UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE GUAYAQUIL

CARRERA INGENIERÍA EN SISTEMAS

Tesis previa a la obtención del título de: INGENIERO DE SISTEMA

TEMA:

ANÁLISIS DE REQUISITOS DE TECNOLOGÍA DE INFORMACIÓN PARA LA APLICACIÓN DE TÉCNICAS DE SEGURIDAD BAJO LA NORMATIVA NTE INEN –ISO/IEC 27001:2011 EN LA UNIDAD EDUCATIVA SALESIANA "DOMINGO COMÍN"

AUTORAS:

BLANCA STEPHANYE DELGADO PIJAL

JOSELYNE GABRIELA GARCÍA BARRERA

DIRECTORA:

ING. SHIRLEY COQUE VILLEGAS

Guayaquil, marzo de 2015

DECLARATORIA DE RESPONSABILIDAD Y AUTORIZACIÓN DE USO DEL TRABAJO DE GRADO

Nosotras Blanca Stephanye Delgado Pijal y Joselyne Gabriela García Barrera, autorizamos a la Universidad Politécnica Salesiana la publicación total o parcial de este trabajo de grado y su reproducción sin fines de lucro.

Además declaramos que los conceptos y análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad de las autoras.

Blanca Stephanye Delgado Pijal
CC: 0919378471

Joselyne Gabriela García Barrera
CC: 0926789017

Dedicatoria

En primer lugar quiero agradecer a Dios por permitirme seguir con vida, salud y por guiarme por el camino del bien, esta meta cumplida le dedico a mi madre por ser el pilar fundamental en mi vida, ella ha sido mi ejemplo a seguir ya que ha sido padre y madre para mí, me ha enseñado a que debo luchar hasta alcanzar las metas que me proponga, sin ella no hubiese sido posible nada de lo que soy ahora.

Es grato mencionar a mis hermanos, a mi abuelita y a cada miembro de mi familia materna que son a fuente de mi inspiración siempre eh sentido el apoyo incondicional de ellos.

Y finalmente quiero dedicarle este logro mi novio que es el amor de mi vida, que gracias a sus consejos hicieron que no dé el brazo a torcer en este largo camino, siempre me impulsó para que siga adelante a pesar de los obstáculos que se me interponían.

Joselyne Gabriela García Barrera

Dedicatoria

Este proyecto va dedicado a mis padres pero muy especialmente a mi mamá que siempre me apoyó en todo momento, sin dejar de creer en mí y en la metas que me he propuesto en el transcurso de mi vida y ha sido siempre mi guía y la persona que me inspira cada día para ser persona mejor, a mi novio por ser mi amigo, mi compañero y uno de mis pilares fundamentales para seguir adelante; a mi familia en general que nunca dudó de mí ni del esfuerzo que puse cada momento para poder culminar este proyecto y por último pero no menos importante quiero dedicar todo mi trabajo, esfuerzo y dedicación a Dios que siempre me ha acompañado, escuchó siempre mis oraciones y se hacía presente cuando más lo necesitaba, Él mi motor de vida y mi mayor inspiración.

Blanca Stephanye Delgado Pijal

Agradecimiento

A nuestra directora de tesis, por la colaboración prestada en cada requerimiento que solicitábamos.

Al Ing. Olmedo Aguayo cuyo apoyo fue crucial para el desarrollo de este proyecto, por su disposición de ayuda.

A cada uno de mis maestros que aportaron con sus conocimientos a través de este tiempo.

Joselyne Gabriela García Barrera

Agradecimiento

Agradezco a la Universidad Politécnica Salesiana porque desde un principio me abrió sus puertas y me mostró un mundo nuevo lleno de conocimientos al cual lograron poner al alcance de mis manos para lograr ser una gran profesional.

A mis maestros que con su paciencia y mayor dedicación compartieron toda su sabiduría, nos ayudaron a tener un mayor desenvolvimiento durante las clases y lograr prepararnos para lo que sería un día nuestro mundo laboral.

A mi tutora por ser quien guíe el trabajo realizado a pesar de las diferentes calamidades y dificultades que se hayan presentado durante todo este tiempo.

Blanca Stephanye Delgado Pijal

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE GRÁFICOS

RESUMEN

Durante décadas y a medida que sigue transcurriendo el tiempo las tecnologías de información han ido desarrollándose y con ellas también todo tipo de amenazas y riesgos a la cual se encuentra expuesta en gran nivel la información específicamente.

Este proyecto se origina con la idea de poder lograr aplicar mejores técnicas de seguridad en la Unidad Educativa Domingo Comín, haciendo un análisis de todos los medios por el cual circulan y manipulan los datos e información del colegio, los cuales pueden ser críticos como no; sin embargo una de las metas es poder contribuir con la mejora continua de todos los procedimientos que llevan a cabo dentro de la Institución.

Tomando como base la norma NTE INEN-ISO/IEC 27001:2011 se realizará un análisis paso a paso de los diferentes campos que contiene la norma y bajo sus procedimientos y controles a seguir obtener el levantamiento de información necesario y más apropiada para poder lograr los objetivos como son principalmente la inclusión de controles, gestionar y mejorar la seguridad de la información y lograr que todo el personal concientice la visión de lo que se desea logar al cumplir con dicho proyecto.

Es importante que durante el análisis que se va a realizar, se vaya identificando los recursos informáticos que presenten más vulnerabilidad y eso se podrá visualizar durante la revisión de los contenidos que se irá desarrollando ya que dependiendo de ello al final del proyecto se tomará en cuenta las medidas de prevención necesarias para con ello lograr obtener que el colegio pueda brindar un mejor servicio académico tomando en consideración los principio de integridad, disponibilidad y confidencialidad que es para un usuario final la mejor manera de percibir el funcionamiento correcto de un sistema.

ABSTRACT

For decades, and as time continues progressing the information technologies have been developed with it and also all kind of threats and risks which the information is exposed to.

This project starts with the idea of being able to implement better security techniques in Domingo Comin High School's system, doing an analysis of all the process (circulation and manipulation) related to the information of the college, which may not be as critical; however, one of the goals is about our contribution with the continuous improvement of all the procedures carried out within the institution.

Based on the standard NTE INEN-ISO/IEC 27001:2011, it will allow us to go carrying out a step-by-step analysis of the different fields that contains the rule and under its procedures and controls continue to obtain the lifting of appropriate and necessary information in order to achieve the objectives as the inclusion of controls, manage and improve the security of the information and ensure that all staff understand about the vision of what we want to accomplish with our project.

It is important that during the analysis we identified the computing resources which shows more vulnerability, it will be reflected during the review of each content that will be developed; depending on this, at the end of our project we will consider some preventive measures to help the college to provide a better academic service taking into account some values like integrity, availability and confidentiality that is the best way to perceive the correct operation of a system for the final costumer.

Introducción

Para el análisis del proyecto de tesis se inició con un levantamiento de información logrando recopilar datos de la Unidad Educativa Salesiana Domingo Comín, como por ejemplo los problemas que podrían ser más persistentes en la Institución, además de cuáles serán mis objetivos para lograr el mejor resultado con el fin de que se beneficien todos los empleados.

Para el siguiente capítulo se encontrará un marco teórico completo de los principales temas y conceptos para lo cual se obtendrá una mejor percepción del enfoque del proyecto.

Continuamente se da a conocer cómo está el marco metodológico del proyecto donde se especifica los tipos de investigación a utilizar, los métodos de investigación; a su vez cómo se realizó la recopilación y análisis de datos y por último la identificación de las variables e indicadores, seguido del cálculo de la muestra.

En el capítulo a continuación ya se encuentra información más detallada de la Institución como funciones departamentales, su arquitectura de hardware, distribución de equipos y la justificación más detallada de los diferentes riesgos a los que está expuesta la Unidad Educativa y se visualiza gráficamente los resultados obtenidos de las técnicas de recolección de datos que se utilizaron para el proyecto.

Luego se expondrá una pequeña redacción muy específica de conclusiones respecto al análisis en general y a su vez un listado de recomendaciones respecto a los activos con mayor vulnerabilidad.

Para finalizar se implantó una propuesta clara y precisa como parte de una iniciativa para lograr disminuir los riesgos encontrados especificando detalladamente la justificación de la misma, sus objetivos, así también como un análisis de factibilidad, fundamentación y la metodología que se implementará para dicha propuesta.

CAPÍTULO 1

PLANTEAMIENTO DEL PROBLEMA

La Unidad Educativa Salesiana Domingo Comín nace de la percepción que se tenía ante la pobreza, falta de educación, el trabajo infantil, entre otros factores que perjudican al desarrollo psicológico e intelectual de la niñez y la juventud, así fue entonces que inició el compromiso por cambiar y mejorar la estabilidad de ellos.

Todo el desarrollo, motivación y colaboración de varias personas implicadas dieron lugar a lo que hoy es una gran institución que solo inicio como un grupo de ayuda, luego la Escuela Popular Don Bosco, por su pronta y afirmada respuesta con las expectativas que iba llenando como ya un centro educativo llego a tomar el nombre de Domingo Comín; finalmente por el nivel educacional y como resultado al acuerdo con la Subsecretaría Regional del Ecuador queda denominada como Unidad Educativa Salesiana Fisco-Misional Domingo Comín. Ahora en tiempos más actuales se busca mucho más allá de la excelencia académica también se buscar priorizar los procesos que conllevan a distinguir el nombre de la Institución.

Durante un recorrido y revisión en la arquitectura tecnológica en los establecimientos de la Unidad Educativa y luego de una breve investigación se determinaron situaciones a las cuales se encuentran expuestos; por ejemplo, si se refiere al control sobre los accesos a las diferentes áreas como laboratorios, oficinas o centro de datos y a la información crítica que se maneja no se posee ningún control de seguridad.

En cuanto a gestión de activos hay cierto conjunto de información que se maneja en parte de forma manual como RRHH, financiera, académica; además el control de inventario se maneja únicamente de forma manual, teniendo así a disposición de cualquiera que intente extraer los archivos encarpetados, además de no poseer políticas o controles de seguridad para acceder a las mismas hace, esto aún más vulnerable cada uno de los activos que manejan información.

Han sucedido ciertas calamidades más que nada con el servidor, y a pesar de ello no cuentan con ningún plan de contingencia en caso de accidentes para la continuidad del negocio que en este caso tiene fines académicos.

1.1 Formulación del problema

¿De qué manera se puede optimizar el uso adecuado de información y servicios informáticos para reducir los riesgos que amenazan al personal de la Unidad Educativa Salesiana Domingo Comín?

¿Qué mecanismos se podrían crear para identificar las vulnerabilidades que presentan los activos de información?

¿Qué medidas se podrían tomar para asegurar que todo el personal haga uso adecuado de la información de los sistemas?

¿Cómo garantizar el uso adecuado de los recursos informáticos que se utilizan dentro de la Unidad Educativa?

¿De qué manera se puede proteger los recursos informáticos de problemas que afecten la disponibilidad de los mismos?

1.2 Objetivo

1.2.1 Objetivo general

Determinar los procedimientos adecuados para lograr optimizar el uso adecuado de información y servicios informáticos que reduzcan los riesgos que amenazan al personal de la Unidad Educativa Salesiana Domingo Comín bajo la norma técnica ecuatoriana.

1.2.2 Objetivos específicos

Establecer los mecanismos necesarios para identificar las vulnerabilidades que presentan los activos de información.

Determinar las prácticas adecuadas para asegurar que todo el personal haga uso adecuado de la información de los sistemas.

Identificar los controles para mejorar el uso adecuado de los recursos informáticos que se utilizan dentro de la Unidad Educativa.

Poner en conocimiento las mejores prácticas para proteger los recursos informáticos de problemas que afecten la disponibilidad de los mismos.

1.3 Justificación

Con la ayuda del análisis de requisitos de tecnología de información para la aplicación de técnicas de seguridad se podrá minimizar el nivel de riesgo de pérdida de información al igual que los posibles incidentes que se pueden ocasionar dentro de la Unidad Educativa Salesiana Domingo Comín.

El mal uso de información confidencial, de recursos informáticos y la falta de disponibilidad de los mismos puede afectar a todos los procesos que se manejen en la institución, incluyendo los servicios prestados que brindan.

Es fundamental incluir al personal que labora en la Institución y se concientice qué tan importante es poder involucrarse y familiarizarse con buenas prácticas respecto a un mejor control de información y a su vez de los diferentes recursos informáticos.

Los beneficios que aporta este proyecto será lograr obtener un mayor control en los accesos al portal de la Unidad Educativa, mantener más seguros los respaldos que se efectúen en las áreas críticas teniendo así como beneficiarios a los docentes, estudiantes, padres de familia y personal técnico - administrativo ya que están

directamente vinculados con los activos que presentan vulnerabilidades y riesgos informáticos dentro de la Unidad Educativa Salesiana Domingo Comín.

CAPÍTULO 2

MARCO TEÓRICO

2.1 ISO e IEC

ISO (Organización Internacional de Normalización) e IEC (Comisión Electrotécnica Internacional) constituyen el sistema especializado para la normalización a nivel mundial. Los organismos nacionales que son miembros de ISO o IEC participan en el desarrollo de las normas internacionales a través de comités técnicos establecidos por las organizaciones respectivas para realizar acuerdos en campos específicos de la actividad técnica. Los comités técnicos de ISO e IEC colaboran en los campos de interés mutuo. Otras organizaciones internacionales, gubernamentales y no gubernamentales, en colaboración con ISO e IEC, también toman parte en el trabajo. (ISO/IEC 17023:2013, 2013)

2.2 ISO 27001

La norma ISO/IEC 27001 originado en el año 1995, el cual es un estándar de buenas prácticas ISO, que ha ido evolucionando. Para entender de manera general pero clave el concepto de un ISO 27001, podemos explicarlo que está dirigida para la organización del diseño, implantación, mantenimiento de un conjunto de procesos para así lograr gestionar de manera eficiente la seguridad de la información, con el propósito de asegurar los confidencialidad, integridad y disponibilidad de los activos de información minimizando a su vez los riesgos a los que está expuesta la seguridad de la información. Esta definición se origina de (LEON, 2010), el mismo que explica los conceptos de:

2.2.1 Confidencialidad de datos

Esto implica que en una organización los colaboradores no pueden compartir, divulgar o dejar al alcance de terceras personas toda documentación que posea datos de gran importancia, por ello nace la importancia de mantenerla segura y libre de los varios riesgos a los que está expuesta.

2.2.2 Integridad de datos

Se define como la exactitud e integridad de datos dentro de una organización, estos no pueden, por ningún motivo ser alterados o manipulados para ningún fin.

2.2.3 Disponibilidad de datos

Característica que implica el acceso y utilización de la información de una organización al tiempo que un usuario o entidad autorizada la requiera y sea para fines que no perjudiquen a dicha empresa.

2.2.4 SGSI

Es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información o también lo podemos conocer como ISMS el cual define en el idioma inglés en Information Security Management System.

Un sistema de gestión de seguridad de la información es un sistema de análisis y administración que se encarga de la información de la seguridad. El término es utilizado principalmente por la ISO/IEC 27001. Este debe implementarse de tal manera que su proceso sea conocido para toda la organización. Por ello debe ser forma sistemática y documentado.

2.2.5 Información

La información es un activo conformado por conjuntos de datos que son de gran valor que se encuentran en poder de una organización, independientemente en la forma en la que se manipule, guarde o transmita. Estos datos pueden en archivos físicos o digitales; por tal motivo necesita priorizarse su seguridad ya que está expuesta a muchos riesgos, amenazas y vulnerabilidades.

2.3 Enfoque por proceso

La norma ISO/IEC 27001 adopta un enfoque por proceso para lograr la creación, implementación, operación, supervisión, mantenimiento y mejora del SGSI de una organización. Una organización siempre debe tener definidas un conjunto de actividades para poder funcionar con mayor eficacia.

Un proceso se puede considerar al conjunto de actividades que utilicen recursos, los mismos que gestionándolos puedan transformar ciertos elementos de entrada en elementos de salida. Entonces para resumir, un enfoque por procesos es la aplicación de un conjuntos de procesos los cuales que se identifican, interaccionan y gestionan. (INEN, 2011)

2.4 Origen e historia de la norma ISO 27001

La norma ISO 27001 como la conocemos en la actualidad, ha pasado un proceso evolutivo de varios estándares que se relacionan con la seguridad de la información, por referencia de (ISOTools Excellence, 2013) lo podemos presentar de la siguiente manera:

*1995- BS 7799-1:1995: Mejores prácticas para ayudar a las empresas británicas a administrar la Seguridad de la Información. Eran recomendaciones que no permitían la certificación ni establecía la forma de conseguirla.

*1998 – BS 7799-2:1999: Revisión de la anterior norma. Establecía los requisitos para implantar un Sistema de Gestión de Seguridad de la Información certificable.

*1999 – BS 7799-1:1999: Se revisa.

*2000 – ISO/IEC 17799:2000: La Organización Internacional para la Estandarización (ISO) tomó la norma británica BS 7799-1 que dio lugar a la llamada ISO 17799, sin experimentar grandes cambios.

*2002 – BS 7799-2:2002: Se publicó una nueva versión que permitió la acreditación de empresas por una entidad certificadora en Reino Unido y en otros países.

*2005 – ISO/IEC 27001:2005 e ISO/IEC17799:2005: Aparece el estándar ISO 27001 como norma internacional certificable y se revisa la ISO 17799 dando lugar a la ISO 27001:2005.

*2007 – ISO 17799: Se renombra y pasa a ser la ISO 27002:2005.

*2007 – ISO/IEC 27001:2007: Se publica la nueva versión.¨

*2009 – Se publica un documento adicional de modificaciones llamado ISO 27001:2007/1M:2009.

2.5 Beneficios que aporta la norma ISO 27001

En base a (ceeisec, 2014) y con referencia de otros proyectos realizados se puede mencionar los siguientes beneficios:

* Demostrar la efectividad y garantía de los controles internos de una organización, además de la continuidad de las actividades que manejan comercialmente.

* Demostrar una ventaja competitiva al garantizar a sus clientes el cumplimiento de los objetivos estratégicos de la empresa.

* Demostrar a los clientes y usuarios en general lo importante que es el resguardo de la información ya que es un activo primordial que debe poseer el mayor nivel de seguridad.

* Demostrar el compromiso que tiene la cúpula directiva de su organización con respecto a la seguridad de la información.

* Realizar evaluaciones de forma periódica permitirá controlar y supervisar el rendimiento y la mejora de los procesos que maneja una empresa.

* Permite demostrar que todos los riesgos de una organización puedan ser debidamente identificados, que se les dé un respectivo seguimiento y gestión desde el momento en que se identifican procesos, procedimientos y ciertas protecciones para resguardo de la información.

2.6 Círculo de Deming

Conocido también como ciclo PDCA comprende la lógica de mejoramiento de los sistemas de administración de la calidad. El círculo de Deming, creado en el decenio de 1950, armoniza esta gestión del progreso. (Gillet Goinard, 2014)

Las 4 etapas del PCDA son:
-Plan (planeación)
-Do (realización, puesta en práctica)
-Check (revisión, control, verificación)
-Act (acción, ajuste)

2.6.1 ¿Cómo adaptarse al círculo de Deming?

Según (ISO27000, 2012) la elaboración de este ciclo requiere de cuidado, análisis, seguimiento y dedicación como se presenta en la siguiente explicación:

Plan (planeación)

Figura 1: Etapa de planificación
Fuente: (ISO27000, 2012)

A continuación se describirá las características de la etapa de planificación como se especifica en la figura 1:

• Definir alcance del SGSI: en función de características del negocio, organización, localización, activos y tecnología, definir el alcance y los límites del SGSI (el SGSI no tiene por qué abarcar toda la organización; de hecho, es recomendable empezar por un alcance limitado).

• Definir política de seguridad: que incluya el marco general y los objetivos de seguridad de la información de la organización, tenga en cuenta los requisitos de negocio, legales y contractuales en cuanto a seguridad, esté alineada con la gestión de riesgo general, establezca criterios de evaluación de riesgo y sea aprobada por la Dirección. La política de seguridad es un documento muy general, una especie de "declaración de intenciones" de la Dirección, por lo que no pasará de dos o tres páginas.

• Definir el enfoque de evaluación de riesgos: definir una metodología de evaluación de riesgos apropiada para el SGSI y las necesidades de la organización, desarrollar criterios de aceptación de riesgos y determinar el nivel de riesgo aceptable. Existen muchas metodologías de evaluación de riesgos aceptadas internacionalmente, la organización puede optar por una de ellas, hacer una combinación de varias o crear la suya propia. ISO 27001 no impone ninguna ni da indicaciones adicionales sobre cómo definirla (en el futuro, ISO 27005 proporcionará ayuda en este sentido). El riesgo nunca es totalmente eliminable ni sería rentable hacerlo, por lo que es necesario definir una estrategia de aceptación de riesgo.

• Inventario de activos: todos aquellos activos de información que tienen algún valor para la organización y que quedan dentro del alcance del SGSI.

• Identificar amenazas y vulnerabilidades: todas las que afectan a los activos del inventario.

• Identificar los impactos: los que podría suponer una pérdida de la confidencialidad, la integridad o la disponibilidad de cada uno de los activos.

• Análisis y evaluación de los riesgos: evaluar el daño resultante de un fallo de seguridad (es decir, que una amenaza explote una vulnerabilidad) y la probabilidad de ocurrencia del fallo; estimar el nivel de riesgo resultante y determinar si el riesgo es aceptable (en función de los niveles definidos previamente) o requiere tratamiento.

• Identificar y evaluar opciones para el tratamiento del riesgo: el riesgo puede reducido (mitigado mediante controles), eliminado (p. ej., eliminando el activo), aceptado (de forma consciente) o transferido (p. ej., con un seguro o un contrato de outsourcing).

• Selección de controles: seleccionar controles para el tratamiento el riesgo en función de la evaluación anterior. Utilizar para ello los controles del Anexo A de ISO 27001 (teniendo en cuenta que las exclusiones habrán de ser justificadas) y otros controles adicionales si se consideran necesarios.

• Aprobación por parte de la Dirección del riesgo residual y autorización de implantar el SGSI: hay que recordar que los riesgos de seguridad de la información son riesgos de negocio y sólo la Dirección puede tomar decisiones sobre su aceptación o tratamiento. El riesgo residual es el que queda, aún después de haber aplicado controles (el "riesgo cero" no existe prácticamente en ningún caso).

• Confeccionar una Declaración de Aplicabilidad: la llamada SOA (Statement of Applicability) es una lista de todos los controles seleccionados y la razón de su selección, los controles actualmente implementados y la justificación de cualquier control del Anexo A excluido. Es, en definitiva, un resumen de las decisiones tomadas en cuanto al tratamiento del riesgo.

Do (realización, puesta en práctica)

Figura 4: Etapa de implementación
Fuente: (ISO27000, 2012)

A continuación se describirá las características de la etapa de implementación como se especifica en la figura 2:

• Definir plan de tratamiento de riesgos: que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.

• Implantar plan de tratamiento de riesgos: con la meta de alcanzar los objetivos de control identificados.

• Implementar los controles: todos los que se seleccionaron en la fase anterior.

• Formación y concienciación: de todo el personal en lo relativo a la seguridad de la información.

• Desarrollo del marco normativo necesario: normas, manuales, procedimientos e instrucciones.

• Gestionar las operaciones del SGSI y todos los recursos que se le asignen.

• Implantar procedimientos y controles de detección y respuesta a incidentes de seguridad.

Check (revisión, control, verificación)

Figura 7: Etapa de seguimiento
Fuente: (ISO27000, 2012)

A continuación se describirá las características de la etapa de seguimiento como se especifica en la figura 3:

• Ejecutar procedimientos y controles de monitorización y revisión: para detectar errores en resultados de procesamiento, identificar brechas e incidentes de seguridad, determinar si las actividades de seguridad de la información están desarrollándose como estaba planificado, detectar y prevenir incidentes de seguridad

mediante el uso de indicadores y comprobar si las acciones tomadas para resolver incidentes de seguridad han sido eficaces.

• Revisar regularmente la eficacia del SGSI: en función de los resultados de auditorías de seguridad, incidentes, mediciones de eficacia, sugerencias y feedback de todos los interesados.

• Medir la eficacia de los controles: para verificar que se cumple con los requisitos de seguridad.

• Revisar regularmente la evaluación de riesgos: los cambios en la organización, tecnología, procesos y objetivos de negocio, amenazas, eficacia de los controles o el entorno tienen una influencia sobre los riesgos evaluados, el riesgo residual y el nivel de riesgo aceptado.

• Realizar regularmente auditorías internas: para determinar si los controles, procesos y procedimientos del SGSI mantienen la conformidad con los requisitos de ISO 27001, el entorno legal y los requisitos y objetivos de seguridad de la organización, están implementados y mantenidos con eficacia y tienen el rendimiento esperado.

• Revisar regularmente el SGSI por parte de la Dirección: para determinar si el alcance definido sigue siendo el adecuado, identificar mejoras al proceso del SGSI, a la política de seguridad o a los objetivos de seguridad de la información.

• Actualizar planes de seguridad: teniendo en cuenta los resultados de la monitorización y las revisiones.

• Registrar acciones y eventos que puedan tener impacto en la eficacia o el rendimiento del SGSI: sirven como evidencia documental de conformidad con los requisitos y uso eficaz del SGSI.

Act (acción, ajuste)

Figura 10: Etapa de ajuste
Fuente: (ISO27000, 2012)

A continuación se describirá las características de la etapa de ajuste como se especifica en la figura 4:

• Implantar mejoras: poner en marcha todas las mejoras que se hayan propuesto en la fase anterior.

• Acciones correctivas: para solucionar no conformidades detectadas.

• Acciones preventivas: para prevenir potenciales no conformidades.

• Comunicar las acciones y mejoras: a todos los interesados y con el nivel adecuado de detalle.

• Asegurarse de que las mejoras alcanzan los objetivos pretendidos: la eficacia de cualquier acción, medida o cambio debe comprobarse siempre.

Objetivos del círculo de Deming

- Mejorar la calidad percibida por los clientes
- Reducir las disfuncionalidades internas
- Optimizar los costos internos y externos por falta de calidad

2.7 Seguridad Informática

Se puede definir como un conjunto de procedimientos, dispositivos y herramientas encargadas de asegurar la integridad, disponibilidad y privacidad de la información en un sistema informático e intentar reducir las amenazas que pueden afectar al mismo. (Cervantes Sanchez & Ochoa Ovalles, 2012)

2.7.1 Tipos de seguridad informática

Según (Alegre Ramos & Garcia-Cervigon Hurtado, 2011) es primordial que dentro de una organización identifiquemos cuáles son los problemas principales que puede presentar un sistema informático en cuanto al tema de seguridad, estos se catalogan dependiendo de sus objetivos. Además deja mencionado que la seguridad informática la podemos dividir en:

2.7.1.1 Seguridad física

Se utiliza para proteger el sistema informático utilizando barreras físicas y mecanismos de control se empieza a proteger físicamente el sistema informático las amenazas físicas pueden ser provocadas por el hombre de forma accidental o voluntaria o bien de factores naturales como observamos en la figura 5.

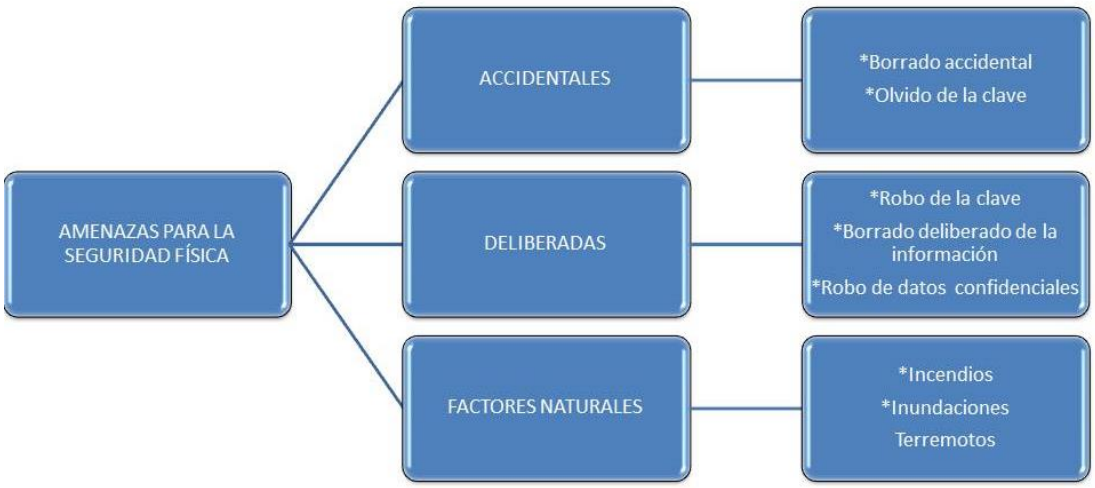

Figura 13: Seguridad física
Elaborado por: Las autoras

2.7.1.2 Seguridad lógica

Se encarga de asegurar la parte software de un sistema informático que se compone de todo lo que no es físico es decir, programas y los datos la seguridad lógica se encarga de controlar el acceso al sistema informático desde el punto de vista del software se realice correctamente y por usuarios autorizados ya sea dentro del sistema informático como desde fuera es decir, desde una red externa usando VPN dentro de la seguridad lógica tenemos una serie de programas o software como el sistema operativo que se debe encargar de controlar el acceso de los procesos o usuarios a los recursos del sistema; cada vez los sistemas operativos controlan más la seguridad del equipo informático ya sea por parte de un error, por el uso incorrecto del sistema operativo o del usuario o bien por el acceso no controlado físicamente o a través de la red como se muestra en la figura 6, es casi imposible que sea totalmente seguro pero se pueden tomar ciertas medidas para evitar daños a la información o a la privacidad.

Figura 16: Amenazas comunes
Elaborado por: Las autoras

2.7.2 Seguridad activa y pasiva

Son mecanismos o técnicas de seguridad que nos permitirán tener a los equipos informáticos más seguro según lo mencionan en (Cervantes Sanchez & Ochoa Ovalles, 2012) y las describe de la siguiente manera:

2.7.2.1 Seguridad activa

Sirve para evitar daños a los sistemas informáticos. Son tales como el empleo de contraseñas adecuadas, la encriptación de datos y el uso de software de seguridad informática.

Seguridad pasiva

Sirve para minimizar los efectos causados por un accidente. Son tales como el uso de un hardware adecuado y la realización de copias de seguridad.

2.7.3 Mecanismos de seguridad

En (Alegre Ramos & Garcia-Cervigon Hurtado, 2011, págs. 6-10) encontramos que un mecanismo de seguridad (también llamado herramienta de seguridad o control) es una técnica que se utiliza para implementar un servicio, es decir, es aquel mecanismo que está diseñado para detectar, prevenir o recobrarse de un ataque de seguridad. Los mecanismos de seguridad implementan varios servicios básicos de seguridad o combinaciones de estos servicios básicos. Los servicios de seguridad especifican que controles son requeridos y los mecanismos de seguridad especifican cómo deben ser ejecutados los controles y (Alegre Ramos & Garcia-Cervigon Hurtado, 2011, págs. 6-10) menciona los siguientes mecanismos:

2.7.3.1 Cifrado

Es el uso de algoritmos matemáticos para transformar datos en una forma inteligente.

2.7.3.2 Control de acceso

Una serie de mecanismos que refuerzan los derechos de acceso a los recursos, como por ejemplo el uso del directorio activo.

2.7.3.3 Relleno del tráfico

La inserción de bits en espacios en un flujo de datos para frustrar los intentos de análisis de tráfico.

2.7.3.4 Control de enrutamiento

Permite la selección de rutas físicamente seguras para determinar datos y permitirte los cambios de enrutamiento especialmente cuando se sospecha de una brecha de seguridad.

2.7.4 Sistemas de protección

Un sistema de protección para (Cervantes Sanchez & Ochoa Ovalles, 2012) es algo que toda empresa debe tener para evitar accidentes de todo tipo y así minimizar los posibles riesgos a la infraestructura o a la información que puedan ser causados por incendios o fallas eléctricas o cualquier otro riesgo, otro de los que pueden ser usados son los llamados sistemas contra incendios y además del uso de extintores y sistemas convencionales antincendios convencionales, hay otros tipo de sistemas más eficaces, como la inserción de gases nobles o la extracción de oxígeno, que preservan mejor los equipos para que no sean alcanzados por el fuego evitando así el contacto con el líquido de los extintores o el agua. Dentro de las ideas de (Cervantes Sanchez & Ochoa Ovalles, 2012) encontramos los siguientes ejemplos de sistemas de protección:

2.7.4.1 Sistemas de identificación

Un sistema de identificación es un método para el acceso al sistema informático, como a las instalaciones donde este se encuentre físicamente. El uso de técnicas y procedimientos se usan para controlar el acceso a las personas que quieran acceder al sistema o al usuario que accede localmente o de forma remota. Algunas de las herramientas destinadas a tal fin son: la firma electrónica, el certificado digital entre otras cosas.

2.7.4.2 Seguridad en el acceso al sistema informático

Es muy importante evitar el acceso no autorizado tanto al sistema informático como al recinto o lugar donde se encuentre ubicado, es una parte muy importante dentro de la seguridad y para eso existen los sistemas de protección.

Todas estas medidas de protección formaran parte de la seguridad activa, ya que se utilizan para evitar el acceso de un usuario no autorizado que podría comprometer tanto la privacidad como la integridad de la información contenida en el sistema informático.

2.7.4.3 Sistemas de control de acceso

Algunos sistemas de control de acceso pueden ser: guardias y cámaras de seguridad que son utilizados para evitar el acceso al edificio tanto exterior o interior y así controlar el acceso a lugares restringidos. El uso de llaves para acceder al edificio o a la habitación donde se encuentran los equipos, así como llaves para bloquear el equipo en sí. También se usan claves de acceso o contraseñas para entrar a lugares protegidos o cuentas de usuario. Los sistemas de contraseñas para entrar en un equipo informático son utilizados para que los sistemas de contraseñas sean correctos y cumplan su función.

La implementación de medidas de seguridad adecuadas para proteger a una empresa normal, representa un trabajo considerable pero no supone mayores problemas. Es una misión accesible para cualquier persona que disponga un buen nivel de competencia informática.

2.8 Conocer las amenazas potenciales

El pirateo, acceso no autorizado de un usuario ajeno a la empresa. Cuando un pirata obtiene acceso, incluso de nivel usuario puede llegar a modificar los datos o detener algunos servidores que podrían poner en riesgo la integridad de la empresa misma. Ningún tipo de atacante deberá obtener ni el más mínimo acceso al sistema de

la empresa porque conseguiría estropear algunos componentes estratégicos, tales como el servidor de correo o el sitio web. (Alegre Ramos & Garcia-Cervigon Hurtado, 2011, págs. 11-12)

La misma protección debe ser usada con los llamados virus, que se reproducen de manera más o menos autónoma y representan una de las amenazas más frecuentes en el interior de la empresa, debido a su variedad son muy difíciles de interceptar y se transmiten principalmente a través del correo electrónico o de las transferencias de archivos por internet. (Alegre Ramos & Garcia-Cervigon Hurtado, 2011, págs. 11-12)

2.9 Tipos de atacantes

Según (Alegre Ramos & Garcia-Cervigon Hurtado, 2011, págs. 19-23) los tipos de atacantes más comunes son:

2.9.1 Virus

Los llamados virus son programas autónomos que son hechos para reproducirse y difundirse de manera autónoma y sus principales características son: la manera en que se reproduce e infecta el sistema informático y las acciones mortíferas que realizara.

Algunas subcategorías de virus son los llamados gusanos (worm en inglés) es casi idéntico al virus clásico solo que el virus necesita una intervención manual para reproducirse y el gusano puede reproducirse de manera autónoma sin ningún tipo de intervención. Este otro llamado caballo de Troya (trojanhorse) es un virus inofensivo que disimula su aspecto nocivo tomando el aspecto externo de un programa inofensivo, incluso atractivo para el usuario. Típicamente se presenta como un juego o más insidiosamente como un programa antivirus.

2.9.1.1 Intercepción de datos confidenciales

Otro de los riesgos importantes que puede dañar a una empresa es la intercepción por parte de un tercero de datos confidenciales, es necesario tomar conciencia que en una conexión de internet normal el 99,9% de los datos que circulan no están cifrados por lo que pueden ser interceptados por cualquiera.

Es más una operación simple y al alcance de cualquier pirata. Existen muchos programas que permiten guardar y luego consultar todo lo que pasa por una red informática. Los datos se transmiten por la red de un ordenador, y así todos los ordenadores situados en la misma red los reciben de forma sistemática, cada ordenador mira la dirección del destinatario de este paquete de datos y lo compara con su propia dirección, si ambas direcciones no corresponden, el ordenador simplemente lo ignora, solo la maquina a la que este destinado el paquete de datos lo tendrá en cuenta.

2.10 Tácticas de protección

Analizando las tácticas más puntuales y de mejora inmediata se encontró que según (Gallinger, 2011) se puede obtener métodos activos y métodos pasivos los cuales se explican a continuación:

2.10.1 Métodos activos

Antivirus

Son programas que tratan de descubrir las trazas que ha dejado un software malicioso, para detectarlo y eliminarlo, y en algunos casos contener o parar la contaminación. Tratan de tener controlado el sistema mientras funciona parando las vías conocidas de infección y notificando al usuario de posibles incidencias de seguridad.

Filtros de archivos

Consiste en generar filtros de archivos dañinos si la computadora está conectada a una red. Estos filtros pueden usarse, por ejemplo, en el sistema de correos o usando técnicas de firewall. En general, este sistema proporciona una seguridad donde no se requiere la intervención del usuario, puede ser muy eficaz, y permitir emplear únicamente recursos de forma más selectiva.

2.10.2 Métodos pasivos

Evitar introducir al equipo medios de almacenamiento removibles que se sospechen estar infectados.

Evitar introducir almacenamiento removible en máquinas que se sospechen infectadas.

No instalar software "pirata". Evitar programas que incluyan crack, generadores de claves, números serie, etc.

Evitar descargar software gratis de Internet de sitios que no demuestren información clara de su actividad y de sus productos o servicios.

No abrir mensajes provenientes de una dirección electrónica desconocida, o con alguna promoción muy tentadora, o con imágenes o nombres muy sugerentes.

No aceptar e-mails de desconocidos. Y si es de contactos conocidos, observar bien el idioma, el léxico utilizado en el mensaje, la hora en que se envió, etc.

Mantener el SO y las aplicaciones actualizadas, ya que suelen publicarse parches de seguridad resolviendo problemas de vulnerabilidad ante inminentes ataques.

Realizar copias de seguridad y tratar de automatizar la recuperación del sistema, es la mejor alternativa ya que nunca se está 100% libre de infección.

Mantener la información centralizada ayudará a restaurar los datos en caso de infección.

CAPÍTULO 3

MARCO METODOLÓGICO

3.1 Tipos de investigación

Durante el proceso de desarrollo para la elaboración del proyecto se tomarán en cuenta varios tipos de investigación los cuales son:

3.1.1 Investigación de campo

Para una mejor percepción y análisis de la situación se necesita visitar algunos días la Unidad Educativa y observar de primera mano las diferentes situaciones que están experimentando para lograr involucrarnos mucho más con el personal y los diferentes procesos que se desempeñan, obteniendo así una mejor interacción con fuentes viables.

3.1.2 Investigación descriptiva

Mediante este tipo de investigación se logra indagar y describir de forma más precisa del fenómeno de estudio, ayudando a reconocer cuáles son los indicadores que ayudan a definir las razones por las que se generan inconvenientes en ciertos procesos, además de la frecuencia con la que se presentan y quienes se relacionan con los mimos.

3.1.3 Investigación explicativa

Con el uso de este tipo de investigación se lleva describir las razones por las que se presentan varias irregularidades además de observar y registrar las diferentes consecuencias que ha traído consigo el fenómeno ocurrido dentro de la Unidad Educativa Salesiana Domingo Comín.

3.1.4 Investigación no experimental

Puesto que no es posible modificar ni manipular los hechos deliberadamente, este tipo de investigación ayuda a observar y a poder medir el alcance del fenómeno de estudio, con el fin de poder analizarlos y encontrar o proponer soluciones a los problemas actualmente corridos.

3.2 Técnicas de recolección de datos

Para el desarrollo del proyecto de tesis se utilizarán varias técnicas de recolección de datos que ayudarán a facilitar el análisis del fenómeno de estudio, entre ellos están:

La observación: Se trata de una técnica de recolección de datos que tiene como propósito explorar y describir ambientes, esto implica adentrarse en profundidad, en situaciones sociales y mantener un rol activo, pendiente de los detalles, situaciones, sucesos, eventos e interacciones.

La entrevista: Es la comunicación establecida entre el investigador y el sujeto de estudio a fin de obtener respuestas verbales a las interrogantes planteadas sobre el problema propuesto.

La encuesta: Es un procedimiento de investigación en el que el investigador busca recopilar datos por medio de un cuestionario de preguntas previamente diseñado.

Datos estadísticos: Un dato estadístico es cada uno de los valores que se han obtenido al realizar un estudio estadístico.

Revisiones documentales: Es una técnica de revisión y de registro de documentos que fundamenta el propósito de la investigación y permite el desarrollo del marco teórico y/o conceptual, que se inscriben el tipo de investigación exploratoria, descriptiva, etnográfica, teoría fundamental, pero que aborda todo paradigma investigativo.

Conversatorio con expertos: Los conversatorios son concebidos como una herramienta de encuentro que permiten focalizar la reflexión en un tema prioritario en la Región, a partir de la reunión de varios teóricos, intelectuales o expertos que elaboran un análisis, dan perspectivas e ideas para el mejoramiento del desarrollo de la misión.

3.3 Plan de procesamiento y análisis de datos

Para desarrollo del proyecto utilizaremos ciertos mecanismos para el plan de procesamiento y análisis de datos que nos servirán para lograr tener un mejor repositorio de información. Las técnicas que utilizaremos son las siguientes:

3.3.1 Experimentación

Esta técnica nos ayuda a identificar variables del objeto de estudio ayudándonos a localizarlos dentro de los parámetros correctos refiriéndonos al lugar y ambiente en la cual se desarrolla el problema, a su vez se irá descartando todo aquello que no se involucre directamente con el proceso.

3.3.2 Validación

Por medio de la validación se organizan las variables que re recolecten de la experimentación y se las clasificará para así dar lugar a indicadores concisos y valederos con los que se trabajará en el desarrollo del análisis.

3.3.3 Análisis

Mediante el análisis podremos ya concientizar y obtener el detalle de qué métodos de investigación se realizan, puesto que nos permite la identificación de los objetos del problema; obtendremos así una mejor idea de que mecanismos de control de llevaran a cabo para la mejoras de los procesos de la Institución.

3.4 Métodos de investigación

Durante el proceso de la investigación se utilizarán los siguientes métodos de investigación:

3.4.1 Analítico

Utilizaremos este método porque mediante su uso nos ayuda a destacar y agrupar los diferentes componentes que se incluirán como mecanismos de control para la Unidad Educativa Salesiana Domingo Comín.

El método analítico mediante su buen uso y al exponer una mejor apreciación y entendimiento de los fenómenos ocurridos se convierte en además, una herramienta que sintetizará lo anteriormente analizado.

Mediante el uso de este método se le incluirá un análisis por medio del método deductivo ya que al comenzar en un campo tan amplio pata la investigación, este nos facilitara ir de temas o problemas tan generalizados y concentrarnos en qué nos interesa realmente y en ciertos fenómenos en particular.

3.5 Variables e indicadores

Variables Dependientes:

- Obtención de informes de los procesos actuales
- Percepción de usuarios de los sistemas de gestión
- Identificación de amenazas y vulnerabilidades

Variables independientes:

- Gestión de procesos del área de Sistemas

Tabla 1: Matriz de operacionalización de variables dependientes

VARIABLE	DEFINICIÓN CONCEPTUAL	DIMENSIONES	INDICADORES
Obtención de informes de los procesos actuales	Con el conocimiento de sus procesos se puede estimar el alcance del análisis.	Tiempo de recolección	Tiempo que se demore la recolección de datos durante si análisis y procesamiento.
		Clasificación de información viable de los informes y procesos	-Categoría 1 los datos de mayor importancia para el análisis. -Categoría 2 los que se podrían considerar durante el análisis. - Categoría 3 los que dejarán fuera del análisis
Percepción de usuarios de los sistemas de gestión	La colaboración y aceptación del usuario interno y externo permitirá la inclusión de mejores prácticas académicas.	Aceptación del personal	-El nivel de información que brinden. -Cuanto predisposición se dé por parte de ellos
Identificación de amenazas y vulnerabilidades	Amenaza se entiende como un daño o acto no ilícito que perjudicará a alguien en un futuro y la vulnerabilidad es el estado disminuido de protección ante un suceso amenazante;	Costo de daños	-Cantidad de dinero invertido en herramientas de mal funcionamiento. -Nivel de economía para absorber nuevas disposiciones y todo lo que involucre

	ambas nos ayudarán a enfocarnos al trabajo esperado.	Clasificación de amenazas	-Nivel alto, amenazas no contraladas y sin nivel de protección. -Nivel medio, amenazas no controladas con mecanismos actuales. -Nivel bajo, amenazas controladas pero no debidamente.

Elaborado por: Las autoras

Tabla 2: Matriz de operacionalización de variables independientes

VARIABLE	DEFINICIÓN CONCEPTUAL	DIMENSIONES	INDICADORES
Gestión de procesos del área de Sistemas	Análisis y seguimiento de tareas o funciones que competan y se relacionen directamente con el área.	Hardware	Funcionabilidad correcta de equipos informáticos.
		Software	-Disponibilidad de herramientas. -Continuidad operacional del colegio. -Eficiencia, completitud y rapidez al generar reportes

Elaborado por: Las autoras

3.6 Población y muestra

3.6.1 Población

Población, es un conjunto de todos los elementos que estamos estudiando, acerca de los cuales intentamos sacar conclusiones.

Se ha considerado como población a la cantidad de usuarios que utilizan un equipo informático ya que ellos se verán directamente beneficiados con los tiempos de respuesta para solucionar sus necesidades de TI, en este caso la Unidad Educativa Salesiana "Domingo Comín" en la que se implementará la solución cuenta con un aproximado de 100 usuarios.

3.6.2 Muestra

La muestra es un subconjunto de la población.

Para calcular el tamaño de la muestra suele utilizarse la siguiente fórmula:

$$n = \frac{N\sigma^2 Z^2}{(N-1)e^2 + \sigma^2 Z^2}$$

Donde:

n = el tamaño de la muestra.

N = tamaño de la población.

$\sigma =$ Desviación estándar de la población que, generalmente cuando no se tiene su valor, suele utilizarse un valor constante de 0,5.

Z = Valor obtenido mediante niveles de confianza. Es un valor constante que, si no se tiene su valor, se lo toma en relación al 95% de confianza equivale a 1,96 (como más usual) o en relación al 99% de confianza equivale 2,58, valor que queda a criterio del investigador.

e = Límite aceptable de error muestral que, generalmente cuando no se tiene su valor, suele utilizarse un valor que varía entre el 1% (0,01) y 9% (0,09), valor que queda a criterio del encuestador.

Cálculo De La Fórmula

N= 120 Usuarios

Z= para un nivel de confianza del 99% =2,58

σ = 0.5%

e=5 % (0,05)

Reemplazando:

$$n = \frac{N\sigma^2 Z^2}{(N-1)e^2 + \sigma^2 Z^2}$$

$$n = \frac{120(0.5)^2(2.58)^2}{(120-1)0.05^2 + (0.5)^2(2.58)^2}$$

$$n = \frac{12(0.25)(6.6564)}{(119)(0.0025) + (0.25)\quad(6.6564)}$$

$$n = \frac{19.9692}{0.2975 + 1.6641}$$

$$n = \frac{19.9692}{1.9616}$$

n: 10.18 $\quad aproximado\, n = 10$

CAPÍTULO 4

ANÁLISIS Y RESULTADOS

4.1 Estructura de la comunidad educativa

4.1.1 Autoridades de la comunidad salesiana de Guayaquil

- Director
- Vicario
- Ecónoma
- Consejero

4.1.2 Autoridades seglares

- Rectora
- Vicerrector
- Inspector general
- Coordinador académico

Todos tienen la función de coordinar acertadamente el desarrollo estudiantil, de convivencia y pastoral de todo el plantel. La rectora y vicerrector (junto al coordinador académico) velan la parte administrativa y académica de la obra respectivamente, así mismo promueven procesos de capacitación a los docentes. El inspector general es designado por la rectora y es el encargado de asegurar un ambiente de disciplina y de orden que permita el normal desarrollo del proceso educativo en los grados y cursos a él designados.

4.1.3 Personal administrativo

En este grupo se encuentran los departamentos de colecturía, contabilidad, secretaría, consejería estudiantil, trabajo social, mantenimiento de instalaciones y equipos electrónicos, apoyo y relaciones públicas.

- Relacionista público y comunicación institucional
- Coordinador del área de informática
- Departamento de consejería estudiantil
- Contabilidad
- Secretaria (2)
- Coordinadora del GTH
- Auxiliar del GTH
- Pastoral

4.2 Funciones de los departamentos

4.2.1 Departamento de sistemas

Es el departamento que va a estar enfocado el mayor nivel de importancia. Las funciones que cumple son principalmente de brindar apoyo y soporte a todo el personal educativo, ayuda a gestionar todos los proyectos que la institución ejecuta en cuanto a áreas de laboratorios y estructura de cableado. Ayuda a controlar los accesos a las diferentes aplicaciones utilizadas, accesos a la red y manipulación de información.

4.2.2 Departamento de secretaría

Atienden las llamadas telefónicas que se realizan al colegio, además manejan la entrada de dinero; es decir los pagos que realizan los padres de familias ya sea de matrículas o pensiones sean puntuales o atrasadas.

4.2.3 Departamento de contabilidad

Programa y organiza todas las actividades contables de la Unidad Educativa, documenta los cobros y pagos que se realizan además ejecuta el registro adecuado de las transacciones que compete para los cuadres de balances contables y gastos.

4.2.4 Departamento Financiero

Este conlleva más responsabilidad ya que realiza los pagos a los profesores, personal administrativo y proveedores, además de administrar todos los recursos económicos.

Maneja todas las transacciones a nivel bancario, analiza, supervisa, crea y archivas todos los balances y estados financieros. Examina las diferentes bases de financiamiento y control de gastos.

4.2.5 Departamento de adquisiciones

Este departamento tiene funciones muy específicas como son el pedido de recursos que se necesitan en la Institución, gestión de pedidos y recibimiento y el inventario de los activos de toda la Unidad Educativa.

4.3 Arquitectura de hardware

4.3.1 Especificación de equipos informáticos

La composición de la red de la Unidad Educativa Domingo Comín está construida de la siguiente manera:

Tabla 3: Descripción general de equipos

	Descripción
No. Pcs.	42 Pcs. Por departamentos – 90 Pcs. Laboratorios
No. Servidores	5 en el DATA CENTER
Cableado	UTP cat. 6 – Fibra Optica
No. Switches	3 Data Center – 4 Laboratorios
Proveedor de Internet	Telconet

Elaborado por: Las autoras

- Los servidores se encuentras divididos en:
    - Firewall
    - PBX
    - Servidor web
    - Servidor de prueba
    - Servidor del sistema académico

- Cable UTP categoría 6 para los racks

- Enlaces de fibra óptica para los laboratorios

- Switches

- D-Link Web Smart Suitch (DGS-1224T – Puertos 24)
    - Configuración vía administración Web
    - 24 puertas UTP 10/100/1000 y 2 puertas 1000Mbps tipo SFP. La instalación de puertas SFP deshabilita la correspondiente puerta UTP Gigabit

- D-Link (DES-1024R – Puertos 24)
    - Switch Layer 2
    - Puertos 10/100Mbps
    - Backplane 2'6Gbps
    - Eslot de expansión por módulo opcional con 2 puertos en fibra óptica de 100Mbps

- TP-Link TL-SF1016 Fast Ethernet Switch (Puertos 16)
    - Innovadora tecnología de eficiencia energética para ahorrar energía hasta un 40%
    - 100% de tasa de datos de filtrado elimina todos los paquetes de error
    - Capacidad de conmutación 3.2Gbps

4.4 Distribución de PCs

Mediante la siguiente tabla podremos observar cómo están divididas las PCs en cada uno de los departamentos de la Institución, de los cuales se maneja inventario y se da soporte técnico.

Tabla 4: Distribución de máquinas por departamento

Departamentos	**No. Maquinas**
Rectorado	1
Vicerrectorado	1
Coordinación Académica	5
Pastoral	7
Consejería Estudiantil	5
Secretaria	2
Adquisición	1
Biblioteca	1
Departamento Educación Física	2
Sala profesores # 1	3
Sala profesores # 2	3
Apoyo y mantenimiento	1
Ajuste Mecánico	1
Departamento de Música	2
Departamento de Sistemas	5
Colecturía	2

Elaborado por: Las autoras

4.5 Análisis obtenido de las encuestas realizadas

Los siguientes gráficos mostrarán de manera directa y resumida el análisis obtenido de las encuestas realizadas a personal administrativo y docentes de la Unidad Educativa Salesiana Domingo Comín.

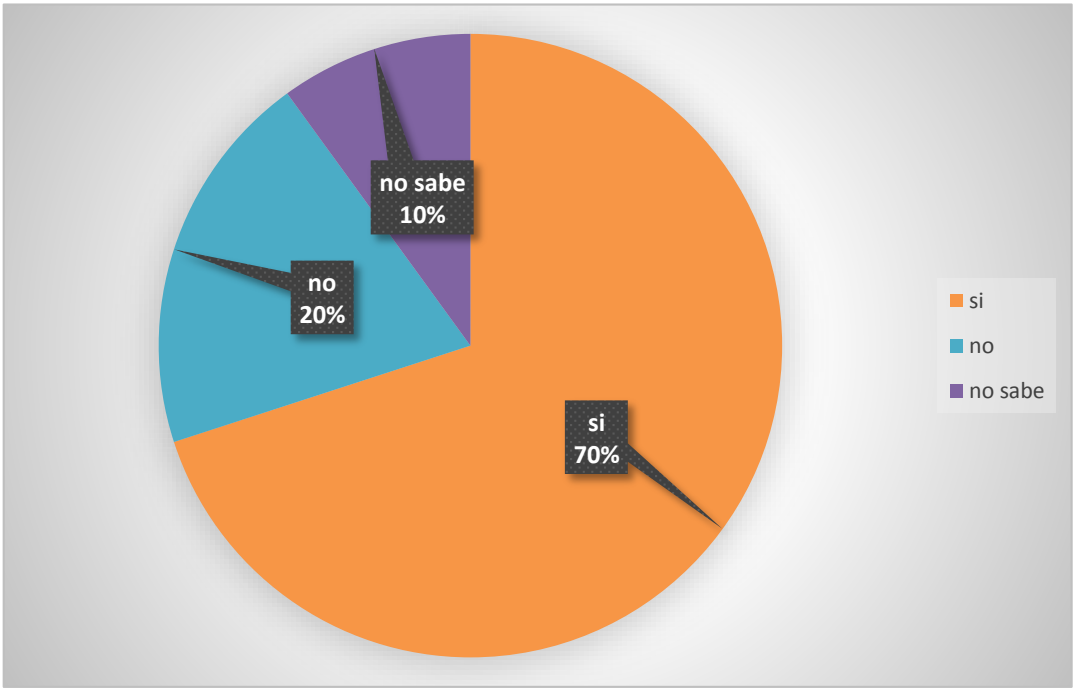

Gráfico 1: Cumplimiento de necesidades (docente-administrativo)
Elaborado por: Las autoras

Como muestra el gráfico 1, podemos comprender que el personal que labora dentro de la institución no está totalmente convencido de los servicios que brinda la Unidad Educativa y a su vez si esto si esto no se causado por el número de persona que contribuyen cada día con las funciones que se realizan día a día.

Como parte del cuestionario de preguntas se precisaba saber si los colaboradores crían conveniente o necesario la admisión de más personal para lograr el cumplir en su totalidad con las necesidades de estudiantes y padres de familia.

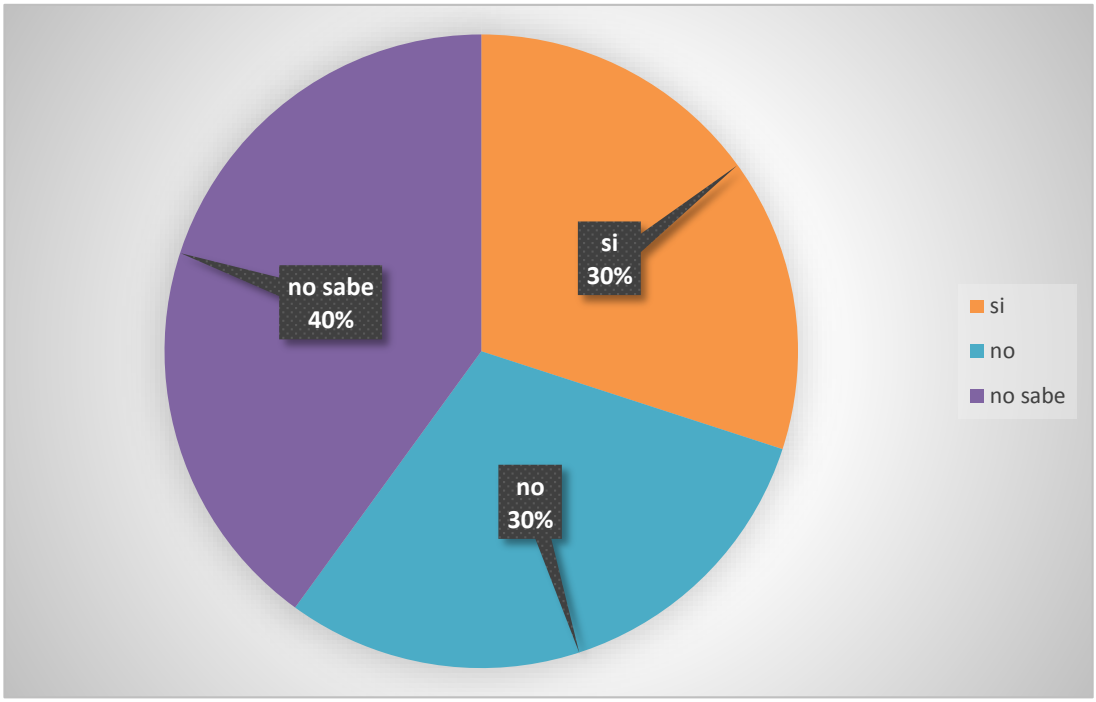

Gráfico 2: Instalaciones adecuadas
Elaborado por: Las autoras

Durante proceso de recopilación de información observamos que en el gráfico 2 se muestra un porcentaje significativo de personas que indicaron no saber si las instalaciones con las que cuenta actualmente la Institución Educativa son las más adecuadas para los alumnos, tomando en cuenta la cantidad de estudiantes y la completitud de las dichas instalaciones.

Dentro de esta observación y durante las encuestas se dejaba en claro que los aspectos que abarcaba una instalación adecuada eran herramientas, acondicionamiento, buena disponibilidad de equipos; en resumen la total disponibilidad de los recursos que son indispensables no solo para estudiantes, sino a la vez que se consideren necesarios para laborar de mejor manera y con mayor facilidad.

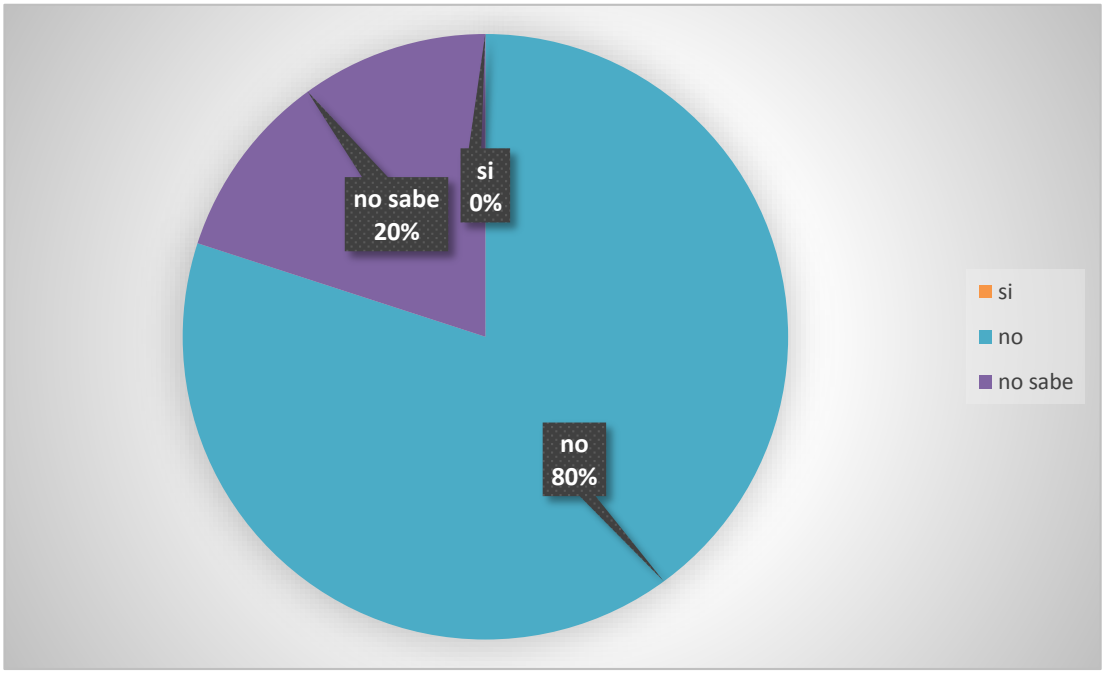

Gráfico 3: Disponibilidad de equipos modernos
Elaborado por: Las autoras

Es verdad que para poder cumplir con funciones básicas dentro de un colegio o cualquier entidad no se necesita de equipos de última tecnología, sin embargo se creyó necesario preguntar sobre el tema para tener conocimiento de ello y poder posteriormente comparar las expectativas de resultados finales tomando en cuenta los recursos que se utilizan en la actualidad.

En el gráfico 3 se observa que según la encuesta realizada el personal que labora dentro de la Institución no cree que se cuente con herramientas y equipos tecnológicos de alta y de la mejor tecnología y algunos preferían añadir que quizás por

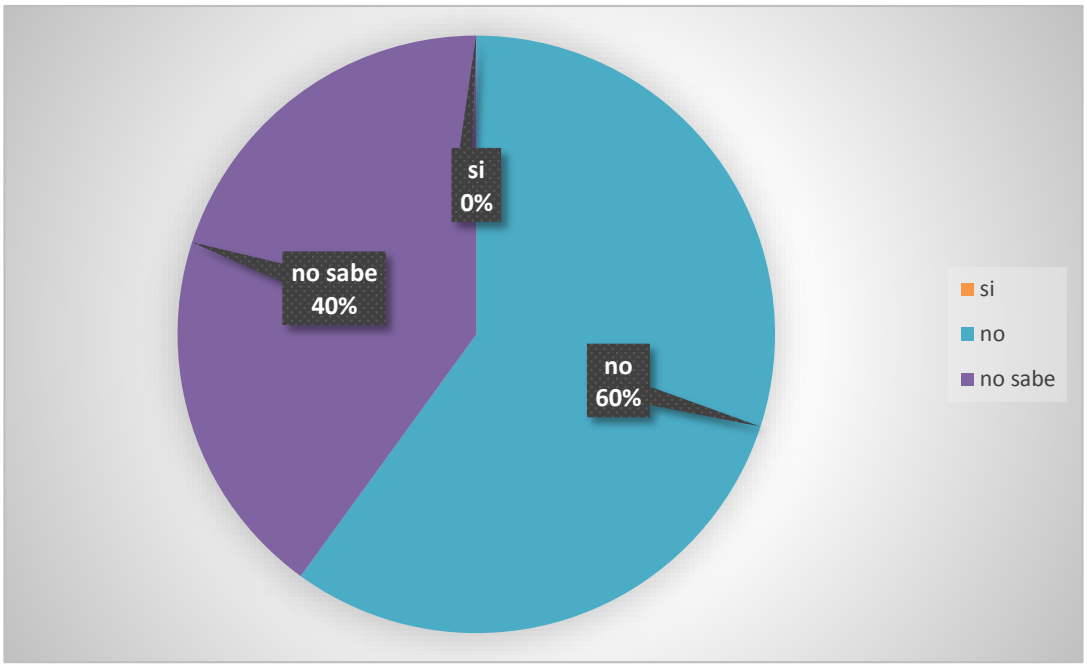

Gráfico 4: Existencia de área de seguridad de la información
Elaborado por: Las autoras

La falta de mejores equipos presenta ciertas falencias y falta de mejores tiempos de respuesta en aplicativos durante el cumplimiento de sus funciones dentro del colegio.

Con respecto a la pregunta de que si existe un área que regularice, controle y maneje la seguridad de la información específicamente y como es notable en el gráfico 4 podemos decir que efectivamente no existe esa área, no hay que separarnos mucho de la realidad de que sí hay un área que se encargue de eso como lo comentaron algunos encuestados, sin embargo no existe la plena seguridad de que la función y la responsabilidad de proteger ese activo tan importante se esté llevando a cabo de la mejor manera.

Como se mostrará en el gráfico 5 podemos visualizar una idea de qué nivel de seguridad existe en ciertos recursos informáticos, los cuales son de mucha utilización para el transporte y resguardo de información.

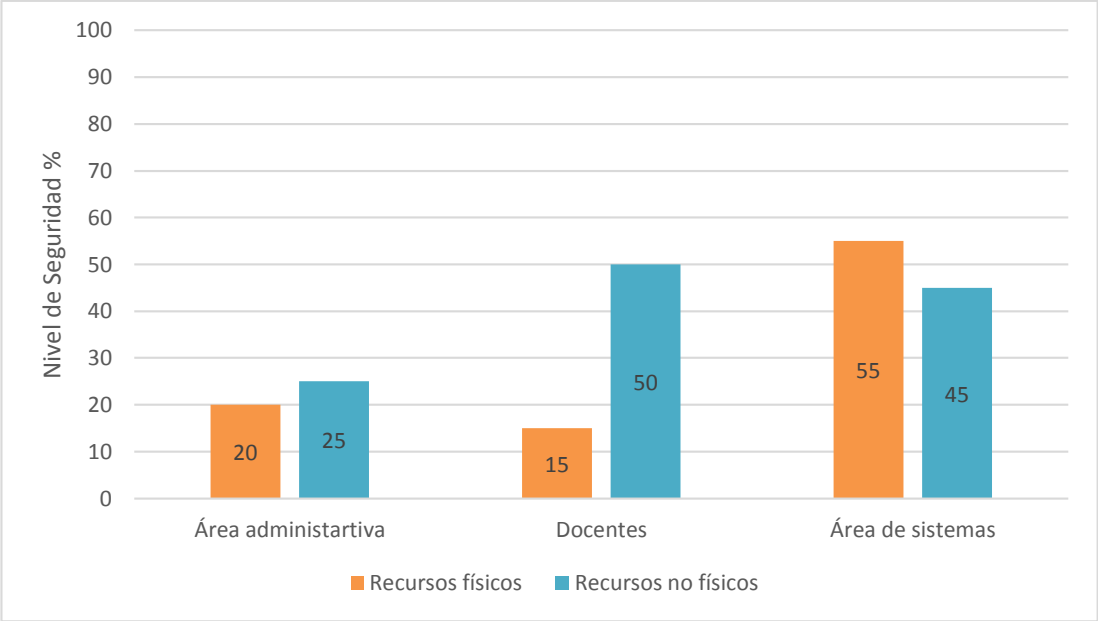

Gráfico 5: Administración de la seguridad informática
Elaborado por: Las autoras

De una manera algo general se representó el nivel de seguridad e importancia a su vez que brinda a los recursos informáticos disponibles en las diferentes áreas que se presentan en la Unidad Educativa Salesiana Domingo Comín.

Al referirnos a recursos físicos podemos hacer referencia a discos duros externos, CDs, pen drives, CPU, monitores, servidores, etc.; mientras que al referirnos a recursos no informáticos son todas aquellas herramientas instaladas en un ordenador específico o a nivel de red para mantener segura la información que se utiliza y que se debería respaldar en la Institución Educativa para poder prevenir cualquier incidente en posteriores ocasiones.

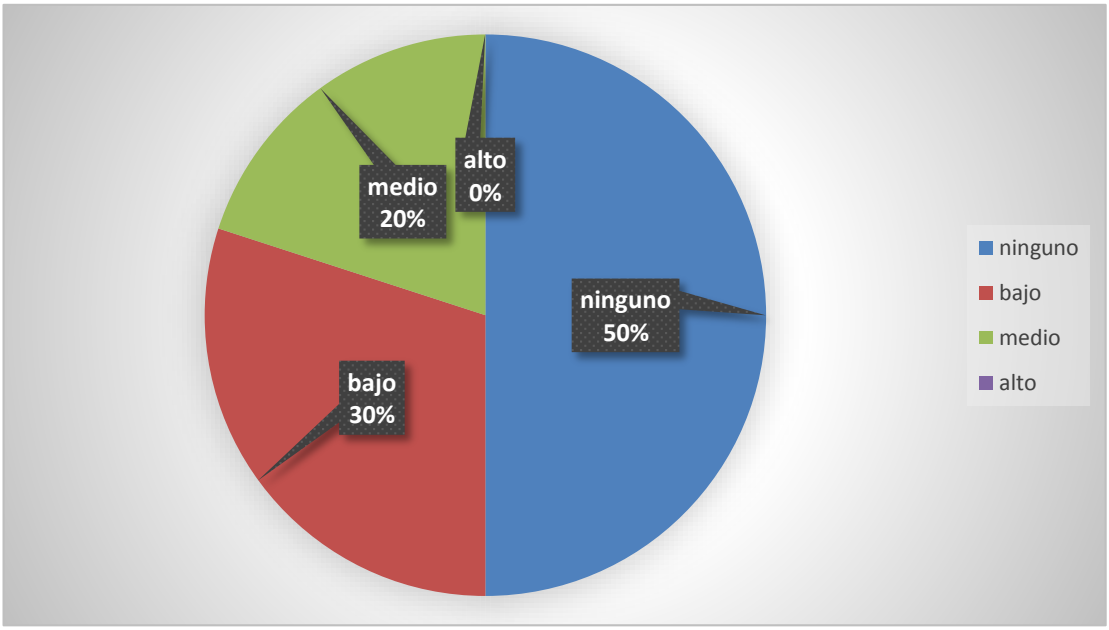

Gráfico 6: Toma de medidas ante incidentes o desastres ambientales
Elaborado por: Las autoras

En el gráfico 6 podemos verificar el nivel de control y preparación ante incidentes informáticos que pueden presentarse o a su vez de desastres ambientales que pueden causar el daño y pérdida total de los equipos que posee la Institución.

Según las encuestas realizadas y la revisión de campo que se realizó al parecer no se cuentan con los recursos necesarios para proteger los activos disponibles, más adelante se hará y mostrará una descripción más detallada de cada activo y su nivel de seguridad antes los diferentes sucesos posibles a suceder. Es importante poder contar con medidas preventivas o correctivas ante los diferentes riesgos que corre la información y a su vez los medios que implican poder mantenerla respaldada y segura.

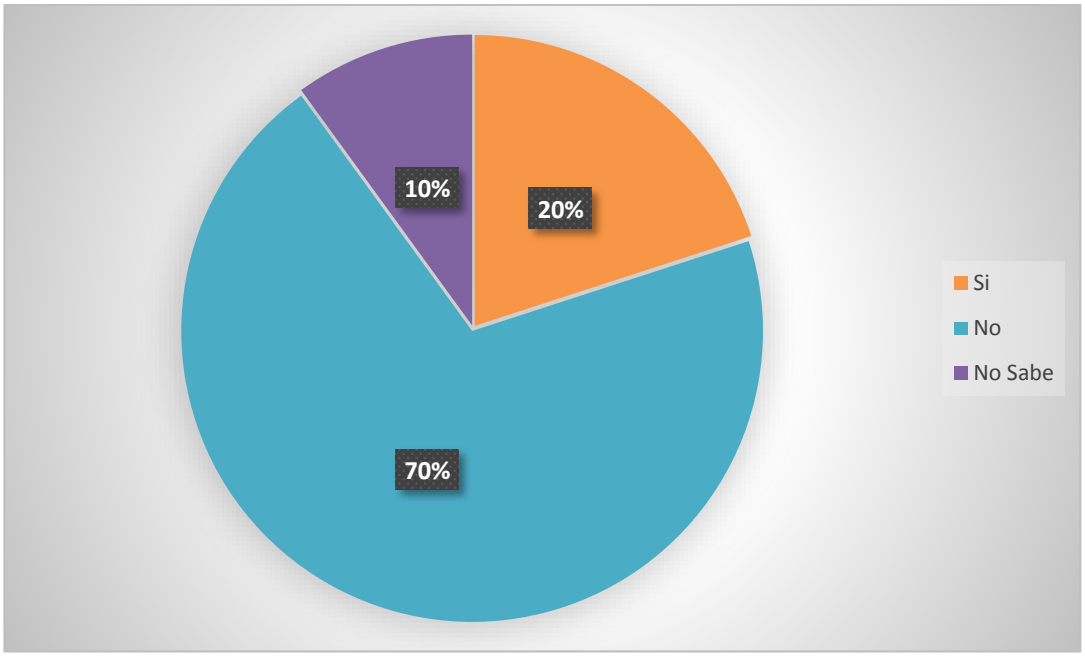

Gráfico 7: Nivel de Confidencialidad de la Información
Elaborado por: Las autoras

De acuerdo al gráfico 7 se muestra que la Unidad Educativa Salesiana "Domingo Comín" no maneja un alto nivel de confidencialidad por lo cual es importante que se ejecute los controles recomendados, para que la información este accesible únicamente a personal autorizado.

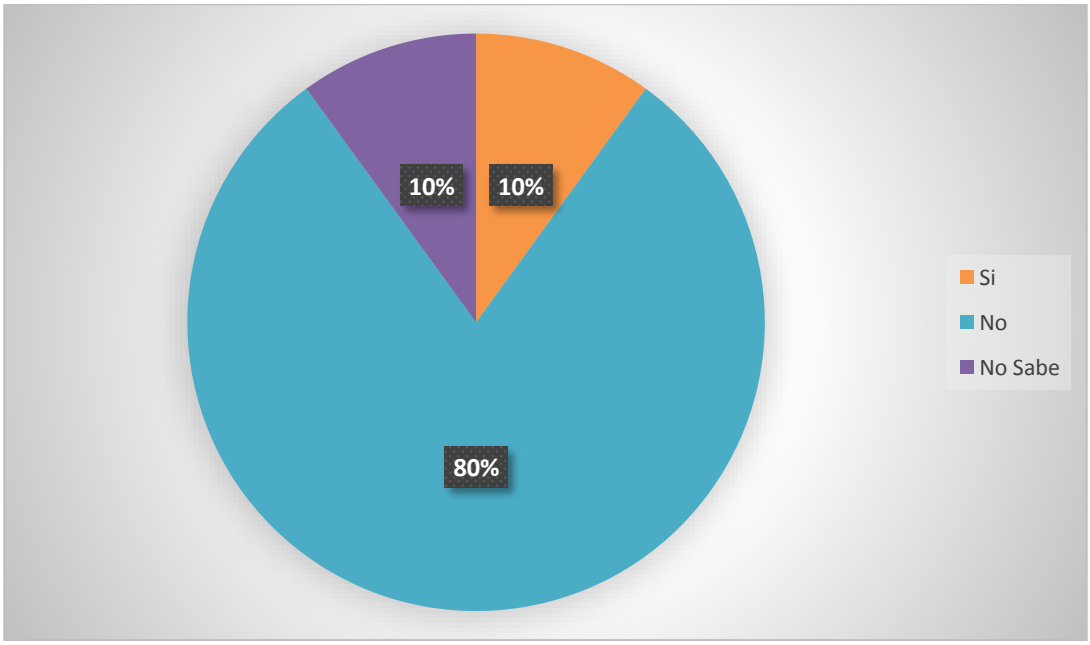

Gráfico 8: Manejo de Controles de Acceso
Elaborado por: Las autoras

En base a lo relacionado con el gráfico 8 se interpreta que no existe manejo de controles de acceso al ingreso del sistema y manejo de información, por lo cual es claro que se debe implementar los controles recomendados para no tener expuesta la información confidencial de la Unidad Educativa Salesiana "Domingo Comín".

4.6 Resultado de las entrevistas

Para poder identificar los activos y controles que tiene la Unidad Educativa Salesiana "Domingo Comín" realizamos encuestas y entrevistas a los encargados del departamento de sistemas y al personal de las áreas críticas, por medio de los cuales los hemos clasificado de la siguiente forma:

Activos físicos: Equipos de comunicación, routers, switches, servidores, equipos de computación entre otros equipos.

Personal: Administrativos, sistemas, profesores, rectorado, vicerrectorado.

Activos de Información: Base de datos, office 365, Sistema GTH.

Documentación Impresa: Inventario de equipo de computación de todos los meses de cada año por departamento, documentación de licencias adquiridas.

Tabla 5: Formato para la identificación de activos

ENCARGADO	CÓDIGO DEL ACTIVO	NOMBRE	CANTIDAD	DESCRIPCIÓN	ÁREA
Responsable del activo	Numero único del activo	Nombre del activo	Números de activos	Función que desempeña el activo	Se indica en donde se encuentra ubicado el activo

Elaborado por: Las autoras

4.6.1 Atributos de valoración

Características que dan valor al activo.

Disponibilidad: La ausencia de disponibilidad detiene a varios procesos críticos dentro de la Unidad Educativa Salesiana "Domingo Comín".

Dimensión: Estas nos dan paso para poder valorar las consecuencias de la materialización de una amenaza. La valoración que se le da a un activo en una determinada dimensión es la medida del perjuicio para la unidad Educativa Salesiana "Domingo Comín".

Confidencialidad: La información debe llegar netamente a personal autorizado.

En forma contraria a la confidencialidad puede llegarse a dar filtraciones de información, dar accesos a personas no autorizadas o dar permisos a usuarios bloqueados.

Integridad: Esta característica afecta directamente al buen funcionamiento de los procesos en la Unidad Educativa.

Des estos atributos que hemos detallado escogimos una escala de cuatro valores, los cuales están clasificados de la siguiente forma:

Tabla 6: Escalas para integridad

Activos de Información	Nivel	Detalle
1	Despreciable	No afectará a la integridad de los datos
2	No Necesaria	Se la utiliza para hacer consultas, no hay daño en los datos
3	Necesaria	No permitir que se juegue con la integridad de los datos, ya que si esto sucede afecta las operaciones que realiza la Unidad Educativa.
4	Importante	Si se pierde la integridad, se distorsionan los datos reales, por lo cual afecta las operaciones de la Unidad Educativa "Domingo Comín".

Elaborado por: Las autoras

Tabla 7: Escalas para Disponibilidad

Activos de Información	Nivel	Detalle
1	Muy Bajo	No afecta a las funciones de la Unidad Educativa.
2	Bajo	En caso de que la información no se encuentre disponible, no hay problema, la Unidad Educativa puede continuar con sus operaciones.
3	Medio	En caso de no estar disponible la información, existe pequeños efectos en las operaciones de la Unidad Educativa. Sin embargo hay métodos alternativos que pueden ser usados o estar a la espera de que la información esté disponible para poder continuar con normalidad las operaciones.
4	Alto	En caso de que la información no esté disponible cuando se la necesite, sería muy grave ya que se detienen las operaciones de la Unidad Educativa.

Elaborado por: Las Autoras

Tabla 8: Escalas para Confidencialidad

Activos de Información	Nivel	Detalle
1	Pública	La información puede ser proporcionada a otras personas que no sean parte de la institución, sin embargo se debe tener en cuenta que esto podría conllevar a efectos mínimos en las operaciones cotidianas de la Unidad Educativa.
2	Uso Interno	La información sólo es revelada y proporcionada para los funcionarios de la Unidad Educativa. En caso de que el contenido sea revelado no causa algún efecto en las operaciones.
3	Secreto	La información sólo puede ser revelada y proporcionada a funcionarios de un área en específica, ya que si esta es revelada o proporcionada puede causar efectos que retrasen las operaciones de la Unidad Educativa
4	Privado	La información solo la puede tener el jefe del departamento de sistemas o la rectora, ya que si esta información es revelada puede provocar grandes efectos que obstaculicen las operaciones de la institución.

Elaborado por: Las autoras

Debido a la constante aparición de las amenazas, hemos seleccionado una lista de ellas las cuales deben de ser analizadas y revisadas en base a la experiencia en operaciones y datos estadísticos que se han recolectado.

En este caso vamos a analizar las amenazas en 4 niveles: muy bajo, bajo, medio, alto.

Tabla 9: Escalas para determinar los niveles de amenazas

PROBABILIDAD QUE OCURRA	Nivel	Detalle
1	Muy Bajo	Es muy poco probable que ocurra una amenaza, sin embargo puede presentarse una vez en cada 3 años.
2	Bajo	Existe baja probabilidad de que ocurra, sin embargo puede darse una vez en el año.
3	Medio	Hay una frecuente ocurrencia pero la cual es controlada, este se da una vez cada seis meses o menos tiempo.
4	Alto	Existe una alta probabilidad que ocurra amenazas frecuentemente, estas pueden darse cada semana o mes.

Elaborado por: Las autoras

Tabla 10: Escalas para determinar los niveles de vulnerabilidades

PROBABILIDAD QUE OCURRA	Nivel	Detalle
1	Muy Bajo	En este nivel no se tiene ningún tipo de control por lo cual los datos son muy sensibles y vulnerables, que se puede llegar a decir que pueden estar al alcance de todos.
2	Bajo	Existen controles muy sensibles y vulnerables, por lo que se puede llegar acceder de una forma fácil a la información.
3	Medio	Los controles aplicados en este nivel son más altos, sin embargo existe un porcentaje considerable de vulnerabilidad por lo que también puede dar a paso a que se obtenga la información.
4	Alto	Se tiene controles de seguridad adecuados, por lo cual es difícil que puedan encontrar alguna vulnerabilidad.

Elaborado por: Las autoras

4.7 Detección de Amenazas y Vulnerabilidades

La idea es identificar las amenazas que afecten a los activos de los sistemas de información y las vulnerabilidades que pueden darse por la amenazas.

A continuación detallaremos las vulnerabilidades que pueden aparecer en cada uno de los activos identificados y las amenazas que pueden afectar a dichas vulnerabilidades, estas fueron analizadas en conjunto con el departamento de sistemas de la Unidad Educativa Salesiana “Domingo Comín”.

Tabla 11: Identificación de Amenazas y Vulnerabilidades- Activos (Equipos De Computación)

Activo	Amenaza	Vulnerabilidad
EQUIPOS DE COMPUTACIÓN	Desastres Naturales	Área del departamento que se les da para que coloquen los equipos, los cuales son fácilmente afectados por algún desastre natural.
	Incendios	Ausencia de protección para los activos contra el fuego.
	Degradación o falla del hardware	Falta de aplicación de los controles necesarios.
	Robo	Falta de controles para bloquear que terceras personas no accedan a la información de la Unidad Educativa Salesiana "Domingo Comín"
	Uso no adecuado	Aumentar más controles para que el personal haga uso sólo de los permisos asignados.
	Cambios de Software	Falta de control de acceso.

Elaborado por: Las autoras

Tabla 12: Identificación de Amenazas y Vulnerabilidades- Activos (Documentos)

Activo	Amenaza	Vulnerabilidad
	Desastres Naturales	Área del departamento que se les da para que coloquen los equipos, los cuales son fácilmente afectados por algún desastre natural.
Documentos	Incendios	Ausencia de protección para los activos contra el fuego.
	Pérdida de la información	Documentación no protegida, falta de controles.
	Robo	Falta de controles para bloquear que terceras personas no accedan a la información de la Unidad Educativa Salesiana "Domingo Comín"
	Uso no adecuado	Aumentar más controles para que el personal haga uso sólo de los permisos asignados.
	Actualización no autorizada de la documentación	Falta de controles que bloqueen a usuarios no asignados hacer la cambios en la documentación.

Elaborado por: Las autoras

4.7.1 Presentación del Riesgo

Se tomara en cuenta la probabilidad de que ocurra cada amenaza y nivel de vulnerabilidad que podrían afectar a los activos, para tener así como resultado el nivel de riesgo de la Unidad Educativa Salesiana "Domingo Comín".

Vulnerabilidad: Probabilidad de que ocurra.

Amenaza: Probabilidad que ocurra algún tipo de amenaza, nos basamos a los datos obtenidos en los últimos dos años.

4.8 Presentación Controles para Reducir los riesgos

Para poder seleccionar los riesgos se debe tomar en cuenta los resultados de la evaluación del nivel del riesgo.

Si se asocian las amenazas con las vulnerabilidades indican en donde hay que implementar mayor controles, para que los activos se encuentren debidamente protegidos.

Los factores que deben ser considerados para poder implementar los controles son los siguientes:

- La función que desempeñan dentro de la Unidad Educativa Salesiana "Domingo Comín".
- Transparencia del personal
- Implementación de controles.

4.9 Procesos Críticos

La Unidad Educativa Salesiana "Domingo Comín" ha clasificado como críticos los siguientes procesos:

- Rectorado
- Vicerrectorado
- Coordinación Académica
- Sistemas
- Secretaria
- Contabilidad
- Adquisición
- Apoyo y mantenimiento
- Ajuste Mecánico

4.10 Riesgos detectados en la Unidad Educativa y los controles seleccionados

En los siguientes cuadros detallaremos el resumen de los riesgos encontrados que afectan a los procesos de la Unidad Educativa Salesiana "Domingo Comín".

A continuación se expone los controles que se deben aplicar para reducir los riesgos.

4.10.1 Procesos Críticos Afectados

Tabla 13. Riesgo: Desastres Naturales

Activo- Equipos de Computación	
Procesos Afectados	**Nivel de Riesgo**
Sistemas	Medio
Adquisición	Alto
Ajuste Mecánico	Alto

Elaborado por: Las autoras

Tabla 14: Riesgo: Degradación o falla del hardware

Activo- Equipos de Computación	
Procesos Afectados	**Nivel de Riesgo**
Secretaria	Medio
Rectorado	Medio
Vicerrectorado	Medio

Elaborado por: Las autoras

Tabla 15. Riesgo: Robo

Activo- Equipos de Computación	
Procesos Afectados	**Nivel de Riesgo**
Sistemas	Medio
Coordinación académica	Bajo
Contabilidad	Alto

Elaborado por: Las autoras

Tabla 16. Riesgo: Uso no adecuado

Activo- Equipos de Computación	
Procesos Afectados	**Nivel de Riesgo**
Apoyo y mantenimiento	Bajo
Adquisición	Alto
Coordinación Académica	Medio
Contabilidad	Medio

Elaborado por: Las autoras

Tabla 17. Riesgo: Pérdida de la Información

Activo- Documentos	
Procesos Afectados	**Nivel de Riesgo**
Secretaria	Medio
Pastoral	Medio
Consejería Estudiantil	Medio

Elaborado por: Las autoras

Tabla 18. Riesgo: Robo

Activo- Documentos	
Procesos Afectados	**Nivel de Riesgo**
Sistemas	Medio
Coordinación académica	Bajo
Contabilidad	Alto

Elaborado por: Las autoras

Tabla 19. Riesgo: Uso no adecuado

Activo- Documentos	
Procesos Afectados	**Nivel de Riesgo**
Apoyo y mantenimiento	Bajo
Adquisición	Alto
Coordinación Académica	Medio
Contabilidad	Medio

Elaborado por: Las autoras

Tabla 20. Riesgo: Actualización no autorizada de la documentación

Activo- Documentos	
Procesos Afectados	**Nivel de Riesgo**
Secretaria	Medio
Contabilidad	Medio

Elaborado por: Las autoras

4.11 Verificación de hipótesis

La falta de uso o implementación de medidas de seguridad basadas en la norma NTE INEN-ISO/IEC 27001:2001 ha dejado una larga brecha de inseguridades dentro de la Unidad Educativa Salesiana Domingo Comín.

Durante el análisis y gestión de varios de los procesas que maneja el área de Sistemas se logró el reconocimiento de las mayores vulnerabilidades de muchos de los recursos tecnológicos ayudando a identificar mejores técnicas de seguridad, como podría reflejarse en el proceso de otorgar accesos, controlando que el personal obtenga mayor conocimiento de cómo resguardar información y como asegurar y cuidar el funcionamiento de equipos.

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

Durante el desarrollo de la tesis se logra identificar las mejores técnicas de seguridad por medio de un análisis minucioso de las diferentes tecnologías y herramientas que utilizan en la Unidad Educativa Domingo Comín para el manejo y resguardo de información.

En base a los diferentes puntos tocados en el desarrollo del proyecto como fueron: Políticas de seguridad, gestión de activos informáticos, seguridad relacionada con el personal, seguridad física y el entorno y seguridad de los accesos se ha logrado establecer todos aquellos procesos donde se utilicen recursos informáticos y a su vez identificar las principales amenazas y vulnerabilidades a las que se encuentran expuestos.

Se pudo medir los niveles de riesgo de los diferentes activos para lograr verificar cuáles serían sus mayores falencias, en qué se puede mejorar y en qué se debe mejorar.

Los cambios y mejoramientos que se recomendarán más adelante dependerán mucho del factor tiempo, costo y hasta el personal administrativo o docentes, puesto que para muchos usuarios la aparición de nuevas disposiciones es sinónimo de más trabajo o de complicaciones; sin embargo con el trato, el asesoramiento y la compresión de qué tan importante es la información que manejan y con ello todo lo que involucre como equipos, dispositivos, sistemas, etc., entenderán que todos los activos informáticos deben ser tratados cuidadosamente y requieren de todas las seguridades convenientes para asegurar el mejor funcionamiento de los mismos.

5.2 Recomendaciones

Como parte principal de las recomendaciones es la implementación de un manual de controles donde se definirá y se dispondrá de manera documentada todas aquellas principales falencias dentro de lo que fue el análisis de estudio. Entre otras muy específicas tenemos:

Mejorar el ambiente de los espacios físicos donde se protegen los respaldos de información para asegurar el funcionamiento correcto de los equipos que deben cumplir con este proceso.

Mejorar los controles de acceso a áreas de nivel crítico implementando por ejemplo sistemas biométricos, cámaras de seguridad para verificar el ingreso del personal a los departamentos.

Fortalecer el nivel de seguridad de los accesos a los diferentes activos informáticos puesto que no todos los usuarios tienen o manejan el mismo nivel de información.

Adquirir herramientas con licencias por ejemplo del antivirus más que nada porque es parte importante del cuidado de información y de equipos ayudando a alargar su periodo de vida.

CAPÍTULO 6

PROPUESTA

En base al proyecto planteado se llegó a la propuesta de implementar controles y políticas de seguridad en las áreas críticas de la Unidad Educativa Salesiana "Domingo Comín".

De acuerdo a la tabla 11 que hace referencia al riesgo de desastres naturales del activo equipos de computación se propone utilizar los siguientes controles:

A.9.1.4: Protección contra amenazas externas y ambientales

Control: "Se debe diseñar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, disturbios civiles y otras formas de desastre natural o creado por el hombre".

A.9.2.4: Mantenimiento de Equipo

Control: "El equipo debe ser mantenido correctamente para permitir su continua disponibilidad e integridad."

Haciendo referencia a la tabla 12 del riesgo de degradación o falla del hardware del activo equipos de computación se deberá implementar el siguiente control:

A.9.2.4 Mantenimiento de Equipo

Control: "El equipo debe ser mantenido correctamente para permitir su continua disponibilidad e integridad.**"**

En la tabla 13 que hace énfasis en el riesgo de robo del activo equipos de computación para evitar este riesgo deberán ejecutar los siguientes controles:

A.11.3.1 Uso de clave

Control: "Se requiere que los usuarios sigan buenas prácticas de seguridad en la selección y uso de claves".

A.11.3.2 Equipo de usuario desatendido

Control: "Se debe requerir que los usuarios se aseguren de dar la protección apropiada al equipo desatendido".

En base al riesgo del uso no adecuado del activo equipos de computación, como se indica en la tabla 14 puede afectar a algunos procesos, por lo cual se ha recomendado los siguientes controles:

A.6.1.1 Compromiso de la gerencia con la seguridad de la información

Control: "La gerencia debe apoyar activamente la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado, asignación explicita y reconocimiento de las responsabilidades de la seguridad de la seguridad de la información".

A.8.1 Roles y Responsabilidades

Control: "Se deben definir y documentar los roles y responsabilidades y seguridad de los empleados, contratistas y terceros en concordancia con la política de la seguridad de información de la organización".

A.8.2.1 Gestión de Responsabilidades.

Control: "La gerencia debe requerir que los empleados contratistas y terceros apliquen la seguridad en concordancia con las políticas y procedimientos establecidos de la organización".

A.8.2.2 Capacitación y Educación en seguridad de la información

Control: "Todos los empleados de la organización y, cuando sea relevante, los contratistas y terceros, deben recibir el apropiado conocimiento, capacitación y actualizaciones regulares de las políticas y procedimientos organizacionales, conforme sean relevantes para su función laboral".

A.8.2.3 Proceso Disciplinario

Control: "Debe existir un proceso disciplinario formal para los empleados que han cometido una violación en la seguridad"

De acuerdo a la pérdida de la información de los documentos como se hace mención en la tabla 15 se deberá implementar los controles que se detallan a continuación:

A.5.1.1 Documentar política de seguridad de seguridad de la información

Control: "La gerencia debe aprobar un documento de política, este se debe publicar y comunicar a todos los empleados y entidades externas relevantes."

A.5.1.2 Revisión de la política de seguridad de la información: La política de seguridad de la información debe ser revisada regularmente a intervalos planeados o si ocurren cambios significativos para asegurar la continuidad idónea, eficiencia y efectividad**.**

A.6.1.1 Compromiso de la gerencia con la seguridad de la información

Control: "La gerencia debe apoyar activamente la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado, asignación explicita y reconocimiento de las responsabilidades de la seguridad de la seguridad de la información".

A.10.4.1 Controles contra Software Malicioso

Control: "Se deben implementar controles de detección, prevención y recuperación para protegerse de códigos maliciosos y se deben implementar procedimientos de conciencia apropiados.

A.10 5 Respaldo (Back- up): Mantener la integridad y la disponibilidad de los servicios de procesamiento de información y comunicaciones.

A.10.5.1 Back-up o respaldo de la información

Control: "Se deben realizar copias de back-up o respaldo de la información comercial y software esencial y se deben probar regularmente de acuerdo a la política."

Se debe tomar controles para evitar el robo de documentos y más aún en los procesos afectados como lo indica en la tabla 16, se detalla a continuación los controles recomendados:

A.11.3.1 Uso de clave

Control: "Se requiere que los usuarios sigan buenas prácticas de seguridad en la selección y uso de claves".

A.11.3.2 Equipo de usuario desatendido

Control: "Se debe requerir que los usuarios se aseguren de dar la protección apropiada al equipo desatendido".

Debido al uso no adecuado de los documentos en los procesos afectados como lo indica en la tabla 17, se hace énfasis para que ejecuten los siguientes controles:

A.6.1.1 Compromiso de la gerencia con la seguridad de la información

Control: "La gerencia debe apoyar activamente la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado, asignación explicita y reconocimiento de las responsabilidades de la seguridad de la seguridad de la información".

A.8.1 Roles y Responsabilidades

Control: "Se deben definir y documentar los roles y responsabilidades y seguridad de los empleados, contratistas y terceros en concordancia con la política de la seguridad de información de la organización".

A.8.2.1 Gestión de Responsabilidades.

Control: "La gerencia debe requerir que los empleados contratistas y terceros apliquen la seguridad en concordancia con las políticas y procedimientos establecidos de la organización".

A.8.2.2 Capacitación y Educación en seguridad de la información

Control: "Todos los empleados de la organización y, cuando sea relevante, los contratistas y terceros, deben recibir el apropiado conocimiento, capacitación y actualizaciones regulares de las políticas y procedimientos organizacionales, conforme sean relevantes para su función laboral".

A.8.2.3 Proceso Disciplinario

Control: "Debe existir un proceso disciplinario formal para los empleados que han cometido una violación en la seguridad".

De acuerdo a la tabla 18 de la actualización no autorizada de la documentación se ha recomendado los siguientes controles:

A.10.1.1 Procedimientos de operación documentados

Control:"Se deben documentar y mantener los procedimientos de operación, y se deben poner a disposicion de todos los usuarios que los necesiten."

A.10.3.1 Gestión de Capacidad

Control: "Se debe monitorear, afinar y realizar proyecciones del uso de los recursos para asegurar el desempeño del sistema requerido".

6.1 Datos Informativos

Nombre de la Institución: Unidad Educativa Salesiana "Domingo Comín"
Departamento: Sistemas
Jornada: Matutina
Ubicación geográfica
País: Ecuador
Provincia: Guayas
Ciudad: Guayaquil
Parroquia: Ximena

6.2 Antecedentes de la Propuesta

En años anteriores la tecnología no estaba al alcance de todos pero en la actualidad esta se encuentra en cada parte que vamos, debido a este avance tecnológico grandes instituciones tienen su información dentro de bases de datos, discos duros entre otros medios, pero en muchas ocasiones dicha información no se encuentra protegida como debería estarlo y por lo cual queda vulnerable, esto da paso a que personas externas de las instituciones quieran saltar la seguridad que tiene dicha información ya sea para venderla o para dejar inoperable la institución.

Debido a esta realidad que se vive muy a menudo se ha realizado el análisis de requisitos de tecnología de información para la aplicación de técnicas de seguridad

bajo la normativa NTE INEN- ISO/IEC 27001:2011 en la Unidad Educativa Salesiana "Domingo Comín".

6.3 Justificación

En la actualidad el mundo está sometido a constantes cambios y la tecnología a menudo que pasa el tiempo va evolucionando, si se compara los medios tecnológicos que teníamos en años anteriores con los que tenemos ahora vamos a encontrar una gran diferencia.

Debido a estos brutales cambios fue necesario realizar el análisis de requisitos de tecnología de información para la aplicación de técnicas de seguridad esta permitirá minimizar las vulnerabilidades y amenazas que pueden llegar a afectar a las operaciones dentro de la Unidad Educativa Salesiana Domingo Comín.

Debido al incorrecto uso de la información confidencial de la unidad Educativa Salesiana "Domingo Comín", hemos hecho énfasis a ciertos controles que son necesarios para llevar en un buen funcionamiento a las operaciones dentro de la institución.

A razón de la falta de controles dentro de los procesos críticos que pueden ser afectados por un desastre natural o por culpa del hombre, es netamente necesario informarles a los funcionarios de la institución para que así ellos puedan hacer conciencia de la importancia de llevar a cabalidad los controles.

6.4 Objetivos

6.4.1 Objetivo General

Reducir las amenazas y vulnerabilidades de los departamentos críticos de la Unidad Educativa Salesiana "Domingo Comín", por medio de la aplicación de técnicas de seguridad bajo la normativa NTE INEN- ISO/IEC 27001:2011.

6.4.2 Objetivos Específicos

- Identificar las amenazas que han sido más constantes en estos últimos años.
- Recomendar los controles para que sean ejecutadas por el personal de la Unidad Educativa Salesiana "Domingo Comín".
- Identificar los controles para evitar el acceso a personas no autorizadas a la información sensible de la Unidad Educativa.

6.5 Análisis de Factibilidad

La presente propuesta es factible porque quienes forman parte de la Unidad Educativa Salesiana "Domingo Comín" han demostrado su interés y compromiso para que se ejecute dicho análisis de requisitos de tecnología de información.

De acuerdo a esto el encargado del departamento de sistemas esta consiente que es importante poner en marcha dichos controles ya que estos pueden llegar a reducir las vulnerabilidades que se encuentran en algunos procesos de la Institución.

6.6 Fundamentación

En el afán de reducir las vulnerabilidades y riesgos, de lograr que las políticas y controles que hemos recomendado se ejecuten en el departamento de sistemas y áreas críticas de la Unidad Educativa Salesiana "Domingo Comín".

Es así que de lo analizado se puede decir que los riesgos detectados afectan a las operaciones de la institución, pero con la ayuda de la ejecución de los controles recomendados va a fortalecer la correcta funcionalidad de los mismos.

Debido a esto los funcionarios de la Unidad Educativa Salesiana "Domingo Comín" también desempeñan un rol importante ya que ellos están comprometidos en seguir paso a paso lo que indican los controles.

Como se puede evidenciar este análisis que se ha realizado es muy importante para así poder contar con la correcta función de los procesos de la Unidad Educativa Salesiana “Domingo Comín”.

6.7 Metodología

El presente análisis se proyecta a la reducción de las vulnerabilidades encontradas en la institución, usando los controles y políticas que se han recomendado, posterior a eso dará seguimiento para evaluar si los controles se han ejecutado, también se propone una estrategia defensiva para cada tipo de método utilizado en cada amenaza.

Evaluar Riesgos

Por cada tipo de Amenaza (ejm: Desastres Naturales)

Para cada tipo de método de seguridad (ejm. Respaldos)

Estrategia Proactiva

Determinar las vulnerabilidades

Minimizar las vulnerabilidades (ejecutar plan de controles sugeridos

Identificar posibles daños

Estrategia Reactiva

Determinar la causa del daño

Reparar daños (ejecutando controles necesarios)

Evaluar daños

Plan de contingencia

Evaluar resultados

Bibliografía

A., M. (2013). *Control Q*. Obtenido de https://controlqblog.wordpress.com/2013/01/05/ciclo-de-mejora-continua-el-padre-de-los-7/

Alegre Ramos, M. d., & Garcia-Cervigon Hurtado, A. (2011). Seguridad Informática. Madrid: paraninfo.

ceeisec. (2014). Obtenido de http://www.ceeisec.com/nuevaweb/doc/informacionSGSI.pdf

Cervantes Sanchez, & Ochoa Ovalles. (Julio de 2012). *Contribuciones a las Ciencias Sociales*. Obtenido de www.eumed.net/rev/cccss/21/

Gallinger, A. (2011). *Informática Argento*. Obtenido de http://argentows.blogspot.com/2011/04/metodos-de-proteccion-contra-virus.html

Gillet Goinard, F. (2014). *La caja de herramientas: control de calidad.* Larousse - Grupo Editorial Patria.

INEN. (2011). *INSTITUTO ECUATORIANO DE NORMALIZACIÓN.* Obtenido de www.inen.gob.ec

ISO/IEC 17023:2013. (2013). *Evaluación de la conformidad — Directrices para determinar la duración de las auditorías de certificación de sistemas de gestión.*

ISO27000. (2012). *El portal de ISO 27001 en español.* Obtenido de www.ISO27000.es

ISOTools Excellence. (2013). *Sistemas de Gestión especialmente diseñados y aplicables a las TICs* . Obtenido de http://www.pmg-ssi.com/2013/12/iso27001-origen/

LEON, E. E. (2010). SGSI ISO 27001. *SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN*.

Unidad Educativa Domingo Comín. (s.f.). *Unidad Educativa Domingo Comín*. Obtenido de http://www.domingocomin.edu.ec/

Anexo # 1

Encuesta realizada en la Unidad Educativa Salesiana "Domingo Comín"

Nombre Encuestado/a:
Cargo:

¿Considera Ud. que el número del personal docente y administrativo alcanza a cumplir con las necesidades de cada uno de los estudiantes y padres de familia que existen en la Unidad Educativa Salesiana "Domingo Comín"?
Si _____ No _____ No sabe _____

¿Cree Ud. que las instalaciones son las más adecuadas para abarcar la cantidad de estudiantes en la Unidad Educativa Salesiana "Domingo Comín"?
Si _____ No _____ No sabe _____

¿Considera Ud. que el número de laboratorios de computación cuentan con equipos de última tecnología?
Si _____ No _____ No sabe _____

¿La Unidad Educativa Salesiana "Domingo Comín" cuenta con un área para labores exclusivas de seguridad de la información?
Si _____ No _____ No sabe _____

¿Los incidentes de seguridad de los sistemas de información son reportados inmediatamente por los usuarios?
Si _____ No _____ No sabe _____

¿En caso de alguna falla de cableado de datos se encuentran preparados para su pronta reparación?
Si _____ No _____ No sabe _____

¿Cuenta con un usuario especifico creado para uso del equipo de cómputo?
Si _____ No _____ No sabe _____

¿Cierra sesión en su equipo de cómputo o lo bloquea mientras está ausente?
Si _____ No _____ No sabe _____

¿Ha compartido alguna vez su contraseña para ingresar en un equipo?
Si _____ No _____ No sabe _____

¿Cree que la información manejada por la Institución Educativa maneja alto nivel de confidencialidad?
Si _____ No _____ No sabe _____

¿Manejan controles de acceso para el ingreso de sistemas y manejo de información confidencial?
Si _____ No _____ No sabe _____

¿Su equipo de cómputo está protegido por un antivirus?
Si _____ No _____ No sabe _____

¿Considera la información como un activo valioso e importante para la Unidad Educativa?
Si _____ No _____ No sabe _____

¿Para ciertas áreas críticas tienen incorporado controles de ingreso para el personal?
Si _____ No _____ No sabe _____

¿Sabe si se les da un debido mantenimiento al hardware y software en la Unidad Educativa Salesiana Domingo Comín?
Si _____ No _____ No sabe _____

¿Cuentan con un control de inventario actualizado y automatizado?
Si _____ No _____ No sabe _____

¿Manejan algún plan de contingencia para incidentes con equipos?
Si _____ No _____ No sabe _____

¿Cuentan con algún plan de continuidad de las operaciones de la Institución?
Si _____ No _____ No sabe _____

Anexo # 2

Universidad Politécnica Salesiana
Encuestas previas a la obtención del título de Ingeniería en Sistemas

Nombre Encuestado/a: Stalin Abad

Cargo: Coordinador Sistemas

¿Considera Ud. que el número del personal docente y administrativo alcanza a cumplir con las necesidades de cada uno de los estudiantes y padres de familia que existen en la Unidad Educativa Salesiana "Domingo Comín"?

Si ✓ No _____ No sabe _____

¿Cree Ud. que las instalaciones son las más adecuadas para abarcar la cantidad de estudiantes en la Unidad Educativa Salesiana "Domingo Comín"?

Si ✓ No _____ No sabe _____

¿Considera Ud. que el número de laboratorios de computación cuentan con equipos de última tecnología?

Si _____ No ✓ No sabe _____

¿La Unidad Educativa Salesiana "Domingo Comín" cuenta con un área para labores exclusivas de seguridad de la información?

Si _____ No ✓ No sabe _____

¿Los incidentes de seguridad de los sistemas de información son reportados con inmendiamente por los usuarios?

Si _____ No ✓ No sabe _____

¿En caso de alguna falla de cableado de datos se encuentran preparados para su pronta reparación?

Si _____ No ✓ No sabe _____

¿Cuenta con un usuario especifico creado para uso del equipo de cómputo?

Si ✓ No _____ No sabe _____

Universidad Politécnica Salesiana
Encuestas previas a la obtención del título de Ingeniería en Sistemas

¿Cierra sesión en su equipo de cómputo o lo bloquea mientras está ausente?

Si ✓ No _____ No sabe _____

¿Ha compartido alguna vez su contraseña para ingresar en un equipo?

Si _____ No ✓ No sabe _____

¿Cree que la información manejada por la Institución Educativa maneja alto nivel de confidencialidad?

Si _____ No ✓ No sabe _____

¿Manejan controles de acceso para el ingreso de sistemas y manejo de información confidencial?

Si _____ No ✓ No sabe _____

¿Su equipo de cómputo está protegido por un antivirus?

Si ✓ No _____ No sabe _____

¿Considera la información como un activo valioso e importante para la Unidad Educativa?

Si ✓ No _____ No sabe _____

¿Para ciertas áreas críticas tienen incorporado controles de ingreso para el personal?

Si _____ No ✓ No sabe _____

¿Sabe si se les da un debido mantenimiento al hardware y software en la Unidad Educativa Salesiana Domingo Comín?

Si ✓ No _____ No sabe _____

¿Cuentan con un control de inventario actualizado y automatizado?

Si _____ No ✓ No sabe _____

¿Manejan algún plan de contingencia para incidentes con equipos?

Si _____ No ✓ No sabe _____

¿Cuentan con algún plan de continuidad de las operaciones de la Institución?

Si _____ No ✓ No sabe _____

Anexo # 3

UNIDAD EDUCATIVA FISCOMISIONAL SALESIANA "DOMINGO COMÍN"
GUAYAQUIL - ECUADOR

Guayaquil, 25 de Marzo del 2015

SEÑORES
UNIVERSIDAD POLITECNICA SALESIANA
SEDE GUAYAQUIL
ECUADOR

Estimados, por medio de la presente, yo STALIN OLMEDO AGUAYO encargado del departamento de sistemas en la UNIDAD EDUCATIVA SALESIANA "DOMINGO COMIN" certifico que las alumnas BLANCA STEPHANYE DELGADO PIJAL y JOSELYNE GABRIELA GARCIA BARRERA entregaron la copia de su proyecto de tesis nombrado como "ANÁLISIS DE REQUISITOS DE TECNOLOGÍA DE INFORMACIÓN PARA LA APLICACIÓN DE TÉCNICAS DE SEGURIDAD BAJO LA NORMATIVA NTE INEN-ISO/IEC 27001:2011 EN LA UNIDAD EDUCATIVA SALESIANA DOMINGO COMÍN".

Les agradezco por la atención a la presente.

Ing. Stalin Aguayo Pérez

UNIDAD EDUCATIVA SALESIANA FISCOMISIONAL "DOMINGO COMIN" GUAYAQUIL

Me basta que sean jóvenes para amarlos...
Don Bosco

Av. Domingo Comín 205 y Callejón Daule
PBX: (04) 244 87 58 - 233 26 13
FAX: (04) 244 61 60