciones y operaciones

5.3.2.1 A.10.4 Protección contra códigos maliciosos y móviles

Objetivo: Proteger la integridad del software y de la información.

No cumple, de todos los computadores que tiene la dependencia solo dos cuentan con antivirus instalado, pero ninguno de esos dos tiene una licencia y no se encuentra actualizado a la fecha para mantener protegido los equipos, lo que ocasiona una falla de seguridad grave para las oficinas.

5.3.2.2 A.10.5 Respaldo

Objetivo: Mantener la integridad y disponibilidad de la información y de los servicios de procesamiento de información.

No cumple, la dependencia no maneja una política de copias de seguridad diarias para salvaguardar los documentos que manejan todos los días, lo que ocasiona un grave riesgo de seguridad en caso de daño o pérdida del computador o del disco duro.

5.3.2.3 A.10.6 Gestión de la seguridad de las redes

Objetivo: Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.

Cumple, la dependencia cuenta con una red que se mantiene y se controla según lo establecido por la división de sistemas, lo que garantiza un grado de seguridad a las redes y buen uso del mismo.

5.3.2.4 A.10.7 Manejo de los medios

Objetivo: Evitar la divulgación, modificación, retiro o destrucción de activos no autorizada, y la interrupción en las actividades del negocio.

Cumple parcialmente, el acceso al sistema de información documental de la universidad está protegido con clave de acceso, lo que mejora su seguridad e impide el acceso de personal no autorizado, pero no cuentan con medidas de protección para el acceso a los documentos almacenados en los computadores(claves de acceso), lo que ocasiona problema de seguridad.

5.3.3 A.11 Control de acceso

5.3.3.1 A.11.3 Responsabilidades de los usuarios

Objetivo: Evitar el acceso de usuarios no autorizados, el robo o la puesta en peligro de la información y de los servicios de procesamiento de información.

Cumple parcialmente, el 89% de los equipos de la dependencia no cuentan con software antivirus, algunos no tienen activado el firewall, el 56% no poseen una clave de acceso al sistema operativo y el 11% no tienen un ambiente de escritorio despejado, todo esto ocasiona problemas de seguridad.

5.3.3.2 A.11.4 Control de acceso a las redes

Objetivo: Evitar el acceso no autorizado a servicios en red.

Cumple, cada funcionario de la dependencia solo tienen acceso a los módulos o sistemas de información a los que se les ha autorizado, evitando acceso a otros sitios no autorizados lo que evita problemas en la seguridad de los sistemas o módulos.

5.3.3.3 A.11.5 Control de acceso al sistema operativo

Objetivo: Evitar el acceso no autorizado a los sistemas operativos.

Cumple parcialmente, alguno de los controles pertenecientes a este subdominio no se cumple entre los que se encuentra el 56% de los equipos de la dependencia no cuentan con proceso de autenticación par el acceso al sistema operativo, lo que ocasiona que cualquier persona pueda acceder a los equipos.

5.3.4 A.13 Gestión de los incidentes de la seguridad de la información

5.3.4.1 A.13.1 Reporte sobre los eventos y las debilidades de la seguridad de la información

Objetivo: Asegurar que los eventos y las debilidades de la seguridad de la información asociados con los sistemas de información se comunican de forma tal que permiten tomar las acciones correctivas oportunamente.

Cumple parcialmente, el 22% de los funcionarios de la dependencia no saben que deben hacer para reportar algún problema presentado en los sistemas de información o módulos usados por ellos, o no se les ha capacitado para realizar dichos reportes, lo que ocasiona demoras y problemas de seguridad.

5.3.4.2 A.13.2 Gestión de los incidentes y las mejoras en la seguridad de la información

Objetivo: Asegurar que se aplica un enfoque consistente y eficaz para la gestión de los incidentes de seguridad de la información.

Cumple parcialmente, el 44% de los funcionarios no saben que procedimientos deben llevar a cabo para reportar errores presentados en los sistemas o módulos usados por ellos, además no saben a quién deben dirigirse para recibir una ayuda inmediata a dichos problemas, lo que conlleva a perdida de horas laborales y dificultades en la seguridad de la información.

5.3.5 A.14 Gestión de la continuidad del negocio

5.3.5.1 A.14.1 Aspectos de seguridad de la información, de la gestión de la continuidad del negocio

Objetivo: Contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres, y asegurar su recuperación oportuna.

No cumple, la dependencia de bienestar universitario no tienen establecidos planes para mantener la continuidad del negocio en caso de presentarse algún problema con las actividades que tienen programadas a diario o establecidas por agenda por semestre, actúan por intuición sin seguir un plan para agilizar los procesos, lo que ocasiona demoras en la prestación del servicio y problemas de seguridad.

5.4 OBE4: Realizar recomendaciones para el aseguramiento de la seguridad de la información en la dependencia de Bienestar Universitario

INFORME DE AUDITORIA

Al Magister Carlos Mauricio Navarro

Jefe de Bienestar Universitario

Universidad Francisco de Paula Santander Ocaña

En uso de su aprobación para la realización de la auditoria en la división de bienestar universitario, para evaluar los aspectos de la seguridad de la información de la dependencia.

1. Objetivo De La Auditoria

- Evaluar la seguridad de la información de la dependencia de Bienestar Universitario

2. Alcance de la auditoria

La auditoría se llevará a cabo a la Seguridad de la Información de la dependencia de Bienestar Universitario de la Universidad Francisco de Paula Santander Ocaña, desde el 01 de febrero al 31 de Mayo de 2018.

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
- Tomas de corriente se encuentran abiertos o en mal estado
- Ambiente de escritorio no despejado
- Falta de un plan de continuidad del negocio
- Falta de una entrada para cargue y descargue (mesas, sillas, equipo sonido)

4. Conclusiones

Como resultado de la Auditoría realizada a la dependencia de Bienestar Universitario de la Universidad Francisco de Paula Santander Ocaña, por el período comprendido entre el 01 de febrero al 31 de Mayo de 2018, 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)
- Arreglar los tomas de corriente que se encuentran abiertos o instalarlos de acuerdo a la norma establecida
- Capacitar a los empleados de la importancia de tener un ambiente de escritorio despejado
- Crear un plan de continuidad del negocio para la dependencia
- Construir una entrada de cargue y descargue

ANYELO JULIAN PAEZ PACHECO
Auditor Líder
A&A Auditores

Carta de entrega de informe (Apéndice K)

Referencias

Advisera. (2012). *Advisera*. Obtenido de 27001 Academy: ttps://advisera.com/27001academy/es/que-es-iso-27001/

Bertolìn, J. A. (2008). *Seguridad de la informacion, redes informatica y sistemas de informacion.* Paraninfo.

Bogota, C. d. (2013). *colombiadigital.net*. Obtenido de PARA PROTEGER LOS DATOS PERSONALES: https://colombiadigital.net/publicaciones_ccd/anexos/certicamara_proteccion_datos_ago28.pdf

Cisco. (s.f.). *Servidor Cisco UCS 5100*. Obtenido de http://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-5100-series-blade-server-chassis/index.html

Colombia, C. d. (Julio de 27 de 2000). Obtenido de http://derechodeautor.gov.co/documents/10181/182597/603.pdf/42c15f4a-afe5-4339-97ca-a61026450307

Colombia, C. d. (5 de Enero de 2009). Obtenido de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

Cuesta, B., & Garcia, A. (2002). Sistema de informacion academico.

HPE. (s.f.). *Servidor HPE*. Obtenido de https://www.hpe.com/lamerica/es/product-catalog/servers/proliant-servers/pip.hpe-proliant-dl380-gen9-server.7271241.html

HPE. (s.f.). *Switch Hp 1910*. Obtenido de https://www.hpe.com/lamerica/es/product-catalog/networking/networking-switches/pip.switches.4218346.html

Iribarne, L. (2001). Pasado, Presente y Futuro de los Sistemas de Informacion. España.

Laudon , F., & Laudon, J. (1996). Sistemas de Información. México.: Diana.

Trasobares, A. H. (s.f.). LOS SISTEMAS DE INFORMACIÓN: EVOLUCIÓN Y DESARROLLO. España.

UFPSO, B. U. (s.f.). *Presentacion*. Obtenido de https://portalbienestar.ufpso.edu.co/index.php#

UFPSO, U. F. (s.f.). *Estructura Organizacional*. Obtenido de https://ufpso.edu.co/Estructura

UFPSO, U. F. (s.f.). *Mapa de Procesos*. Obtenido de https://ufpso.edu.co/sig/procedimientos_sig

UFPSO, U. F. (s.f.). *Mision y Vision*. Obtenido de https://ufpso.edu.co/Mision-vision

UFPSO, U. F. (s.f.). *Objetivos*. Obtenido de https://ufpso.edu.co/Objetivos

UPC, D. d. (2004). Sistemas de informacion. Tecnologias de la informacion. *El futuro tecnológico de las terminales Marítimas de vehiculos: la integracion de sus sistemas de informacion.* Barcelona.

Hernandez Sampieri, R., Fernandez Collado, C., & Batipsta Lucio, P. (2014). *Metodología de la Investigación*. Mexico: McGraw-Hill.

Tamayo y Tamayo, M. (2009). *El proceso de la Investigación Cientifica.* Mexico: Limusa.

Apéndice A: Encuesta

Encuesta dirigidita a funcionarios de la Universidad Francisco de Paula Santander Ocaña en el área de bienestar

Objetivo:

Diagnosticar La Seguridad De La Información A La Dependencia De Bienestar Universitario 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 el 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 B: Entrevista

Entrevista dirigidita al jefe de la Dependencia de Bienestar Universitario de la Universidad Francisco de Paula Santander Ocaña

Objetivo:

Diagnosticar La Seguridad De La Información A La Dependencia De Bienestar Universitario De La Universidad Francisco De Paula Santander Ocaña

1. ¿La dependencia de bienestar universitario 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. ¿Bienestar 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 bienestar 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?

Apéndice C: Inventario de Software

Inventario de Software

	Día	Mes	Año
Del	1	2	2018
Al	31	5	2018

Empresa: Bienestar Universitario UFPSO

Periodo: 01 febrero al 31 mayo

Responsable: Anyelo Julián Páez Pacheco – Alba Luz Sánchez

INVENTARIO DE SOFTWARE

REF.	Software	Versión	Numero de Inv.	Licencias	Presentación	Asignado a	Localización
W01	Office Profesional	2013	1970-07-101-01185-00	14		Bienestar Universitario	Bienestar Universitario
A01	Antivirus Eset Endpoint Security		1970-07-101-01385-00	1		Bienestar Universitario	Jefatura
B01	Oracle		1976-07-101-00570-00	5		Bienestar Universitario	Jefatura, Cultura, Deportes, Secretaria
S01	DeepFreeze		1970-07-101-00049-00	14		Bienestar Universitario	Bienestar Universitario

Apéndice D: Inventario de Hardware

Inventario de Hardware

	Día	Mes	Año
Del	1	2	2018
Al	31	5	2018

Empresa: Universidad Francisco de Paula Santander Ocaña

Auditor:

Área Auditada: Bienestar Universitario – Oficina de Deportes

Inventario Individual de Hardware

Computador Principal

NÚM.	EQUIPO	MARCA	NÚM. INVENTARIO	CARACTERÍSTICAS	OBSERVACIONES
1	Computador todo en uno	HP	1670021010118600		
2	Procesador	Intel Core		Intel Core i7	
3	Teclado				GK-670006/U
4	Mouse				MOFYOU

Computador Secundario

NÚM.	EQUIPO	MARCA	NÚM. INVENTARIO	CARACTERÍSTICAS	OBSERVACIONES
1	Pantalla	HP	1670021010048113		
2	Teclado		1670021010004015		
3	Mouse				M-5BF96
4	Torre		16700210100048100		
5	Procesador	Intel Core		Intel Core 2 Duo	

Área Auditada: Bienestar Universitario – Oficina de Cultura

Inventario Individual de Hardware

Computador Principal

NÚM.	EQUIPO	MARCA	NÚM. INVENTARIO	CARACTERÍSTICAS	OBSERVACIONES
1	Computador todo en uno	HP	1670021010004200		
2	Procesador	Intel Core		Intel Core 2 Duo	
3	Teclado		1670021010004215		
4	Mouse		1670021010004216		

Computador Secundario

NÚM.	EQUIPO	MARCA	NÚM. INVENTARIO	CARACTERÍSTICAS	OBSERVACIONES
1	Pantalla	HP	1670021010004200		
2	Teclado		16700210110054715		
3	Mouse		1670021010054716		
4	Torre		1670021010031201		
5	Procesador	Intel Core		Intel Core 2 Duo	

Área Auditada: Bienestar Universitario – Secretaria

Inventario Individual de Hardware

Computador Principal

NÚM.	EQUIPO	MARCA	NÚM. INVENTARIO	CARACTERÍSTICAS	OBSERVACIONES
1	Computador todo en uno	HP	1670021010112800		
2	Procesador	Intel Core		Intel Core i7	
3	Teclado		1670021010112815		
4	Mouse		1670021010112816		
5	Impresora	Hp	1670901040014500		

Computador Secundario

NÚM.	EQUIPO	MARCA	NÚM. INVENTARIO	CARACTERÍSTICAS	OBSERVACIONES
1	Pantalla	HP	1670021010011813		
2	Teclado		1670021010029915		
3	Mouse				X812824
4	Torre		1670021010029915		
5	Procesador	Intel Core		Intel Core 2 Duo	

Área Auditada: Bienestar Universitario – Psicología

Inventario Individual de Hardware

Computador Principal

NÚM.	EQUIPO	MARCA	NÚM. INVENTARIO	CARACTERÍSTICAS	OBSERVACIONES
1	Computador todo en uno	HP	1670021010079800		
2	Procesador	Intel Core		Intel Core i3	
3	Teclado		1670021010079815		
4	Mouse		1670021000078816		

Área Auditada: Bienestar Universitario – Trabajo Social

Inventario Individual de Hardware

Computador Principal

NÚM.	EQUIPO	MARCA	NÚM. INVENTARIO	CARACTERÍSTICAS	OBSERVACIONES
1	Computador todo en uno	HP	1670021010080100		
2	Procesador	Intel Core		Intel Core i3	
3	Teclado		1670021010080115		
4	Mouse		1670021010112816		

Computador Secundario

NÚM.	EQUIPO	MARCA	NÚM. INVENTARIO	CARACTERÍSTICAS	OBSERVACIONES
1	Pantalla	HP	1670021010080100		
2	Teclado		1670021010029915		539130-161
3	Mouse				M-UAE119
4	Torre		1670021010053800		
5	Procesador	Intel Core		Intel Core 2 Duo	

Área Auditada: Bienestar Universitario – Enfermería

Inventario Individual de Hardware

Computador Principal

NÚM.	EQUIPO	MARCA	NÚM. INVENTARIO	CARACTERÍSTICAS	OBSERVACIONES
1	Computador todo en uno	HP	1670021010080015		
2	Procesador	Intel Core		Intel Core i7	
3	Teclado		1670021010080000		
4	Mouse				674316-001
5	Impresora	Samsung	5111141330000700		

Área Auditada: Bienestar Universitario – Consultorio Medico

Inventario Individual de Hardware

Computador Principal

NÚM.	EQUIPO	MARCA	NÚM. INVENTARIO	CARACTERÍSTICAS	OBSERVACIONES
1	Computador todo en uno	HP	1670021010079900		
2	Procesador	Intel Core		Intel Core i3	
3	Teclado		1670021010079915		
4	Mouse				GM- 070005

Área Auditada: Bienestar Universitario – Asesoría Espiritual

Inventario Individual de Hardware

Computador Principal

NÚM.	EQUIPO	MARCA	NÚM. INVENTARIO	CARACTERÍSTICAS	OBSERVACIONES
1	Computador todo en uno	HP	1670021010009000		
2	Procesador	Intel Core		Intel Core 2 Duo	
3	Teclado		1670021010009015		
4	Mouse		1670021010009016		

Área Auditada: Bienestar Universitario – Oficina Egresados

Inventario Individual de Hardware

Computador Principal

NÚM.	EQUIPO	MARCA	NÚM. INVENTARIO	CARACTERÍSTICAS	OBSERVACIONES
1	Computador todo en uno	HP	1670021010112900		
2	Procesador	Intel Core		Intel Core i7	
3	Teclado		1670021010112916		
4	Mouse		1670021010112915		

Área Auditada: Bienestar Universitario – Jefatura

Inventario Individual de Hardware

Computador Principal

NÚM.	EQUIPO	MARCA	NÚM. INVENTARIO	CARACTERÍSTICAS	OBSERVACIONES
1	Computador todo en uno	HP	1870021010078800		
2	Procesador	Intel Core		Intel Core i3	
3	Teclado	Hp	1670021010078815		
4	Mouse	Hp			
5	Impresora	Hp	1670901040015400		

Apéndice E: Listas de chequeo

AA AUDITORES	A.9 SEGURIDAD FÍSICA Y DEL ENTORNO			
A.9.1 Áreas seguras	Si	Algunos	No	Observaciones
1. El acceso al área de Bienestar Universitario está restringido por una puerta con chapa adecuada				
2. Cada oficina cuenta con sus controles de acceso apropiados				
3. El área de Bienestar cuenta con dispositivos adecuados contra emergencia(detector humo, extintores, camillas, entre otros)				
4. Cuenta con área de acceso única para carga y despacho para evitar el ingreso de personal no autorizado				

AA AUDITORES	A.9 SEGURIDAD FÍSICA Y DEL ENTORNO			
A.9.2 Seguridad de los equipos	Si	Algunos	No	Observaciones
1. Los equipos de la dependencia están ubicados en lugares estratégicos para evitar amenazas o peligro al entorno, además de manipulación externa				
2. Los equipos deben estar protegidos contra fallas en el suministro de energía y otras anomalías				

3. El cableado eléctrico y de datos se encuentran establecidos según la norma ()				

AA AUDITORES	**A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES**			
A.10.4 Protección contra códigos maliciosos y móviles	Si	Algunos	No	Observaciones
1. Los computadores cuentan con software para la prevención de código malicioso (Virus, Malware, etc.)				

AA AUDITORES	**A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES**			
A.10.5 Respaldo	Si	Algunos	No	Observaciones
1. Los equipos cuentan con copias de seguridad de la información a una hora determinada pare evitar la pérdida de documentos				

AA AUDITORES	**A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES**			
A.10.6 Gestión de la seguridad de las redes	Si	Algunos	No	Observaciones
1. Las redes de la dependencia cuenta con las medidas de seguridad para garantizar el buen uso de los servicios de la red y la seguridad de la información				

2. La universidad cuenta con acuerdos, requisitos, acuerdos y características para el uso de la red				

AA AUDITORES	A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES

A.10.7 Manejo de los medios	Si	Algunos	No	Observaciones
1. La documentación del sistema de información documental cuenta con clave de acceso				
A.11 CONTROL DE ACCESO				
A.11.3 Responsabilidades de los usuarios	Si	Algunos	No	Observaciones
1. Los equipos de la dependencia cuentan con protección adicional para evitar problemas de seguridad (claves de acceso, antivirus, firewall, etc)				
2. Los equipos se encuentran con un ambiente de escritorio despejado				
3. Los equipos se encuentran con un ambiente de pantalla despejada				

AA AUDITORES	**A.11 CONTROL DE ACCESO**

A.11.4 Control de acceso a las redes	Si	Algunos	No	Observaciones
1. Los usuarios sólo tienen acceso a los servicios para cuyo uso están específicamente autorizados				

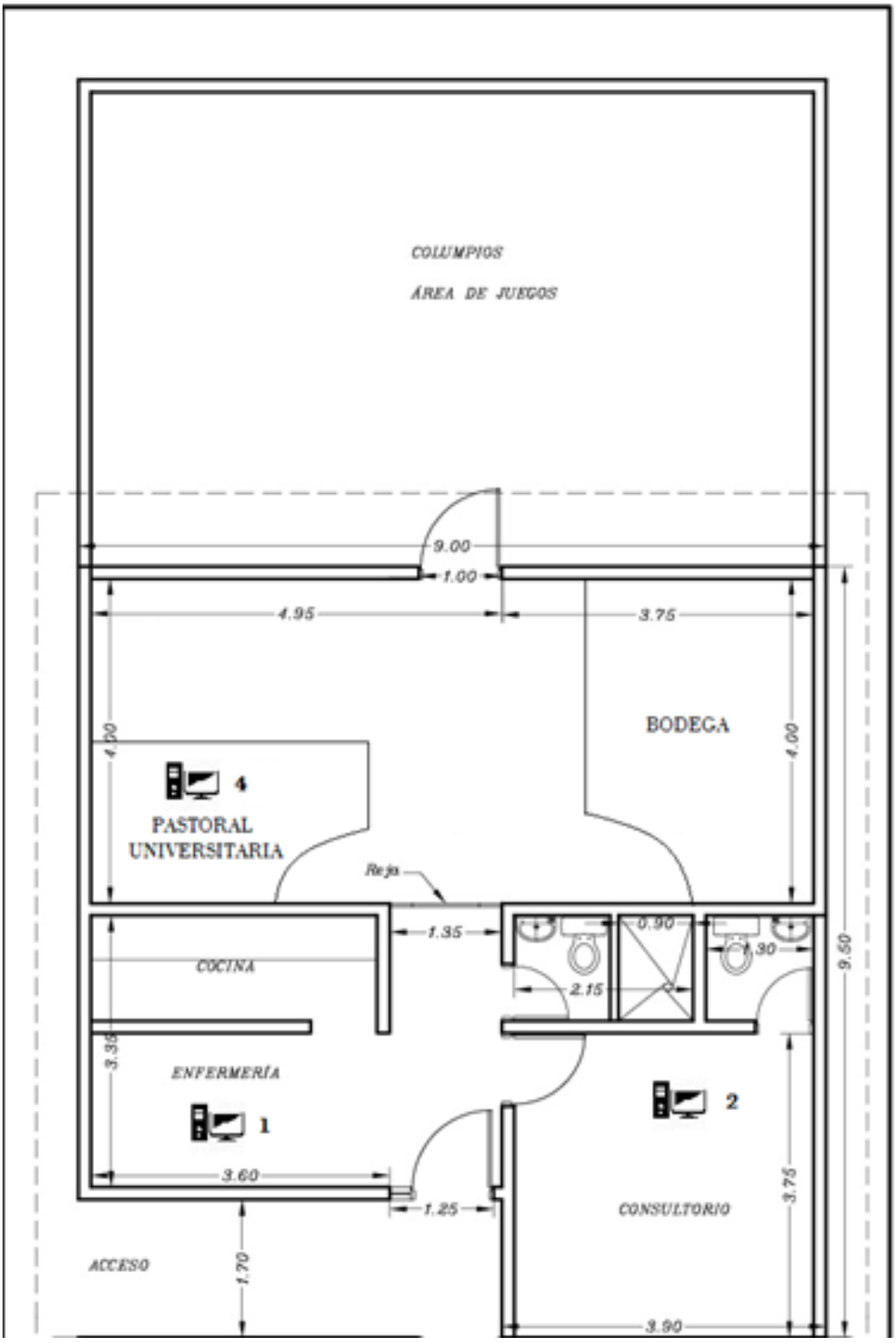
AA AUDITORES	A.11 CONTROL DE ACCESO			
A.11.5 Control de acceso al sistema operativo	Si	Algunos	No	Observaciones
1. Para el acceso al sistema operativo existe un procedimiento de autenticación				
2. Cada funcionario de la dependencia cuenta con un usuario único con su respectiva contraseña				
3. Existe instalado algún que viole las políticas de seguridad establecidas				
4. Las sesiones tienen un control de inactividad donde se suspendan automáticamente				
5. Las conexiones de usuario cuentan con restricción de tiempo de conexión				

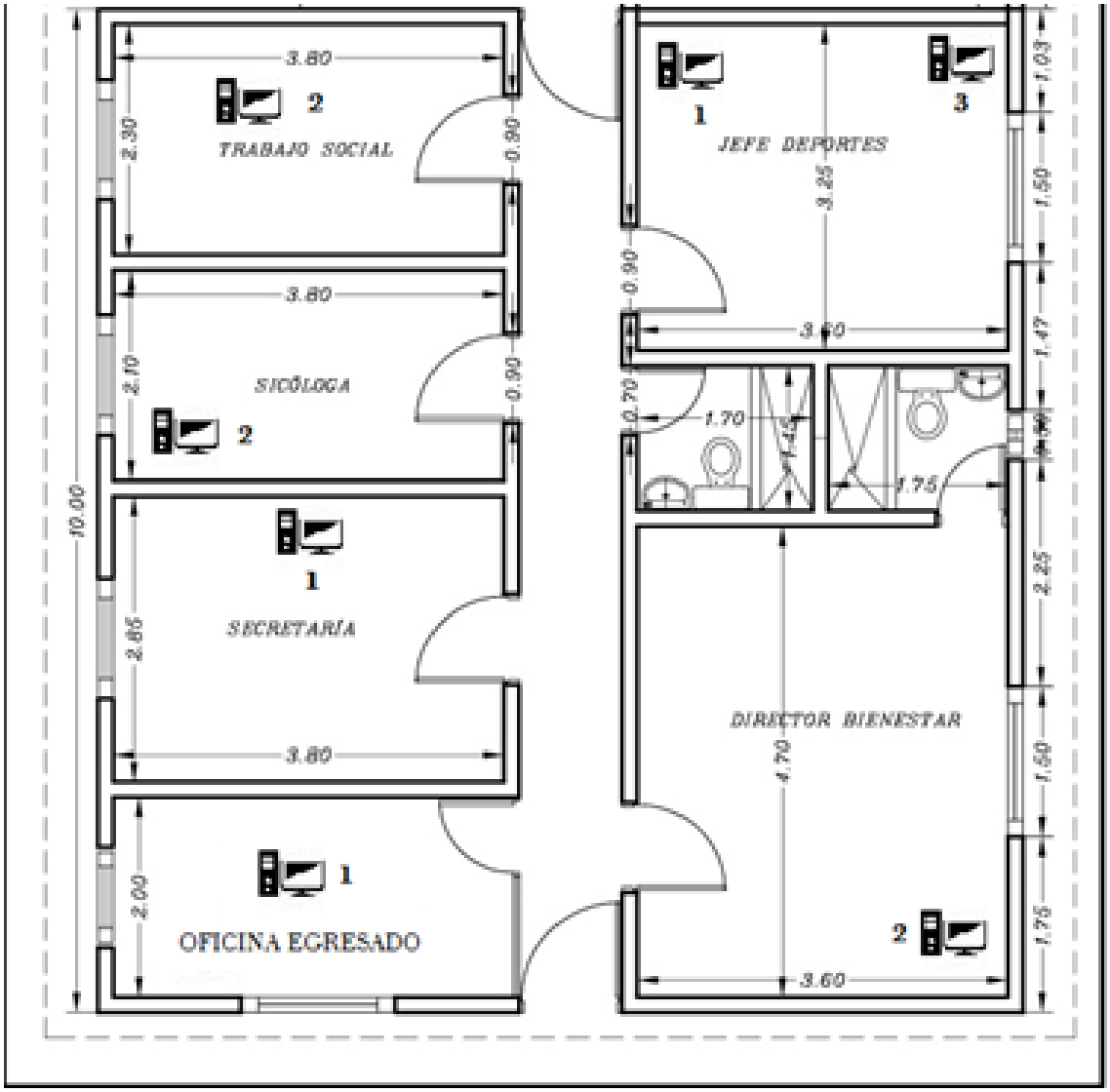
Apéndice F: Programa de Auditoria

AA AUDITORES	PROGRAMA DE AUDITORIA			
Empresa: Universidad Francisco de Paula Santander Ocaña – Bienestar Universitario				Fecha: 01-02-2018
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 Bienestar Universitario	6 Hrs 2 Hrs	8 Hrs	
2	Desarrollo de la auditoria • Entrevista con el jefe de Bienestar Universitario • 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 Bienestar universitario	60 Hrs 100 Hrs 120 Hrs 20 Hrs	300 Hrs	
4	Informe • Elaboración y presentación del diagnóstico final al Jefe de Bienestar Universitario	52 Hrs	52 Hrs	

Apéndice G: Mapa Tecnológico




3.80
2
TRABAJO SOCIAL
2.30
0.90
3.80
SICÓLOGA
2.10
2
0.90
10.00
1
SECRETARÍA
2.85
3.80
1
OFICINA EGRESADO
2.00
1
JEFE DEPORTES
3
3.25
0.90
3.80
0.70
1.70
1.45
1.75
DIRECTOR BIENESTAR
4.70
2
3.60
1.03
1.50
1.47
2.25
1.50
1.75

Apéndice H: Dominios Excluidos

Dominios y Subdominios excluidos para la aplicación de la auditoria	
Dominio	Observación
A.5: política de seguridad	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.
A.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.
A.7: 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.
A.8: 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.
A.9.2.5: seguridad de los equipos fuera de las Instalaciones	Los equipos pertenecientes a la dependencia no pueden ser retirados de la universidad.
A.10.1: procedimientos operacionales y responsabilidades A.10.2: gestión de la prestación del servicio por terceras partes A.10.3: planificación y aceptación del sistema	La división de sistemas se encarga de la aplicabilidad de los subdominios
A.10.4.2: controles contra códigos móviles A.10.7.1: gestión de los medios removibles A.10.7.2: eliminación de los medios.	Estos controles no son aplicables
A.10.8: intercambio de la información	Este subdominio no se aplica, debido que la universidad no intercambia sus software con entidades externas
A.10.9: servicios de comercio electrónico	Este subdominio no se aplica debido a que la universidad no realiza comercio electrónico

A.10.10: monitoreo	La división de sistemas se encarga de la aplicabilidad del subdominio
A.11.4.2: Autenticación de usuarios para conexiones externas. A.11.4.3: identificación de los equipos en las redes.	Estos controles no son aplicables debido a que la universidad no realiza este tipo de autenticación
A.11.4.4: protección de los puertos de configuración y diagnóstico remoto A.11.4.5: separación en las redes A.11.4.6: control de conexión a las redes A.11.4.7: control de enrutamiento en la red	La división de sistemas es la encargada de la aplicabilidad de estos controles
A.11.6: control de acceso a las aplicaciones y a la información	La división de sistemas es la encargada de la aplicabilidad de este subdominio
A.11.7: Computación móvil y trabajo remoto	La universidad no tiene trabajo remoto y uso de computación móvil
A.12: adquisición, desarrollo y mantenimiento de sistemas de información	La división de sistemas junto con la oficina de almacén son los encargados de la aplicabilidad de este dominio, aplica para todo el dominio
A.15: cumplimiento	La división de sistemas y la oficina de jurídica son los encargados de la aplicabilidad del dominio, aplica para todo el dominio.

Apéndice I: Dictamen de Auditoria

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 Bienestar 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 solo 22% cuentan con software de protección, pero ninguno de ellos tiene su respectiva licencia y no se encuentra actualizado a la fecha, 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 solo el 44% 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.

De las medidas de seguridad que posee la universidad en caso de emergencias, muchos de los funcionarios no tienen una idea clara de que deben hacer en caso de presentarse una calamidad dentro de la dependencia y de la misma universidad, la cual ellos esperan que la oficina de salud ocupacional en cabeza de COPASO les de las respectivas indicaciones de que deben hacer en una emergencia, lo que puede ocasionar pérdidas humanas, como también perdidas de los bienes de la dependencia

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 Bienestar Universitario.

En las medidas de seguridad tecnológica ninguno de los equipos de la dependencia cuentan 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, además algunos tomas de corriente se encuentran abiertos lo que ocasiona un peligro para los funcionarios como para los usuarios, como también un cable de red dañado.

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.

La dependencia no cuenta con una entrada exclusiva para el cargue y descargue de objetos usados por la dependencia y demás dependencias de la universidad como sillas, mesas, equipo de sonido,

implementación deportiva, lo que ocasiona un peligro para los usuarios que ingresan a diario, además de que algún usuario ingrese de manera indebida a la bodega.

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 programado de manera semestral.

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

Atentamente,

ANYELO JULIAN PAEZ PACHECO
Auditor Líder
A&A Auditores

SITUACIONES ENCONTRADAS

AREA AUDITADA
BIENESTAR UNIVERSITARIO

DIA	MES	AÑO
10	04	2018

Ref.	Situación	Causas	Solución	Fecha de Solución	Responsable
SE1	Falta de antivirus en los equipos	Esta situación se presenta debido a controles mínimos de tecnología	Instalación de antivirus gratuito, o un antivirus de pago con su respectiva licencia actualizado a la fecha	10-09-2018	Jefe de la división de sistemas

SE2	Falta de claves de acceso a los equipos	Esta situación se presenta debido a controles mínimos de tecnología	Capacitar al personal de la importancia de una clave de acceso a los equipos	10-09-2018	Jefe de Bienestar Universitario
SE3	Desconocimiento de la importancia del reporte de errores presentados en los módulos o sistemas de información	Esta situación se presenta debido a falta de capacitaciones en el personal de Bienestar	Capacitar al personal sobre la importancia del reporte de errores de manera inmediata	10-09-2018	Jefe de Bienestar Universitario, División de Sistemas
SE4	Falta de copias de seguridad internas	Esta situación se presenta debido a faltas de políticas internas en la dependencia	Crear una política interna de copias de seguridad	10-09-2018	Jefe de Bienestar Universitario
SE5	Falta de un plan de continuidad del negocio	Esta situación se presenta por desconocimiento del Jefe de Bienestar Universitario	Capacitar al jefe de Bienestar Universitario sobre la importancia y creación de un plan de continuidad del negocio	10-09-2018	División de sistemas

ELABORO
ALBA LUZ SANCHEZ PERILLA

APROBO
ANYELO JULIAN PAEZ PACHECO

RESUMEN DE DESVIACIONES DETECTADAS

AREA AUDITADA
BIENESTAR UNIVERSITARIO

DIA	MES	AÑO
10	04	2018

Ref.	Situación	Causas	Solución
DD1	Falta de antivirus en los equipos	Esta situación se presenta debido a controles mínimos de tecnología	Instalación de antivirus gratuito, o un antivirus de pago con su respectiva licencia actualizado a la fecha

ELABORO
ALBA LUZ SANCHEZ PERILLA

APROBO
ANYELO JULIAN PAEZ PACHECO

Apéndice J: Pruebas de Cumplimiento

<table>
<tr><td colspan="4">PRUEBAS</td><td colspan="4"> 
</td></tr>
<tr><td>OBJETIVO</td><td colspan="4">Verificar la existencia de antivirus en los equipos de la dependencia, y que estos estén actualizados.</td><td>PRUEBA</td><td>1</td></tr>
<tr><td>TECNICAS EMPLEADAS</td><td colspan="6">Observación
Listas de chequeo</td></tr>
<tr><td>TIPO DE PRUEBA</td><td>CUMPLIMIENTO</td><td></td><td>SUSTANTIVA</td><td>X</td><td>DOBLE FINALIDAD</td><td></td></tr>
<tr><td>PROCEDIMIENTO A EMPLEAR</td><td colspan="6">1. Verificar la existencia de un antivirus en cada equipo de la dependencia de Bienestar Universitario de la Universidad Francisco de Paula Santander Ocaña
2. Determinar que los antivirus estén actualizados y estén activos sus módulos de protección.
3. Evaluar si el antivirus cumple su objetivo de protección a los equipos usados por la dependencia.</td></tr>
<tr><td>RECURSOS</td><td colspan="6">1. Humano: Auditor de sistemas y usuario final
2. Tecnológico: Equipo cómputo para anotaciones</td></tr>
<tr><td colspan="7">RESULTADOS DE LA PRUEBA</td></tr>
<tr><td>HALLAZGOS</td><td colspan="6">Realizada la prueba se encontró que de todos los equipos de la dependencia, solo el 22% de los equipos tienen un antivirus instalado, pero sin licencia y no están actualizados a la fecha.</td></tr>
<tr><td>CAUSA</td><td colspan="6">Esta situación se presenta debido a controles mínimos de tecnología</td></tr>
<tr><td>SITUACIÓN DE RIESGO QUE GENERA</td><td colspan="6">Perdida de información y manipulación del equipo por virus y malware</td></tr>
<tr><td>RECOMENDACIONES DE AUDITORIA</td><td colspan="6">Instalación de antivirus a todos los equipos con su respectiva licencia</td></tr>
<tr><td>ELABORADO POR</td><td colspan="2">Alba Luz Sánchez Perilla</td><td>REVISADO POR</td><td colspan="3">Anyelo Julián Páez Pacheco</td></tr>
</table>

<table>
<tr><td colspan="6">PRUEBAS</td><td colspan="3"> 
AA
AUDITORES</td></tr>
<tr><td>OBJETIVO</td><td colspan="5">Comprobar la existencia de claves de acceso a los equipos usados en la dependencia</td><td>PRUEBA</td><td>2</td></tr>
<tr><td>TECNICAS EMPLEADAS</td><td colspan="7">Observación
Listas de chequeo</td></tr>
<tr><td>TIPO DE PRUEBA</td><td>CUMPLIMIENTO</td><td></td><td>SUSTANTIVA</td><td>X</td><td>DOBLE FINALIDAD</td><td></td></tr>
<tr><td>PROCEDIMIENTO A EMPLEAR</td><td colspan="7">1. Observar la existencia de claves de acceso a los equipos de la dependencia.
2. Verificar que las claves de acceso sean seguras.
3. Observar la cantidad de usuarios existentes en el computador y sus privilegios.
4. Verificar que cada usuario este con su debida protección de ingreso.</td></tr>
<tr><td>RECURSOS</td><td colspan="7">1. Humano: Auditor de sistemas
2. Tecnológico: Equipo cómputo para anotaciones</td></tr>
<tr><td>HALLAZGOS</td><td colspan="7">Algunos equipos usados por la dependencia cuentan con claves de acceso</td></tr>
<tr><td>CAUSA</td><td colspan="7">Esta situación se presenta debido a controles mínimos de tecnología</td></tr>
<tr><td>SITUACIÓN DE RIESGO QUE GENERA</td><td colspan="7">Intrusión de personas ajenas a los equipos de la dependencia, perdida de información.</td></tr>
<tr><td>RECOMENDACIONES DE AUDITORIA</td><td colspan="7">Creación de claves de acceso a todos los equipos de la dependencia.</td></tr>
<tr><td>ELABORADO POR</td><td colspan="2">Alba Luz Sánchez Perilla</td><td>REVISADO POR</td><td colspan="3">Anyelo Julián Páez Pacheco</td></tr>
</table>

PRUEBAS							AA AUDITORES
OBJETIVO	Verificar la existencia de un plan de continuidad del negocio				PRUEBA		3
TECNICAS EMPLEADAS	Entrevista						
TIPO DE PRUEBA	CUMPLIMIENTO		SUSTANTIVA		DOBLE FINALIDAD		X
PROCEDIMIENTO A EMPLEAR	1. Realizar entrevista al jefe de Bienestar Universitario para verificar la existencia de un plan de continuidad del negocio. 2. Verificar que el plan de continuidad del negocio incluya toda la dependencia.						
RECURSOS	1. Humano: Auditor de sistemas, usuarios finales 2. Tecnológico: Equipo cómputo para anotaciones						
HALLAZGOS	No cuentan con un plan de continuidad del negocio						
CAUSA	Esta situación se presenta debido a desconocimiento del jefe de la dependencia del plan de continuidad del negocio						
SITUACIÓN DE RIESGO QUE GENERA	Demora en los procesos de la dependencia en caso de presentarse algún problema interno						
RECOMENDACIONES DE AUDITORIA	Capacitar al jefe de la dependencia de la importancia de un plan de continuidad del negocio, creación del plan de continuidad del negocio						
ELABORADO POR	Alba Luz Sánchez Perilla		REVISADO POR		Anyelo Julián Páez Pacheco		

Apéndice K: Carta Entrega Informe Final

Ocaña, 22 de Agosto de 2018

Magister

CARLOS MAURICIO NAVARRRO

Jefe Bienestar Universitario

Universidad Francisco de Paula Santander

Ciudad

Cordial saludo,

Respetuosamente me permito presentar el Informe de Resultados de la Auditoría efectuada a la Seguridad de la Información de la Dependencia de Bienestar Universitario de la Universidad Francisco de Paula Santander, que se realizó entre el 01 de Febrero y el 31 de Mayo del año en curso.

Atentamente,

ANYELO JULIAN PAEZ PACHECO
Auditor Líder
A&A Auditores

Apéndice L: Evidencias

Toma de corriente abierto Psicología

Toma de corriente abierto Psicología

Cable de red dañado Medico

Toma de corriente abierto Trabajo Social

Entrada de acceso a la Dependencia de Bienestar


OCAÑA
ENFERMERÍA