UNIVERSIDAD POLITECNICA SALESIANA
SEDE GUAYAQUIL

Facultad de: Ingeniería
CARRERA: Ingeniería en Sistemas

TESIS DE GRADO

Previa la obtención del Títulos de:

INGENIERO EN SISTEMAS CON MENCIÓN EN TELEMÁTICA

TEMA:

"ANÁLISIS E IMPLEMENTACIÓN DE LA NORMA ISO 27002 PARA EL DEPARTAMENTO DE SISTEMAS DE LA UNIVERSIDAD POLITÉCNICA SALESIANA SEDE GUAYAQUIL"

Autores:
Sr. Daniel Romo Villafuerte
Sr. Joffre Valarezo Constante

Director de Tesis:
Ing. Javier Ortiz

GUAYAQUIL – ECUADOR

2012

DECLARACIÓN EXPRESA

La responsabilidad del contenido de este Proyecto de Grado, Corresponde exclusivamente a los autores; y el patrimonio intelectual de la misma a la Universidad Politécnica Salesiana.

Guayaquil, Agosto 14 del 2012

_____ _____

Daniel Romo Villafuerte **Joffre Valarezo Constante**

DEDICATORIA

A mis padres por el apoyo incondicional en todo momento y en cada etapa de mi vida, por ser un ejemplo a seguir.

Y en especial a mi hija Bianca Romo Pinto y esposa por demostrarme siempre que son mi fuerza para superar todos los obstáculos y salir adelante por ellas.

Daniel Romo Villafuerte

DEDICATORIA

A mi familia, pues con sus enseñanzas, buenas decisiones y sobre todo amor han ayudado en mi crecimiento como persona y profesional.

Y en especial a mi hijo José Ricardo y esposa por su constancia, dedicación y sacrificio.

Joffre Valarezo Constante

AGRADECIMIENTO

En primer lugar quiero dar gracias a Dios por haber guiado mi camino, por bendecirme para llegar a esta etapa de mi vida y hacer realidad este sueño tan anhelado; en segundo lugar a cada uno de mi familia a mi PADRE, mi MADRE, a mi ESPOSA e HIJA los cuales siempre me alentaron para seguir adelante y terminar esta etapa.

Daniel Romo Villafuerte

AGRADECIMIENTO

Quiero agradecer a mis padres, hermanos, esposa e hijo que con su apoyo, confianza, motivación de terminar esta carrera, han dejado una palabra más en este proyecto y nunca dejaron de estar pendientes en el desarrollo de mi carrera.

De igual manera agradezco a los profesores, directores de carrera y a la Universidad Politécnica Salesiana por brindarme la oportunidad de aprender y de compartir experiencias, casos prácticos y profesores totalmente preparados, lo cual hace que tengamos un excelente nivel académico y podamos mejorar la situación actual de nuestro país.

Joffre Valarezo Constante

RESUMEN

El presente trabajo busca informar y orientar al lector en todo lo que corresponda las buenas prácticas de seguridad de la información; las mismas que fueron creándose con el pasar del tiempo y todas las estafas por fuga de información sean está impresa o no.

En el primer capítulo podremos observar una pequeña pero importante introducción en la que se podrá destacar la necesidad y evolución de las buenas prácticas de seguridad, así mismo se darán a conocer objetivos tanto generales como específicos que se tuvieron presentes en la elaboración de este proyecto, se planteará algunos casos de los problemas más frecuentes que surgieron con la carencia de normas y/o políticas de seguridad de la información.

En el segundo capítulo se profundizará más en el tema dando a conocer terminología básica y sustentando cada una de las partes que conforman esta tesis en las buenas prácticas de seguridad.

En el capítulo 3 se presentará la Guía para el cumplimiento de Políticas de Seguridad de la Información, donde se detallará las buenas prácticas que el departamento de sistemas de la Universidad Politécnica Salesiana sede Guayaquil debe seguir y cumplir paso a paso para poder adquirir el conocimiento necesario que le permitirá en base a las políticas establecer controles de seguridad, y a su vez, para mitigar riesgos como por ejemplo fuga de información.

ÍNDICE GENERAL

Índice Inicial

Contenido

ÍNDICE DE CUADROS

ÍNDICE DE GRÁFICOS

CAPITULO 1

1. ASPECTOS GENERALES

1.1. Antecedentes de la investigación

En la investigación realizada en el departamento de Sistemas de la Universidad Politécnica Salesiana sede Guayaquil se pudo detectar la falta de políticas o normas de seguridad de la información, es por eso que se planteo el presente proyecto para el análisis e implementación de una norma internacional como es la ISO 27002 la cual ayudará al departamento de Sistemas a la protección de los activos de información de la Universidad Politécnica Salesiana.

Hoy en día existen muchas herramientas que de forma relativamente fácil se logra tener acceso a personas no autorizadas y llegar hasta la información que la organización tiene protegida, cuando los controles no están bien definidos logran su objetivo con poco esfuerzo y conocimiento, causando graves perjuicios para la empresa.

Para la protección de los activos de información nos basaremos en los pilares fundamentales de la seguridad de la información que son disponibilidad, integridad y confidencialidad, partiendo de los pilares de seguridad se definirán las políticas a seguir por el personal docente, administrativo y externos.

Con la ejecución del presente proyecto dará lugar a la un análisis e investigaciones de lo que actualmente la Universidad Politécnica Salesiana sede Guayaquil cuenta para la protección de la información.

1.2. Planteamiento del problema

Una de las principales preocupaciones del departamento de sistemas de la Universidad Politécnica Salesiana sede Guayaquil, debe ser el control de los riesgos que atentan contra la Seguridad de la Información de sus activos, entre estos, equipos informáticos, servicios, datos, recursos humanos y equipamiento auxiliar. Una observación rigurosa, se llego a la conclusión, que los colaboradores de la Universidad Politécnica Salesiana (personal docente, administrativo y de servicio), cuentan con altos factores de inseguridad, fuga de información que si no se tratan adecuadamente pueden ocasionar posibles daños económicos y de prestigio para la Universidad Politécnica Salesiana.

Si no se tiene controles de buenas prácticas, normas de seguridad, podría explotar alguna amenaza y causar un riesgo a los activos de información originando así hasta una probabilidad alta que las pérdidas económicas para la Universidad Politécnica Salesiana ocurran.

Una de las maneras de reducir los riesgos que están afectando a los activos es de la elaboración de normas, políticas y concientización a los usuarios, basados en norma de buenas prácticas de seguridad para reducir la probabilidad de ocurrencia de un impacto de los riesgos que están expuestos los activos de información de la Universidad Politécnica Salesiana.

1.3. Justificación.

Los activos de información son recursos que representan una gran importancia y costos vitales para la Universidad Politécnica Salesiana sede Guayaquil. Si estos activos llegaran a fallar o tener un daño, quedaría fuera de línea el negocio en especial en horarios con los que los sistemas de procesamiento de información intervienen y por tal razón la Universidad Politécnica Salesiana tienen el deber y obligación de preservarlos, utilizarlos y mejorarlos. Esto implica que para tomar las acciones apropiadas sobre la

Seguridad de la información y los sistemas informáticos, estas decisiones deben ser basadas en la protección de muchas clases de amenazas y riesgos tales como fraude, sabotaje, espionaje industrial, extorsión, violación de la privacidad, intrusos, hackers, interrupción de servicio, accidentes y desastres naturales que todos los activos están expuestos.

La Universidad Politécnica Salesiana deberá realizar la protección de la información de acuerdo al valor y nivel de importancia. Las medidas de seguridad implementadas deben de aplicarse sin importar cómo la información se guarda (en papel o en forma electrónica), o como sea procesada (PCs, correo de voz, etc.), o cómo se la transmite (correo electrónico). Todas las medidas de protección deberán incluir controles de acceso a los usuarios para garantizar la disponibilidad, integridad y confidencialidad basadas en funciones del cargo que desempeña el usuario.

La finalidad del Manual de Políticas de Seguridad de la Información que se desea implementar en este proyecto es proporcionar instrucciones específicas sobre cómo proteger los activos de la Universidad Politécnica Salesiana ya sean estos computadores de la organización (conectados o no), como toda la información guardada en ellos. La violación de dichas políticas está sujeta a medidas disciplinarias e incluso el despido.

Otras de las razones por las que creemos conveniente el desarrollo de este proyecto es el creciente avance de la tecnología y software en nuestro país así como también el avance en formas y manías de las amenazas que nuestro activo más valioso la Información.

1.4. Objetivos

1.4.1. Objetivo general.

- Impedir accesos no autorizados y violaciones de las normas reglamentos, contratos, políticas y procedimientos de los estándares de

seguridad de la información definidos en la Universidad Politécnica Salesiana. El cumplimiento de las políticas y estándares de seguridad de la información debe ser observado por todo el personal tanto docente como administrativo de la Universidad Politécnica Salesiana.

1.4.2. Objetivos específicos.

- Comprender toda la protección de la información contra acceso, modificación o divulgación no autorizada así como también servirá para garantizar la disponibilidad de la información. El cumplimiento de estas políticas debe ser observado por todo el personal tanto administrativo como docente.

- Promover las mejores prácticas de seguridad al desarrollo o adquisición de sistemas de información.

- Implementar las normas de seguridad y concientizar al usuario de dichas normas para la protección de los activos de información.

1.5. Marco teórico

1.5.1. Información

La información es un activo que representa un gran valor dentro de la organización, sea este tangible o intangible, por lo tanto requiere una protección adecuada ya sea por diferentes medios o técnicas de seguridades implantadas. Para estos hay que tomar muy en cuenta el creciente ambiente interconectado de negocios es por esto que la información está expuesta a un mayor rango de amenazas y vulnerabilidades.

"La información es un activo que, como otros activos comerciales importantes, tiene valor para la organización y, en consecuencia, necesita ser protegido adecuadamente". [1]

Al hablar de información nos referimos, sin importar la forma que esta adopte, como documentación impresa o escrita, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en video o hablada en conversación. Este activo se debería proteger de forma correcta mediante los controles de seguridad independientemente de la forma que este tome o los medios por los que se comparta o almacene.

El buen funcionamiento de una organización depende de la información, el cual es uno de los activos más valiosos. El proteger su integridad, confidencialidad y disponibilidad es un punto clave para lograr los objetos comprometidos del negocio. Por esta razón, año a año la organización ha invertido en medios necesarios para evitar el robo y manipulación de sus datos confidenciales ya sean estos por accesos no autorizados o fuga de información.

Actualmente el desarrollo de las nuevas tecnologías ha tomado un rumbo esencial a la estructura del negocio, así mismo ha aumentado los riesgos que las empresas tienen en sus diferentes activos y se exponen a nuevas amenazas.

[1] National Information Systems Security (INFOSEC) Glossary, NSTISSI No. 4009, January 2000

Gráfico #1

Amenazas para la Seguridad

Fuente: Segu-Info, Seguridad de la Información - www.cfbsoft.com.ec

Elaborado por: www.cfbsoft.com.ar

Como paso inicial para la protección de los activos de información de nuestras organizaciones frente a todas las amenazas es necesario realizar un estudio, conocerlas y gestionarlas de forma adecuada. Para ello debemos ejecutar procedimientos adecuados, implementar controles de seguridad basados en la evaluación de los riesgos.

1.5.2. Seguridad de la Información

La seguridad de la información se refiere a la protección de una gama de amenazas para salvaguardar la continuidad de las operaciones del negocio sean estas ocasionadas dentro o fuera de la organización, disminuyendo los daños que estas amenazas causarían a la organización y aumentar las oportunidades de negocios.

"Seguridad de los Sistemas de Información consiste en la protección de los sistemas de información respecto al acceso no autorizado o modificación de la información en el almacenamiento, proceso y tránsito y contra la denegación de servicio para los usuarios

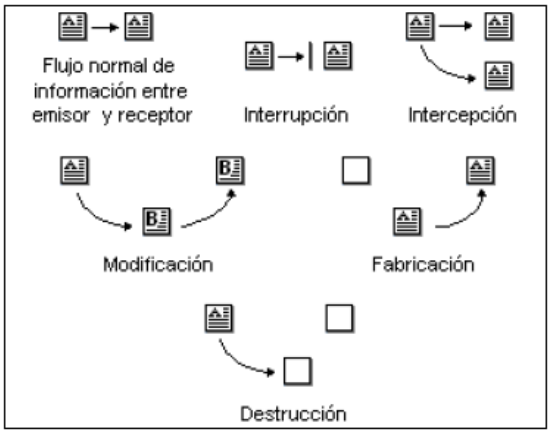
autorizados, incluyendo aquellas medidas necesarias para detectar, documentar y contrarrestar dichas amenazas." [2]

La seguridad de la información se consigue desarrollando mediante un conjunto de controles efectivos, que pueden ser políticas, prácticas, manual de funciones, procedimientos, estructuras organizativas, planes de contingencia y funciones de software y hardware. Estos controles necesitan ser establecidos, implementados, monitoreados, revisados y mejorados donde sea necesario, para asegurar que se cumplan los objetivos específicos de seguridad y negocios de la organización.

En los sistemas de información es donde la mayor parte de la información procesada o no procesada es resguardada, ya sea en equipos informáticos, soportes de almacenamiento y redes de datos. Estos sistemas de información son activos que están sujetos a vulnerabilidades y amenazas que pueden influir desde personal de la propia organización o del exterior.

Gráfico #2

Tipos de ataques a activos



Fuente: CERT, Software Engineering Institute - www.cert.org

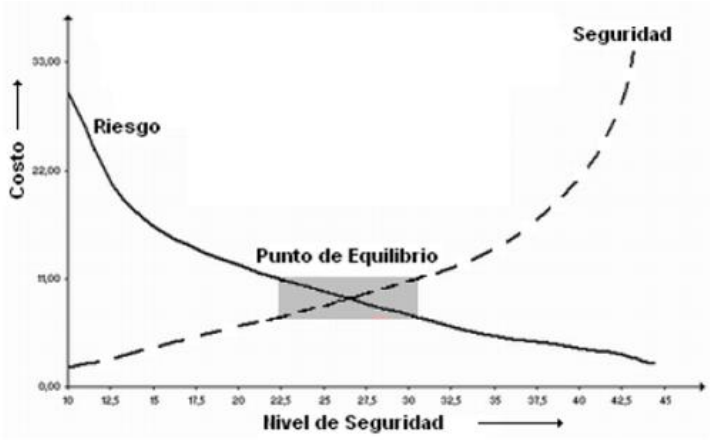
Elaborado por: Howard, John D.

[2] Irwin Valera Romero, Auditorias de Sistemas, pag.2

Existen un sin número de riesgos físicos como incendios, inundaciones, terremotos o terrorismos que al explotar una amenaza pueden afectar la disponibilidad de nuestra información y recursos al no estar preparados contra cualquier probabilidad de ocurrencia del riesgos y no contar con un plan de continuidad del negocio nos afectaría significantemente. Es por eso que se debe realizar una evaluación de riesgos de forma periódica estableciendo un punto de equilibrio en relación de costo – beneficio.

Gráfico #3

Punto de equilibrio costo – seguridad



Fuente: Segu-Info, Seguridad de la Información - www.cfbsoft.com.ec

Elaborado por: Cristian Borghello

Además de los riesgos físicos, también nos encontramos con los riesgos lógicos relacionados con la tecnología y, que como se citó anteriormente aumentan día a día, estos pueden ser hackers, robos de identidad, accesos no autorizados, spam, virus, robos de información y espionaje industrial, estos afectan directamente con la confidencialidad que la organización transmite a sus clientes y al verse comprometida la confidencialidad afecta a nuestra imagen en el mercado.

1.5.3. Bases de la Seguridad de la Información.

"*La Seguridad de la Información está apoyada en 3 pilares fundamentales de la seguridad estos son:*" [3]

- Disponibilidad.
- Integridad.
- Confidencialidad.

1.5.4. Pilares fundamentales de Seguridad de la Información.

Confidencialidad: Certificar que solo los usuarios con accesos autorizados puedan acceder a la información. La seguridad que se implementará debe asegurar que solo las personas tengan acceso a la información que fueron autorizados.

Integridad: Certificar la protección de la información en cuanto a la exactitud y totalidad de los datos y los métodos de procesamiento ingresados por los usuarios con acceso autorizado. La pérdida de integridad en la información puede deberse a errores humanos, modificaciones intencionales, o alguna contingencia por métodos inusuales y al modificar estos datos inapropiadamente, estos se convierten en defectuosos, y en ocasiones peligrosos para el negocio y la toma de decisiones.

Disponibilidad: Certificar que los usuarios previamente autorizados a la información y sus activos asociados tengan acceso cuando lo requieran. Los recursos deben estar disponibles cuando se necesite usarlos.

3 Seguridad de la Información, Los pilares de la seguridad de la información. Dirección URL: <http://info-segur.blogspot.ca/?m=1>

Gráfico #4

Pilares Fundamentales de la Seguridad de la Información.

Fuente: Los pilares de la seguridad Informática - http://seguridaddeinformacion.bligoo.com/los-pilares-de-la-seguridad-informatica
Elaborado por: Daniel Romo y Joffre Valarezo

1.5.5. Características de Seguridad de la Información.

Autenticidad: Asegura el origen de la información, la identidad de usuarios al momento de un acceso debe ser validada, de modo que se puede demostrar que es quien dice ser.

No repudio: Imposibilidad de negación ante terceros del envío y/o recepción por parte del emisor y/o receptor de la información.

Trazabilidad: Es el conjunto de acciones, medidas y procedimientos técnicos que permite autenticar y registrar (No repudio) la información desde que esta es enviada al usuario hasta que este último la recibe

1.5.6. La necesidad de la Seguridad de Información

En la actualidad la información y los procesos en los que están apoyados, los sistemas y redes son activos de una gran importancia para la organización. Limitar, ejecutar, conservar y optimizar la seguridad de información, pueden ser fundamentales para conservar la competitividad.

Cada vez más, las empresas y sus sistemas de información afrontan una gama de riesgos y huecos de seguridad como fraudes establecidos en informática, ingeniería social, sabotaje, terrorismos, vandalismo, desastres naturales.

Ciertos orígenes de los riesgos como virus informáticos, negación de servicios y ataques de intrusión cada día estos riesgos a los que todo sistema de información están expuestos se están volviendo cada vez más frecuentes y sofisticados.

Toda organización ya sea pública o privada independientemente del tipo del negocio tienen presente la importancia de la seguridad de la información para poder contar con una protección adecuada de las infraestructuras críticas del negocio.

Para poder explotar y lograr en ambos sectores públicos y privados, el gobierno electrónico o el comercio electrónico, se debe tener gestionada la seguridad de información permitirá evitar y reducir los riesgos que conllevan la implementación de estas tecnologías.

En el desarrollo de los sistemas de información no están siendo diseñados con una seguridad al 100% ya que la seguridad que puede conseguirse a través de los medios técnicos es limitada, y debería sustentarse en una gestión y procedimientos.

En cuanto a los controles que se deberían implementar demanda una planificación meticulosa y una investigación al detalle. Para la implementación de la gestión de la seguridad de la información requiere, como requisito mínimo, la participación de todos los empleados de la organización.

Y además se deberá incluirá la participación de los proveedores, consumidores o socios. Para contemplar la gestión de seguridad de la información se necesitará la asesoría especializada de organismos externos.

1.5.7. Establecer requisitos de seguridad

La organización debe identificar sus requisitos de seguridad. Fundamentalmente son tres requisitos principales.

El primer requisito se enfoca en los objetivos y estrategias generales del negocio la cual permite realizar la valoración de los riesgos de la

organización, con este requisito se identifican las amenazas de los activos, se calcula la vulnerabilidad y la probabilidad de su ocurrencia para realizar una probabilidad de su posible impacto en el negocio.

EL segundo requisito es el conjunto de requisitos legales, estatutos, regulaciones y contratos que satisface a la organización, sus accionistas, socios comerciales y los proveedores.

El tercer requisito está basado en los principios, objetivos y requisitos del tratamiento de la información que la organización ha desarrollado para sus operaciones.

1.5.8. Punto de partida de la seguridad de la información

El punto de partida de la seguridad de la información se considera principios orientativos a un número de controles los cuales apoyan a la inicialización para implantar la seguridad de la información.

Los puntos de partida de la seguridad de la información se los divide en 2 grandes grupos:

1. Controles desde el punto de vista legislativo.

   a) Protección de los datos de tipo personal.
   b) Salvaguardas de los requisitos de la organización.
   c) Derechos de propiedad privada.

2. Controles de mejores prácticas habituales.

   a) Documentación de la política de seguridad de la información.
   b) Asignación de responsabilidades.
   c) Formación y capacitación
   d) Procedimiento correcto en las aplicaciones.

e) Gestión de la vulnerabilidad técnica

f) Gestión de la continuidad del negocio

g) Registro de las incidencias de seguridad y las mejoras

Nota: Estos controles están diseñados para que sean adaptables a las organizaciones y en los diferentes ambientes.

1.5.9. Políticas de Seguridad

Una Política de Seguridad es una técnica de los activos de la organización y la forma en que se debe de gestionar ellos debe y pueden ser protegidos adecuadamente, informando que está permitido y que no, así como la responsabilidad de protección de los recursos que deben asumir todos los miembros de la organización.

"Son una forma de comunicación con el personal, ya que las mismas constituyen un canal formal de actuación, en relación con los recursos y servicios informáticos de la organización. Esta a su vez establecen las reglas y procedimientos que regulan la forma en que una organización previene, protege y manea los riesgos de diferentes daños, sin importar el origen de estos." [4]

Con la implementación del Manual de Políticas de Seguridad de la información de la Universidad Politécnica Salesiana se pretende lograr que los colaboradores de la institución se rijan a las normas expuesta en el documento para así asegurar que los bienes y recursos sean y estén utilizados de una manera correcta, asegurando también que la información este debidamente protegida, para tal efecto se debe realizar la difusión y concientización a los empleados de lo que deberán cumplir para proteger todos activos de la organización.

[4] Universidad de Oriente UNIVO, Manual de Normas y Políticas de Seguridad Informática, pág. 8.

El objetivo principal de las políticas de seguridad es de proteger, prevenir y gestionar los daños que estos tengan cuando una de las vulnerabilidades a los cuales están en constante riesgos explota, esto se consiguen con normas, reglas y procedimientos concretos por personas especializadas o un sistema en particular.

1.5.10. ¿Cuándo escribir políticas de seguridad?

Las políticas de seguridad deberían ser diseñadas y elaboradas dentro de la organización en cualquier momento, siendo necesaria que estas sean documentadas formalmente.

- Antes de que se produzcan ataques.
- Luego de que ha ocurrido un ataque.
- Para evitar problemas legales
- Antes de una auditoria
- Al iniciar una organización

1.5.11. Modificar las políticas de seguridad

Las políticas de seguridad diseñadas e implementadas en una empresa cumplen un ciclo de vida dentro de esta, es por ello que están propensas a cambios, mejoras o eliminación.

Las causas por las que se llega a la modificación de las políticas de seguridad son las siguientes:

- Cambios en la tecnología empleada en la organización.
- Implementación de nuevos proyectos de software.
- Necesidades de regulaciones vigentes.
- Requerimientos especiales de clientes o proveedores.
- Cambios del negocio.

1.5.12. ¿Qué protege una política de seguridad?

La certificación ISO 17799 define una política de seguridad como un documento que ofrece instrucciones de administración y soporte para la seguridad de la información de acuerdo con los requisitos empresariales y las leyes y reglamentaciones relevantes.

Durante el proceso de desarrollo de software es importante utilizar estas políticas como guía para todas las funcionalidades de seguridad que serán desarrolladas.

Este punto es sutil, pero es fundamental comprenderlo. La política de seguridad de la aplicación no debe ser definida por el proceso de desarrollo sino que solamente debe implementar los requisitos de seguridad establecidos en una organización.

Recuerde que la aplicación que desarrolle debe adaptarse al modelo de seguridad del usuario, ya sea que se trate de su empresa o de sus clientes.

1.5.13. La seguridad es descuidada.

En varios esfuerzos de desarrollo de software, la seguridad frecuentemente se implementa en un momento posterior. De hecho, con frecuencia la seguridad no es considerada en el proceso de desarrollo en absoluto.

Un motivo para que esto suceda es la poca importancia que las organizaciones asignan al desarrollo de software seguro. La parte alarmante es que las compañías a menudo ni siquiera se dan cuenta de que están haciendo esto. Sin embargo esto ocurre, y hay una continua falta de políticas de seguridad disponibles durante la etapa

de diseño de las aplicaciones. Esto frecuentemente resulta en la omisión de funcionalidades de seguridad en la capa de aplicación.

En otro escenario común, los arquitectos de aplicaciones intentan implementar la seguridad sin utilizar una política corporativa. Cuando la seguridad es añadida de esta manera, su efectividad se ve reducida y no existe garantía que las amenazas reales estén siendo tratadas.

He preguntado a varias organizaciones de desarrollo por qué no diseñan e implementan la seguridad como una funcionalidad. Una razón que mencionan es la falta de políticas disponibles para el personal de desarrollo. En algunas organizaciones, la seguridad informática frecuentemente se considera como responsabilidad del proveedor del sistema operativo. En general la seguridad se considera como costosa de implementar y a menudo se deja de lado debido a restricciones de tiempo y dinero.

No estoy de acuerdo con estas acciones y creo que la seguridad es realmente responsabilidad de todos. Los desarrolladores de software corporativo y de terceros deben garantizar que sus aplicaciones no introduzcan riesgos adicionales en el entorno operativo. Como los sistemas operativos son cada vez más seguros, los atacantes de software buscan blancos más sencillos.

1.5.14. Importancia de las políticas de seguridad

Es fundamental para las compañías reconocer la necesidad de políticas de seguridad de aplicaciones porque sin tales políticas no existe una forma confiable de definir, implementar y hacer cumplir un plan de seguridad entro de una organización.

¿El plan se seguridad física de su compañía incluye por ejemplo políticas y procedimientos relacionados con accesos y salidas, o la existencia de alarmas de incendios o el acceso a zonas restringidas? Si usted considera que su aplicación forma parte de este mismo entorno físico, será más sencillo ver cómo este software, que por ejemplo puede administrar su nómina de pagos e información contable, requiere el mismo proceso de pensamiento para la seguridad que el acceso físico a los activos materiales de su empresa.

Cuando existe una política de seguridad disponible para el equipo de desarrollo, pueden integrar fácilmente la política en la aplicación como una funcionalidad. Si su compañía se encuentra en el extremo de compra de una aplicación, la política de seguridad que se aplicó en el desarrollo de la aplicación ofrece funcionalidades de seguridad que deben tornar el paquete de software aceptable para su corporación.

Existen beneficios reveladores en la implementación de políticas de seguridad en el proceso de desarrollo de aplicaciones. La disponibilidad de los requisitos de seguridad en la política hace posible que el equipo de desarrollo pueda crear un software con una mentalidad de privilegios mínimos de tal forma que pueda implementarse con una mínima superficie de ataque en un entorno operativo restringido.

Asimismo, los colaboradores pueden acoger las nuevas políticas de seguridad para las configuraciones requeridas en la institución.

1.5.15. Estructura de este estándar

Esta norma ISO 27002 contiene 11 dominios de control y controles de seguridad de la información, los cuales contienen un total de 39 sub dominios principales de seguridad.

1.5.16. Dominios

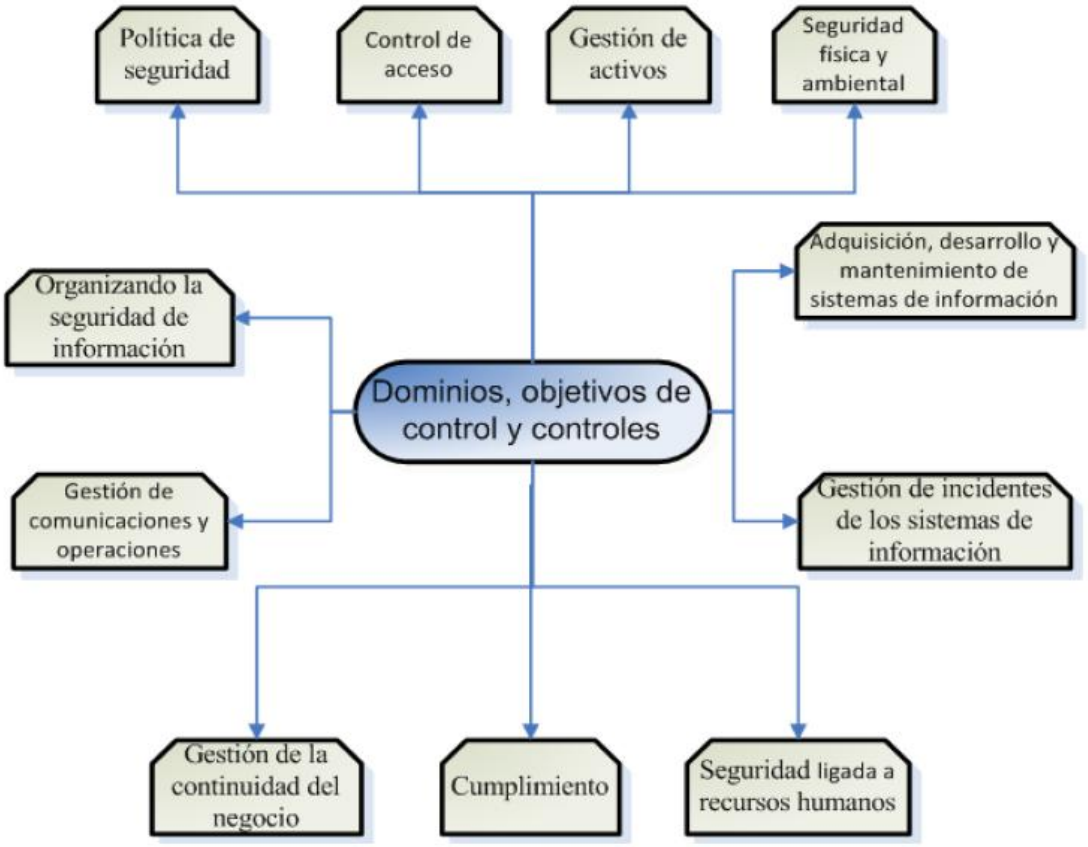
"Cada dominio contiene un número de dominios de seguridad. Estos 11 dominios son:" [5]

- Política de seguridad (1 control)
- Organizando la seguridad de información (2 controles)
- Gestión de activos (2 controles)
- Seguridad ligada a recursos humanos (3 controles)
- Seguridad física y ambiental (2 controles)
- Gestión de comunicaciones y operaciones (10 controles)
- Control de acceso (7 controles)
- Adquisición, desarrollo y mantenimiento de sistemas de información (6 controles)
- Gestión de incidentes de los sistemas de información (2 controles)
- Gestión de la continuidad del negocio (1 control)
- Cumplimento

5 ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: http://iso27002.wiki.zoho.com

Gráfico #5

Los dominios de control de ISO 27002:2005



Fuente: ISO/IEC 27002:2005 http://www.iso27001security.com/html/27002.html
Elaborado por: ISO/IEC 27002:2005 http://www.iso27001security.com/html/27002.html

La norma ISO/IEC 27002:2005 es una herramienta sencilla que permitirá establecer políticas, y controles bajo el objetivo de disminuir los riesgos que tienen los activos de la organización. En primer lugar, obtenemos una reducción de riesgos debido al establecimiento y seguimiento de controles sobre ellos. Con ello lograremos reducir las amenazas hasta alcanzar un nivel asumible por nuestra organización.

De este modo si se produce una incidencia, los daños se minimizan y la continuidad del negocio está asegurada. En segundo lugar se produce un ahorro de costes derivado de una racionalización de los recursos.

Se eliminan las inversiones innecesarias e ineficientes como las producidas por desestimar o sobrestimar riesgos. En tercer lugar, la seguridad se considera y se convierte en una actividad de gestión. La seguridad deja de ser un conjunto de actividades más o menos organizadas y pasa a transformarse en un ciclo de vida metódico y controlado, en el participa toda la organización.

En cuarto lugar, la organización se asegura del cumplimiento de la legislación vigente y se evitan riesgos y costes innecesarios. La entidad se asegura del cumplimiento del marco legal que protege a la empresa de aspectos que probablemente no se habían tenido en cuenta anteriormente.

Por último, pero no por ello menos importante, la certificación del sistema de gestión de seguridad de la información contribuye a mejorar la competitividad en el mercado, diferenciando a las empresas que lo han conseguido y haciéndoles más fiables e incrementando su prestigio.

1.6. Marco conceptual

Accesos autorizados: Autorizaciones concedidas a un usuario para la utilización de los diversos recursos.

Activo: Cualquier cosa que tenga valor para la organización.

Amenaza: Sinónimo de un evento interno o externo que pueden causar daño a la empresa.

Ataque: Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.

Auditoria: Examinar de forma independiente los log's del sistema y actividades para comprobar la eficiencia y controlar la integridad de los datos.

Autorización: Garantizar que todos los accesos a datos y/o transacciones que los utilicen, cumplan con los niveles de autorización correspondientes para su utilización y divulgación.

Autenticidad: La información es lo que dice ser o el transmisor de la información es quien dice ser.

Confidencialidad: Información solo disponible a personas autorizadas.

Control de acceso: Mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

Controles: Políticas o procedimientos que aplican a una vulnerabilidad.

Desastre o Contingencia: Interrupción de la capacidad de acceso a información y procesamiento de la misma a través de computadoras necesarias para la operación normal de un negocio.

Disponibilidad: Que la información esté disponible cuando se la necesite.

Dominios de la Norma: Estructura más general de la norma ISO27002, dentro de esta se encuentran los objetivos de control y los controles.

Gusanos (Worms): Son programas independientes (no necesitan insertarse en otros archivos) que se expanden a través de la red realizando distintas acciones como instalar virus, o atacar una PC como un intruso.

Hacker (pirata): Una persona que goza alcanzando un conocimiento profundo sobre el funcionamiento interno de un sistema, de un ordenador o de una red de ordenadores. Este término se suele utilizar indebidamente como peyorativo, cuando en este último sentido sería más correcto utilizar el término cracker. Los hackers proclaman tener una ética y unos principios contestatarios e inconformistas pero no delictivos.

Identificación: Procedimiento de reconocimiento de la identidad de un usuario.

IEC: International Electrotechnical Commission, Comisión Electrotécnica Internacional.

Impacto: Consecuencia de la materialización de una amenaza.

Integridad: Información va a estar completa y correcta.

ISO: International Organization for Standardization, Organización Internacional de Estandarización.

Manual: Es el documento que contiene la descripción de actividades, normas que deben seguirse. Estos documentos deben de ser aprobados por la Gerencia.

Políticas: Un conjunto de reglas que sean compresibles para toda la audiencia a quien va dirigido.

Propiedad: (derecho a propiedad) Asegurar que todos los derechos de propiedad sobre la información utilizada en el desarrollo de las tareas, estén adecuadamente establecidos a favor de sus propietarios.

Proveedores: Persona que provee o abastece a otra persona de lo necesario o conveniente para un fin determinado. Empresa que se dedica a proveer o abastecer de productos necesarios a una persona o empresa.

Registro: Es una evidencia de que lo que se dice se ha cumplido, es un aval que permite presentar que se está cumpliendo con lo acordado.

Riesgo: Es la probabilidad de que una amenaza sea explotada por las vulnerabilidades.

Seguridad de la información: Preservación de la confidencialidad, disponibilidad e integridad de la información.

SGSI: Sistema de Gestión de Seguridad de la Información.

Sistemas de información: Conjunto de archivos automatizados, programas, soportes y equipos empleados para el almacenamiento y tratamiento de datos.

Software malicioso: (malware) Es un término común que se utiliza al referirse a cualquier programa malicioso o inesperado o a códigos móviles como virus, troyanos, gusanos o programas de broma.

Spam: Correo comercial no solicitado que se envía a través de Internet. El volumen y contenido del SPAM puede dificultar notablemente el uso de servicios de correo electrónico.

Terceros: Persona que es reconocida por ser independiente de las partes involucradas concerniente al tema en cuestión.

Trazabilidad: Poder asegurar en todo momento quien hizo y en cuando lo hizo.

UPS: Sistema de alimentación ininterrumpida. Fuente ininterrumpida de energía. Es un dispositivo eléctrico que puede proporcionar energía eléctrica ante un apagón gracias a sus baterías internas que almacenan energía eléctrica.

Usuario: Sujeto o proceso autorizado para acceder a datos o recursos.

Virus: El tipo más conocido de código malicioso. Programa que se copia dentro de otros programas e intenta reproducirse el mayor número de veces posible. Aunque no siempre es así, la mayoría de las veces el virus, además de copiarse, altera o destruye la información de los sistemas en los que se ejecuta. .

Vulnerabilidad: Es una debilidad, una falencia que podría atacar a las amenazas.

1.7. Hipótesis.

1.7.1. Hipótesis General.

El no tener implementadas normas internacionales de seguridad de la información para la Universidad Politécnica Salesiana sede Guayaquil, podrá provocar riesgos de pérdidas económicas, fuga de información

1.7.2. Hipótesis Particulares.

La falta de normas de seguridad en la Universidad Politécnica Salesiana sede Guayaquil trae como consecuencia que los riesgos asociados a los activos de información exploten y causen daños, paralizar las operaciones.

Proporcionar información más de la necesaria al presentarse errores en los sistemas de la Universidad Politécnica Salesiana, causaría pistas que podrían hacker dichos sistemas.

Controlar el cumplimiento de las políticas de Seguridad de la Información para la protección de los activos de información.

1.8. Variables.

1.8.1. Variables Dependientes.

- Riesgos de pérdidas económicas.
- Fuga de información.

1.8.2. Variables Independientes.

- No tener implementadas normas internacionales de seguridad de la información.

1.9. Matriz Causa – Efecto.

Tabla #1: Matriz Causa - Efecto

Fuente: Los Autores

MATRIZ CAUSA - EFECTO		
Formulación del Problema	**Objetivo General**	**Hipótesis general**
¿Qué normas de seguridad se están aplicando a la Universidad Politécnica Salesiana sede Guayaquil para salvaguardar la disponibilidad, integridad y confidencialidad de los activos de información?	Impedir accesos no autorizados y violaciones de las normas reglamentos, contratos, políticas y procedimientos de los estándares de seguridad de la información definidos en la Universidad Politécnica Salesiana. El cumplimiento de las políticas y estándares de seguridad de la información debe ser observado por todo el personal tanto docente como administrativo de la Universidad Politécnica Salesiana.	El no tener implementadas normas internacionales de seguridad de la información para la Universidad Politécnica Salesiana sede Guayaquil, podrá provocar riesgos de pérdidas económicas, fuga de información.
Sistematización del problema	**Objetivo especifico**	**Hipótesis especifica**
¿Qué consecuencias ocasionan la falta de normas de seguridad en la Universidad Politécnica Salesiana sede Guayaquil?	Comprender toda la protección de la información contra acceso, modificación o divulgación no autorizada así como también servirá para garantizar la disponibilidad de la información. El cumplimiento de estas políticas debe ser observado por todo el personal tanto administrativo como docente.	La falta de normas de seguridad en la Universidad Politécnica Salesiana sede Guayaquil trae como consecuencia que los riesgos asociados a los activos de información exploten y causen daños, paralizar las operaciones.
¿Qué seguridades existen con respecto a los sistemas de información desarrollados o adquiridos?	Promover las mejores prácticas de seguridad al desarrollo o adquisición de sistemas de información.	Proporcionar información más de la necesaria al presentarse errores en los sistemas de la Universidad Politécnica Salesiana, causaría pistas que podrían hacker dichos sistemas.
¿Cómo podría mejorar la Seguridad de la Información que se manejan en la Universidad Politécnica Salesiana sede Guayaquil?	Implementar las normas de seguridad y concientizando al usuario de dichas normas para la protección de los activos de información.	Controlar el cumplimiento de las políticas de Seguridad de la Información para la protección de los activos de información.

1.10. Población y muestra

El presente trabajo se llevó a cabo en la UNIVERSIDAD POLITECNICA SALESIANA SEDE GUAYAQUIL, la cual está ubicada en la ciudad de Guayaquil Chambers 227 y 5 de Junio, la muestra es conformada por el departamento de sistemas de la Institución.

"Una población es el conjunto de todos los individuos (objetos, personas, eventos, etc.) en los que se desea estudiar el fenómeno. Éstos deben reunir las características de lo que es objeto de estudio"[6]

"Una muestra es parte o porción extraída de un conjunto por métodos que permiten considerarla como representativa de él"[7]

Para recopilar la información y/o datos se manejarán técnicas como las encuestas y observación directa, empleando en los involucrados los diferentes módulos a desarrollar, recopilando así información para realizar un respectivo análisis de la seguridad de la información que cuentan en el momento del desarrollo.

1.11. Marco metodológico.

1.11.1. Tipo de Estudio.

Para poder realizar el manual de políticas de seguridad de la información necesitamos conocer la infraestructura tecnológica de la universidad y serán analizados cada proceso en base a las siguientes investigaciones:

[6] Latorre, Rincón y Arnal, 2003
[7] El Diccionario de la Lengua Española (RAE, 2001)

1.11.2. Tipo de investigación descriptiva

Podremos decir que este proyecto es de investigación descriptiva porque necesitamos trabajar con las actividades, procedimientos y características fundamentales que se tienen actualmente en la Universidad para poder comprobar los riesgos que existen en ella por la falta de políticas.

1.11.3. Tipo de investigación experimental

Es experimental, porque no solo vamos a identificar los riesgos en la universidad si no que se definirán políticas para poder reducir el riesgo.

1.11.4. Tipo de investigación mixta

También podríamos decir que el proyecto se desarrollara con investigación mixta porque las políticas que constaran en el manual serán en base a entrevistas al personal administrativo, por un formato (Check list), o revisando procedimientos actuales y todo esto para verificar que políticas aplicarían a los procesos de la universidad.

1.11.5. Tipo de investigación transversal

Es de investigación transversal porque la recolección de información para el desarrollo del manual de políticas será en un tiempo definido.

1.11.6. Método de Investigación

El método científico: Uno de los métodos de investigación que llevaremos a cabo es el científico ya que el proyecto se lo va a regir y alinearse con la norma ISO/IEC 27002:2005.

El método deductivo: Realizaremos método deductivo por lo que la norma ISO/IEC 27002:2005 control y controles de seguridad nos plantea una guía de implementación general para ser aplicada en todo tipo de organización:

El método inductivo: Finalmente se realizar el método inductivo, por el cual nos basaremos de datos particulares (lo investigado) para realizar políticas generales y detalladas.

1.11.7. Fuentes y técnicas para la recolección de información.

Para la obtención de la información nos regiremos a las siguientes técnicas:

Check list:

Para recoger la información relevante, desarrollaremos un Check list referente a los controles de gestión y operación planeados o usados en el Sistema de Información. Este Check list nos ayudara a seguir pasa a paso cada control de la norma ISO/IEC27002 y verificar su aplicabilidad.

Entrevistas Locales:

Las entrevistas al personal administrativo, de sistemas docente, la cual nos permitirán recoger información útil.

Visitas locales también nos permiten observar y juntar la información sobre la seguridad física, ambiental, y operacional del sistema de información.

Para sistemas todavía en la fase de diseño, la visita local podría proporcionar la oportunidad de evaluar el ambiente físico en el cual el sistema de información funcionará.

Revisión de Documentación:

Otra de las técnicas que realizaremos es la revisión de documentación como por ejemplo:

- Documentación de políticas generales
- Documentación legislativa
- Documentación de directrices
- Documentación del sistema de información: Guía de usuario del sistema, Manual administrativo del sistema
- Manual del diseño del sistema
- Manual de requerimientos.
- Documentación relacionada con la seguridad: Último informe de auditoría,
- Informe de evaluación de riesgos
- Resultados de pruebas del sistema
- Plan de seguridad del sistema
- Toda esta información puede proporcionar una mejor visión sobre las políticas de seguridad de la información que realizaremos en el manual.

CAPITULO 2

2. ANÁLISIS, PRESENTACIÓN DE RESULTADOS Y DIÁGNOSTICOS.

2.1. Análisis de la situación actual

Hoy en día la amenaza más importante contra nuestra información, la encontramos dentro de la misma empresa donde laboramos. Ya sea por accesos indebidos o no autorizados a la información corporativa son realizados principalmente por los empleados de la misma.

Adicionalmente se suman los ataques de virus informáticos que son ocasionados intencionalmente o por desconocimiento de los mismos empleados, en sentido general, las empresas de nuestro país se inclinan más preocupándose por los agentes externos que por los internos.

Lo importante es que las empresas realicen una evaluación de riesgos formal, para poder tener un conocimiento de la importancia que tienen estos riesgos. El resultado del análisis establecerá si se está exponiendo la información internamente o externamente.

La clave está en que existan políticas de Seguridad de la Información y que sean puestas en práctica por los empleados de las empresa para que estén concientizados de la importancia de la información.

Luego del desarrollo de las políticas de Seguridad de la Información es necesaria una difusión a todos los empleados que intervienen con los activos de la información, ya sea por medio de correo electrónico, por memos de entrega, por capacitaciones, en fin cualquier medio es válido, el fin es de concientizar a los empleados. Todas estas técnicas nos ayudarán a controlar nuestros datos.

2.2. Análisis FODA de norma ISO 27002

Tabla #2

Análisis FODA de la ISO 27002.

Fuente: Los Autores

FORTALEZAS	OPORTUNIDADES	DEBILIDADES	AMENZAS
Es un estándar adoptado en Ecuador como NTE ISO/IEC 27002:2009	Es una norma internacional y por eso se la puede aplicar para cualquier institución.	En los objetivos de control no se contempla la trazabilidad.	Es una norma conceptual, no se tienen las herramientas puntuales para su implementación.
Cada control tiene su guía de implementación para una fácil visión	Para la implementación de los controles no se requiere revisar los 133 controles, solo los que aplique a la organización	No es una guía madura para el análisis de riesgos.	Esta norma no es certificable.
Fácil adaptación para cada organización.			
Guía para mejorar la seguridad de la información.			

2.3. Reseña histórica de la empresa

"La presencia Salesiana en el Ecuador es una realidad social desde enero de 1888, como respuesta al Convenio firmado por Don Bosco y el representante del Gobierno del Ecuador en Turín (Italia) en 1887, por el que se confía a los salesianos el Protectorado Católico de Artes y Oficios de Quito, para que impartan educación moral y científica a los hijos del pueblo y para el desarrollo de la industria nacional mediante una enseñanza sistemática de la artesanía".[8]

Gráfico #6

Presencia salesiana

Fuente: Universidad Politécnica Salesiana

Elaborado por: Universidad Politécnica Salesiana

"Muy pronto la obra evangélica-educativa de los salesianos se extendió a otras ciudades del Ecuador, destacándose entre las principales acciones la fundación de las Misiones en el Oriente Ecuatoriano como Gualaquiza (1893), Indanza (1914), Méndez (1915), Macas (1924), Sucúa (1931) y Limón (1936). En lo educativo también se fundan obras como las de Quito (1888) con los talleres de Artes y Oficios en el Protectorado Católico; en Riobamba (1881), se funda la escuela Primaria, Talleres y el Oratorio festivo; en Cuenca (1893) empiezan los Talleres y el Oratorio Festivo; en

[8] Universidad Politécnica Salesiana. Dirección URL: < http://www.ups.edu.ec/conoce>

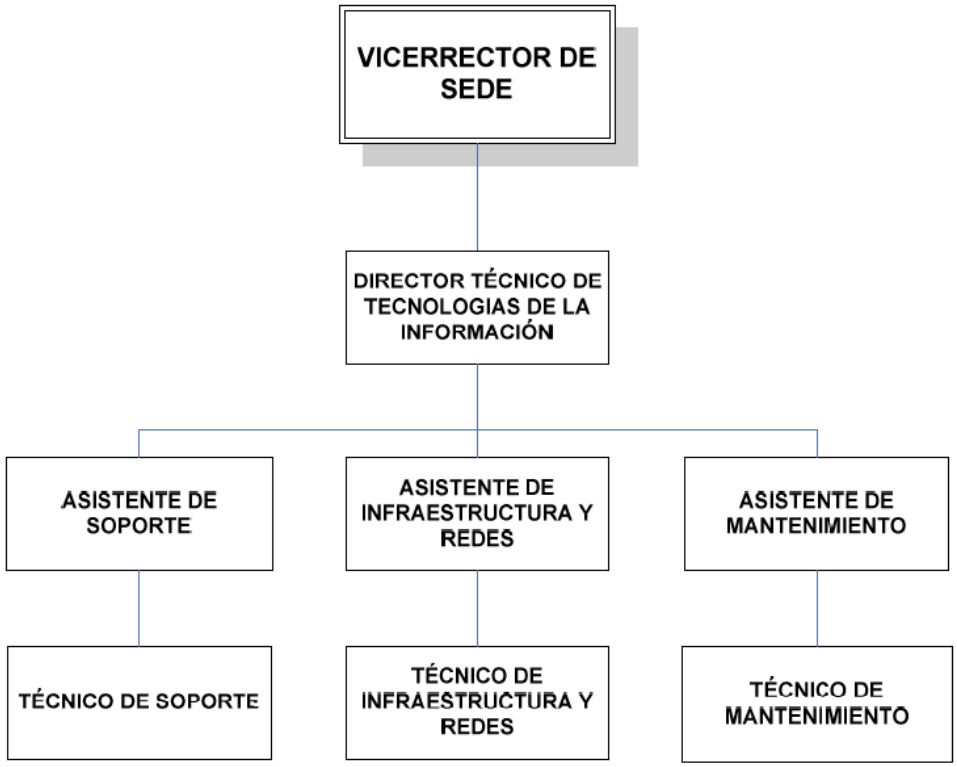
Quito en el barrio La Tola (1896), se abren los Talleres de Mecánica y Carpintería, la Escuela Primaria y la Iglesia dedicada a María Auxiliadora; Guayaquil (1904) vio la primera fundación con el Instituto Domingo Santistevan para niños huérfanos con el patrocinio de la Junta de Beneficencia. En el Barrio Centenario de esta misma ciudad se fundó el Colegio Cristóbal Colón (1911) para la educación humanística de la juventud guayaquileña; en Manabí (1927) los salesianos reciben la Parroquia Rocafuerte, en la que se abre igualmente una Escuela Primaria y un Oratorio festivo".[9]

2.4. Estructura organizacional de IT

2.4.1. Organigrama

Gráfico #7

Organigrama



Fuente: Universidad Politécnica Salesiana

Elaborado por: Universidad Politécnica Salesiana

[9] Universidad Politécnica Salesiana. Dirección URL: < http://www.ups.edu.ec/conoce>

2.4.2. Descripción de las principales funciones del departamento de Tecnología de Información.

Tabla #3

Descripción de funciones del Director Técnico de TI.

Fuente: Universidad Politécnica Salesiana – Sistemas

DIRECTOR TÉCNICO DE TECNOLOGÍAS DE LA INFORMACIÓN.	**Objetivo:** Coordinar las actividades referentes a TI en la Sede.
Responsabilidades: 1. Elaboración y seguimiento del Plan Operativo del Departamento. 2. Participar en la planeación estratégica de la sede. 3. Asesoría tecnológica para la adecuada adquisición del hardware y software. 4. Asesoría informática para el adecuado uso del hardware y software de la sede. 5. Corresponsable del plan de adquisiciones de la sede. 6. Realizar documentación informática de acuerdo a los estándares de la industria en conjunto con los responsables de áreas locales y/o nacionales. 7. Dar seguimiento a las labores de las áreas de redes, hardware y soporte a usuarios, así como la reasignación de tareas, temporal o definitivamente, acorde con las necesidades de la sede. 8. Proponer mejoras a los actuales procesos internos de la sede, temporales o definitivos, en donde el área informática estuviere involucrada. 9. Seguimiento al proyecto del repositorio de datos. 10. Colaborar con el plan de capacitación del área de TI, acorde a las necesidades de la sede. 11. Cumplir con las demás funciones que le sean asignadas por el Vicerrector.	

Tabla #4

Descripción de funciones de Asistente de Soporte.

Fuente: Universidad Politécnica Salesiana - Sistemas

ASISTENTE DE SOPORTE.	**Objetivo:** Brindar soporte a nivel de aplicaciones de gestión docente y administrativa.
Responsabilidades: 1. Brindar soporte a usuario final en las aplicaciones académicas. 2. Ofrecer soporte a usuario final en las aplicaciones administrativas. 3. Realizar soporte a usuario final en las aplicaciones web. 4. Llevar una bitácora del soporte brindado. 5. Escalar la el soporte a los analistas programadores en caso de ser necesario. 6. Reportar defectos en las aplicaciones.	

Tabla #5

Descripción de funciones del Asistente de Mantenimiento.

Fuente: Universidad Politécnica Salesiana - Sistemas

ASISTENTE DE MANTENIMIENTO.	**Objetivo:** Garantizar el correcto funcionamiento del hardware y software de la sede a nivel de usuario final.
Responsabilidades: 1. Instalar y mantener el software y hardware 2. Supervisar, actualizar y controlar el inventario de software y hardware 3. Dar soporte a usuarios en el uso de herramientas informáticas 4. Elaborar y ejecutar planes de mantenimiento preventivo de hardware y software. 5. Otras funciones asignadas por el Coordinador de Tecnologías de Información. 6. Atender el Call Center de soporte.	

Tabla #6

Descripción de funciones de Asistente de Infraestructura y Redes.

Fuente: Universidad Politécnica Salesiana – Sistemas

ASISTENTE DE INFRAESTRUCTURA Y REDES.	**Objetivo:** Garantizar el buen funcionamiento de la infraestructura de servidores y redes.

Responsabilidades:

1. Participar en la planificación, políticas y especificaciones técnicas de la infraestructura tecnológica de la Universidad Politécnica Salesiana.
2. Instalar, administrar, monitorear y mantener la Infraestructura de Servidores y redes de comunicación de la Sedes.
3. Administrar y mantener operativos los servicios de servidores y la infraestructura de comunicaciones de la Sede.
4. Custodiar el inventario de infraestructura de servidores, hardware y software.
5. Cumplir los planes de mantenimiento preventivo, correctivo y de contingencia de la infraestructura tecnológica.
6. Elaborar y Mantener actualizada la información relacionada a la infraestructura de servidores y redes de comunicaciones.
7. Ejecutar el respaldo de información de servidores de acuerdo al reglamento e instructivos de respaldo de información.
8. Investigar e implementar nuevas tecnologías informáticas.
9. Implementar seguridad a nivel de sistemas operativos.
10. Cumplir con las demás funciones que le sean asignadas.

Tabla #7

Descripción de funciones de Técnico de Soporte.

Fuente: Universidad Politécnica Salesiana – Sistemas

TÉCNICO DE SOPORTE.	**Objetivo:** Ayudar en el soporte a usuario final en las aplicaciones académicas y administrativas y de ofimática.
Responsabilidades: 1. Apoyar a los usuarios finales in-situ en la utilización de las aplicaciones académicas, administrativas y de ofimática.	

Tabla #8

Descripción de funciones de Técnico de Infraestructura y Redes.

Fuente: Universidad Politécnica Salesiana - Sistemas

TÉCNICO DE INFRAESTRUCTURA Y REDES.	**Objetivo:** Dar soporte efectivo de redes y comunicaciones en la sede.
Responsabilidades: 1. Instalar y/o supervisar la instalación y funcionamiento de la red informática 2. Las demás funciones que el Asistente de infraestructura y Redes le asigne.	

Tabla #9

Descripción de funciones de Técnico de Mantenimiento

Fuente: Universidad Politécnica Salesiana – Sistemas

TÉCNICO DE MANTENIMIENTO.	**Objetivo:** Apoyar en el correcto funcionamiento del HW y SW de la Sede.
Responsabilidades: 1. Instalar y mantener el software y hardware en las unidades departamentales 2. Realizar el levantamiento del inventario de software y hardware de la sede 3. Dar soporte a usuarios en el uso de herramientas informáticas 4. Ejecutar planes de mantenimiento preventivo de hardware y software 5. Otras funciones asignadas por el Asistente de Soporte y Mantenimiento.	

2.4.3. Misión

La formación de honrados ciudadanos y buenos cristianos, con excelencia humana y académica. El desafío de nuestra propuesta educativa liberadora es formar actores sociales y políticos con una visión crítica de la realidad, socialmente responsables, con voluntad transformadora y dirigida de manera preferencial a los pobres.

2.4.4. Visión

La Universidad Politécnica Salesiana, inspirada en la fe cristiana, aspira constituirse en una institución educativa de referencia en la búsqueda de la verdad, el desarrollo de la cultura, de la ciencia y tecnología, mediante la aplicación de un estilo educativo centrado en el aprendizaje, docencia, investigación y vinculación con la colectividad, por lo que se compromete, decididamente, en la construcción de una sociedad democrática, justa, equitativa, solidaria, con responsabilidad ambiental, participativa y de paz.

2.5. Diagnóstico

2.5.1. Análisis de las encuestas

Para el desarrollo de la presente tesis se ha realizado las entrevistas con el Responsable del Área de Sistemas, se pudo comprobar que no se mantienen normas de seguridad de la información en la Universidad Politécnica Salesiana sede Guayaquil, tomando en cuenta todos los controles de la norma ISO 27002.

Se realizaron entrevistas, con el Director de Sistemas.

Estas entrevistas fueron realizadas previas al desarrollo de la norma ISO 27002 y por medio de la información adquirida en las entrevistas realizadas al responsable de Sistemas, se pudo realizar un diagnóstico que influyó y ayudó a la justificación del proyecto en mención.

Según las entrevistas que se dieron en su momento se tuvo los siguientes criterios:

Políticas de seguridad de la información

- ¿Se cuentan con políticas de seguridad de la información?

  SI ( ) NO (*)

- ¿Se tienen implementados controles de cumplimiento de las políticas de seguridad de la información?

  SI ( ) NO (*)

- ¿Las políticas de seguridad de la información son de conocimiento de todo el personal de la Institución?

  SI ( ) NO (*)

Aspectos organizativos para la seguridad

- ¿La Universidad Politécnica Salesiana cuenta con un área para labores exclusivas de seguridad de la información?

  SI ( ) NO (*)

- ¿La Universidad Politécnica Salesiana ha contratado un asesoramiento en materia de seguridad de la información?

  SI ( ) NO (*)

- ¿Al realizar contratos con empresas externas exige clausulas de seguridad de la información?

  SI ( ) NO (*)

Con relación a la clasificación y control de activos informáticos

- ¿Se cuenta con un inventario de activos de información actualizado?

  SI (*) NO ( )

- ¿Este inventario esta automatizado?

  SI (*) NO ( )

- ¿El inventario de activos informáticos se lo actualiza periódicamente?

  SI (*) NO ( )

Políticas del personal respecto a la seguridad Informática

- ¿Los incidentes de seguridad de los sistemas de información son reportados brevemente por los usuarios?

  SI (*) NO ( )

- ¿La Universidad Politécnica Salesiana cuenta con convenios de confidencialidad de la información?

  SI ( ) NO (*)

Seguridad física y ambiental de los sistemas de Información

- ¿Todas las áreas esta identificadas?

  SI (*) NO ( )

- ¿Para áreas seguras se cuentan con controles de ingreso del personal?

  SI (*) NO ( )

- ¿En caso del alguna falla en el cableado de datos se está preparados para su pronta corrección?

  SI (*) NO ( )

- ¿Se realiza mantenimiento periódico del hardware y software en la Universidad Politécnica Salesiana?

  SI ( ) NO (*)

Con relación a la gestión de las comunicaciones de datos y operaciones de los sistemas informáticos

- ¿La Universidad Politécnica Salesiana cuenta con controles contra software malicioso (antivirus, antispyware, etc)?

  SI ( ) NO (*)

- ¿La Universidad Politécnica Salesiana cuenta con registros de accesos y uso de los aplicativos y servicios de la red de los colaboradores?

  SI ( ) NO (*)

- ¿Se cuentan con controles de seguridad de los medios de almacenamiento?

  SI (*) NO ( )

- ¿La Universidad Politécnica Salesiana cuentan con compromisos de responsabilidades del uso de los recursos de la Institución?

  SI ( ) NO (*)

Control de acceso

- ¿Para las aplicaciones de la Universidad Politécnica Salesiana de tienen políticas de control de acceso?

  SI (*) NO ( )

Nota: La Universidad Politécnica Salesiana tiene definida normas internas para control de accesos, estas normas no aplican para todas las herramientas o aplicaciones de la institución.

- ¿Las políticas de control de acceso son aplicadas?

  SI (-*) NO ( )

- ¿Cuentan con un inventario actualizado para los accesos otorgados a los sistemas informáticos?

  SI ( ) NO (*)

- ¿Todas las aplicaciones de la Universidad Politécnica Salesiana cuentan con una contraseña para permitir el acceso a los usuarios?

  SI (-*) NO ( )

- ¿Para el acceso remoto se tienen establecidos mecanismos de autenticación de usuarios a la red interna de la Universidad Politécnica Salesiana?

  SI ( ) NO (*)

- ¿Se cuenta con controles de monitoreo para los recursos de la Universidad Politécnica Salesiana?

  SI ( ) NO (*)

Desarrollo y mantenimiento de sistemas informáticos

- ¿Para el desarrollo de aplicaciones se cuenta con controles de validación de datos de entrada y de salida?

  SI (*) NO ( )

- ¿La Universidad Politécnica Salesiana cuenta con controles criptográficos, como por ejemplo el uso de certificados digitales u otros programas para la encriptación de datos?

  SI (*) NO ( )

- ¿Se tienen controles que impidan el acceso no autorizado a los programas fuente de las aplicaciones de la Universidad Politécnica Salesiana?

  SI (*) NO ( )

- ¿Se cuenta con un procedimiento de control de los cambios para las aplicaciones, software y sistema operativo?

  SI (*) NO ( )

- ¿Se validan los códigos fuentes desarrollados por personal externo antes de la puesta en producción?

  SI (*) NO ( )

Gestión de incidentes de sistemas informáticos

- ¿La Universidad Politécnica Salesiana cuenta con un procedimiento formal para reportes de incidentes?

  SI ( ) NO (*)

- ¿Cuentan con una herramienta de registro de incidentes o Help desk?

  SI ( ) NO (*)

- ¿Al reporta un incidente de seguridad se cuenta con un plan de respuesta?

  SI ( ) NO (*)

- ¿Se investiga y recolectan evidencias sobre el incidente de seguridad?

  SI ( ) NO (*)

Administración de la continuidad de los sistemas Informáticos

- ¿La Universidad Politécnica Salesiana cuenta con planes de continuidad de las operaciones?

  SI ( ) NO (*)

- ¿Realizan pruebas, mantenimiento y evaluación constante de los planes de continuidad de las operaciones?

  SI ( ) NO (*)

Cumplimiento legal referido a los sistemas Informáticos

- ¿Tienen identificada la normativa legal que aplican a las aplicaciones que usa la Universidad Politécnica Salesiana?

  SI ( ) NO (*)

- ¿La Universidad Politécnica Salesiana cuneta con políticas de protección de datos y privacidad de la información de los colaboradores?

  SI (*) NO ( )

- ¿Cuentan con controles del uso inadecuado de los recursos de la Universidad Politécnica Salesiana?

  SI ( ) NO (*)

- ¿La Universidad Politécnica Salesiana cuenta con controles del cumplimiento de las políticas de seguridad de la información?

  SI ( ) NO (*)

- ¿Realizan auditoria a los sistemas informáticos de su institución?

  SI (*) NO ( )

Por medio de la información adquirida en la entrevista, se pudo definir que a la Universidad Politécnica Salesiana sede Guayaquil es vulnerable a ataques de colaboradores internos o externos, es por eso que se llego a la conclusión de que se requiere políticas de seguridad de la información. Partiendo de las políticas se puede tener una línea base para realizar los controles y por darles una adecuada protección a los activos de la Universidad Politécnica Salesiana.

CAPITULO 3

3. IMPLEMENTACION DE LA NORMA ISO 27002

3.1. Desarrollo de Políticas de Seguridad de la Información

El desarrollo de las políticas de Seguridad de la Información realizada en el departamento de sistemas de la Universidad Politécnica Salesiana sede Guayaquil, proviene de la recopilación de información, hallazgos y análisis de la situación actual del departamento basándonos en los controles de la ISO 27002 correspondientes a los once dominios de la norma:

- Política de seguridad (1)
- Aspectos Organizativos de la Seguridad Informática (2)
- Gestión de Activos (2)
- Seguridad ligada a los recursos humanos (3)
- Seguridad física y del entorno (2)
- Gestión de comunicaciones y operaciones (10)
- Control de acceso (7)
- Adquisición, desarrollo y mantenimiento de sistemas de información (6)
- Gestión de incidentes en la seguridad de la información (2)
- Gestión de la continuidad del negocio (1)
- Cumplimiento (3)

Las Políticas creadas en el desarrollo del presente proyecto no serán incluidas ya que son de carácter confidencial, por lo tanto el manual de políticas de Seguridad de la Información será custodiado por el Departamento de Sistemas.

3.2. Objetivo de control de la norma ISO 27002

3.2.1. Política de seguridad

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

A.5.1.1 Documento de políticas de seguridad de la información.

Control

"Se debe definir claramente todas las responsabilidades en cuanto a seguridad de la información."[10]

Lista de chequeo para implantación de políticas

1. ***Verificar que para todos los cargos concernientes a Seguridad de la Información, existan roles y responsabilidades.***

   La universidad politécnica salesiana posee un documento formal el cual detalla los roles y responsabilidades, según el organigrama la Universidad Politécnica Salesiana no posee un departamento de seguridad de la información.

2. ***Revisar en los manuales de políticas y procedimientos que no existan inconsistencias, en cuanto a la asignación de responsabilidades concernientes a seguridad de la información.***

   Para el caso revisado de la universidad politécnica salesiana Guayaquil tienen las asignaciones de responsabilidades correctamente, los roles de seguridad se los desempeñan según la especialidad de cada área. Además cuentan con Funciones de los Departamentos de TI.

[10] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

Servicios para la docencia

Las áreas de TI deben asegurar a los estudiantes y docentes de la Universidad el uso confiable de los equipos de TI. Brindará asistencia técnica en la adquisición de hardware y software que ayuden al desenvolvimiento de la academia.

Servicios para la administración

Las áreas de TI, una vez recibido los requerimientos de las diferentes áreas técnicas o administrativas; analizarán, diseñarán y desarrollarán los programas necesarios para la gestión.

Servicios institucionales

Los departamentos de TI deberán promover la automatización de los servicios académicos y administrativos de la Universidad Politécnica Salesiana, así como el uso de las tecnologías de información y comunicación.

Detalle los códigos de los procedimientos revisados.

- Estructura Orgánica Funcional y de Responsabilidades para las Áreas de Información.

Detalle las debilidades detectadas en la lista de chequeo

- Se evidencia que no se cuentan con segregación de responsabilidades en cuanto a seguridad de la información.

A.5.1.2 Revisión y evaluación

Control

"La política de seguridad debe ser revisada en intervalos planificados o si cambios significantes ocurren con el fin de asegurar su uso continuo, adecuación y efectividad."[11]

3.2.2. Aspectos organizativos de la Seguridad de la Información.

ORGANIZACIÓN INTERNA

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

Control

"La gerencia debe apoyar activamente en la seguridad dentro de la organización a través de direcciones claras demostrando compromisos, asignaciones explicitas y reconocimiento de las responsabilidades de la seguridad de la información."[12]

Lista de chequeo para implantación de políticas

1. ***Verificar que el Rectorado asegure que las metas de seguridad de la información sean identificadas, y que provea los recursos necesarios para la seguridad de la información.***

   Actualmente si se está recibiendo el apoyo del Rectorado con la implementación del sistema de gestión de seguridad de la información.

[11] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >
[12] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

La cual se ha decidido que será de iniciativa propia de cada sede su avance y planificación.

A.6.1.2 Coordinación de seguridad de la información.

Control

"La información de las actividades de seguridad deben ser coordinadas por representantes de diferentes partes de la organización con roles relevante y funciones de trabajo."[13]

Lista de chequeo para implantación de políticas

1. ***Verificar como se está asegurando que las actividades de seguridad sean ejecutadas en cumplimiento con la política de seguridad de la información.***

   Para asegurar que las actividades de seguridad sean ejecutadas se ha asignado a un responsable o líder del proyecto de la implantación del sistema de seguridad de la información, la cual se maneja por medio de un cronograma con fechas ya establecidas para la entrega de proyectos que mitigan las amenazas.

   Detalle los códigos de los procedimientos revisados.

   - Ficha de amenaza de activos de información.

   Detalle las debilidades detectadas en la lista de chequeo

[13] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

- Se pudo detectar que la coordinación del proyecto de sistema de gestión de seguridad de la información recae en una persona, debería de involucrar a personal de otras áreas con roles relevantes.

A.6.1. 3 Asignación de responsabilidades para seguridad de la información.

Control

"Se debe definir claramente todas las responsabilidades en cuanto a seguridad de la información."[14]

Lista de chequeo para implantación de políticas

1. ***Revisar en los manuales de políticas y procedimientos que no existan inconsistencias, en cuanto a la asignación de responsabilidades concernientes a seguridad de la información.***

   El responsable del departamento de sistemas de las Universidad Politécnica Salesiana nos sede Guayaquil, nos proporciono uno documento de la Estructura Orgánica Funcional y de Responsabilidades para las Áreas de Tecnologías Información y se verificó los diferentes roles y responsabilidades del área.

   En el momento de la revisión, no se hallaron evidencias de asignación de roles y funciones s concernientes a seguridad de la información, actualmente no existe personal dedicado a la seguridad.

Detalle los códigos de los procedimientos revisados.

- Manual de configuración de impresoras SIGAC y SNA.

[14] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

- Manual de configuración Pichincha.
- Estructura Orgánica Funcional y de Responsabilidades para las Áreas de Tecnologías Información.
- Documentación de correos masivos.
- Manual de respaldos.
- Fichas de amenazas de activos de información de Guayaquil.

Detalle las debilidades detectadas en la lista de chequeo

- Actualmente la institución no se ha preocupado de la seguridad de la información.

A.6.1.4 Proceso de autorización de recursos para el procesado de la información.

Control

"Debería establecerse un proceso de autorización para la gestión de cada nuevo recurso de tratamiento de la información."[15]

Lista de chequeo para implantación de políticas

1. ***Verificar si actualmente se necesita de la aprobación de la dirección académica para los nuevos medios informáticos.***

   Actualmente la Universidad Politécnica Salesiana sede Guayaquil, implementa nuevos medios informáticos solo con la autorización de la dirección académica.

2. ***Se realizan evaluaciones del uso de medios informáticos personales, como laptops o aparatos móviles, para el tratamiento de la***

[15] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

información de la organización así como los controles necesarios, ya que pueden introducir nuevas vulnerabilidades.

Actualmente todos los equipos personales del personal docentes y administrativo tienen instalado un antivirus para prevenir infecciones al momento de conectarse a la red interna.

Detalle los códigos de los procedimientos revisados.

- Documentación de correos masivos.

A.6.1.5 Acuerdos sobre confidencialidad

Control

"Se debe identificar y revisar con regularidad los requisitos de confidencialidad o los acuerdos de no-divulgación que reflejan las necesidades de la organización para la protección de la información."[16]

Lista de chequeo para implantación de políticas

1. ***Revisar si existe un convenio de confidencialidad que sea aplicado a personal interno y externo.***

   No existe convenio de confidencialidad para que sea aplicable para personal tanto interno como externo.

   De aprobar el convenio de confidencialidad entregado deberá ser aplicado a todo personal a la cual se le entregue información de la universidad.

[16] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

Detalle los códigos de los procedimientos revisados.

- Fichas de amenazas de activos de información de Guayaquil.

Detalle las debilidades detectadas en la lista de chequeo

- Actualmente no se dispone de un convenio de confidencialidad, sin embargo está incluida en el cronograma de las amenazas para su implementación. Adicional se entrega un modelo de convenio de confidencialidad.

A.6.1.6 Contacto con autoridades

Control

"Deben ser mantenidos contactos apropiados con autoridades relevantes."[17]

Control no aplica para la Universidad Politécnica Salesiana sede Guayaquil.

A.6.1.7 Contacto con grupos de interés especiales

Control

"Se debe de mantener los contactos apropiados con grupos de interés especiales, otros foros especializados en seguridad de la información, y asociaciones de profesionales."[18]

[17] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

Control no aplica para la Universidad Politécnica Salesiana sede Guayaquil.

A.6.1.8 Revisión independiente de la seguridad de la información.

Control

"El alcance de la organización para gestionar la seguridad de información y su implementación (objetivos de control, controles, políticas, procesos y procedimientos para seguridad de información) deben ser revisados independientemente en intervalos planificados o cuando cambios significativos a la puesta en marcha de la seguridad ocurran."[19]

Lista de chequeo para implantación de políticas.

1. ***Verificar si existen intervalos de planificación para la implementación de nuevos proyectos para salvaguardar la información.***

   Existe un cronograma de implementación de nuevos proyectos (Salvaguardas) que está a cargo del administrador de sistemas de la universidad.

Detalle los códigos de los procedimientos revisados.

- Ficha de amenazas de activos de información de Guayaquil.

Detalle las debilidades detectadas en la lista de chequeo

---

[18] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

[19] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

- No todas las salvaguardas tienen fechas de entrega.

TERCEROS

A.6.2.1 Identificación de los riesgos relacionados con partes externas.

Control

"Se deben identificar los riesgos para la información y los servicios de procesamiento de información de la organización de los procesos del negocio que involucran partes externas e implementar los controles apropiados antes de autorizar el acceso."[20]

Lista de chequeo para implantación de políticas

1. ***Verifique en los actuales procedimientos, si existe una política especificando controles para acceso a recursos por parte de terceros.***

   La Universidad Politécnica Salesiana sede Guayaquil, no cuenta en sus documentos con políticas que especifique controles para otorgar acceso a los recursos por parte de terceros.

   Esta política no va acorde con la realidad actual, debido a que el personal externo, debido a sus necesidades laborales requiere acceso a correo electrónico externo.

2. ***Verifique si estos usuarios externos tienen firmado un acuerdo de confidencialidad y buen uso de los recursos.***

[20] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com>

No existe en la Universidad Politécnica Salesiana sede Guayaquil, documento de un acuerdo de confidencialidad y buen uso de los recursos tanto para personal interno como para el externo.

Detalle los códigos de los procedimientos revisados.

- Contrato.
- Propuesta de Estructura Orgánica Funcional y de Responsabilidades para las Áreas de Información.

Detalle las debilidades detectadas en la lista de chequeo.

- Por las necesidades laborales se ha otorgado acceso a personal externo.

A.6.2.2 Requisitos de seguridad cuando se tratan con clientes

Control

"Todos los requisitos identificados de seguridad deben ser anexados antes de dar a los clientes acceso a la información o a los activo de la organización."[21]

Lista de chequeo para implantación de políticas

1. ***Documente si existen términos contractuales antes de otorgar el acceso.***

La Universidad politécnica Salesiana no tiene términos contractuales para los proveedores. Son los alumnos de la Institución a los que se le dominará clientes, ya que son a ellos los que se les otorga un identificador y clave de acceso, para los ingresos al sistema.

A.6.2.3 Requisitos de Seguridad de Outsourcing

Control

"Los acuerdos con terceras partes que implican el acceso, proceso, comunicación o gestión de la información de la organización o de las instalaciones de procesamiento de información o la adición de productos o servicios a las instalaciones, deben cubrir todos los requisitos de seguridad relevantes."[22]

Lista de chequeo para implantación de políticas

[21] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com>
[22] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com>

1. ***Verifique que disposiciones están vigentes con respecto a acuerdos con terceros para la contratación.***

   La Universidad Politécnica Salesiana sede Guayaquil, no cuenta con documentación interna para la contratación de proveedores.

2. ***Verifique que en los acuerdos con terceras partes exista la política de seguridad de la información.***

   Según la revisión, en los acuerdos con terceras partes (contratos) no es encontrar una cláusula de confidencialidad, además no existe cláusula del buen uso que se debe a Hardware, Software y otros activos organizacionales.

   Y para aquellos servicios provistos por terceros que no tienen uso de la tecnología (limpieza, etc.) no se detalla en los contratos cláusulas de confidencialidad, buen uso de los activos, etc.

3. ***Detalle que procedimientos se utilizaran para proteger la información, hardware y software (activos organizacionales).***

   La Universidad Politécnica Salesiana sede Guayaquil, no cuenta con procedimientos para proteger la información. En los contratos revisados no hay información de protección hardware y software por parte del contratado.

4. ***Controles para la protección de software malicioso.***

   Para la protección de software malicioso existen tan solo las políticas de antivirus, la Universidad Politécnica Salesiana sede Guayaquil tiene como política que ningún usuario puede instalar software y además si en caso de que un usuario instale algún software al reiniciar la estación de trabajo vuelve a su estado original.

5. ***Controles que aseguren el retorno o la destrucción de la información al final del acuerdo.***

   No existe ningún control que asegure la destrucción de la información al final del acuerdo. No es aplicable a la Universidad Politécnica Salesiana sede Guayaquil, debido a que existe información que le puede servir y no debe ser destruida. En los contratos revisados no existen cláusulas del retorno de la información al final del acuerdo.

6. ***Acuerdos de confidencialidad.***

   En los contratos revisados no existen cláusulas de acuerdos de confidencialidad. Para la protección de la información interna de la Universidad Politécnica Salesiana sede Guayaquil, todo contrato con un proveedor externo debería i9ncluir clausulas de confidencialidad y hacerles firmar convenio de confidencialidad.

7. ***Asegurar el conocimiento del usuario para temas y responsabilidades de seguridad de la información.***

   No hay un procedimiento que asegure a personal de Outsourcing que han recibido y conocido por medio de publicaciones, charlas, difusión en general sobre las políticas relacionadas con Seguridad de la Información

8. ***Derecho a controlar y revocar cualquier actividad relacionada con los activos de la organización.***

   Según lo revisado no existe a nivel de contrato ni en políticas internas derechos a controlar y revocar cualquier actividad relacionada con los activos de la universidad para personal de Outsourcing.

9. ***Derecho a auditar las responsabilidades definidas en el acuerdo.***

Según lo revisado no existe a nivel de contrato ni en políticas internas derechos a auditar las responsabilidades definidas en el acuerdo.

10. Escalamiento de problemas Niveles de servicio

En los contratos revisados se pudo cae en cuenta que poseen clausulas de escalamiento y niveles de servicios y superficialmente.

Antes de la contratación de un Outsourcing todo contrato debería explicar de forma clara y detallada los niveles de servicios y escalamiento de problemas y además con una clausula en caso de no cumplimiento.

11. Condiciones para terminación de acuerdos.

Según lo revisado en los contratos de los proveedores de la Universidad politécnica salesiana si se cuenta con clausulas de terminación de contrato. Estas cláusulas comprenden algunos casos como por ejemplo:

a. Por cabal cumplimiento de las obligaciones contractuales;
b. Por mutuo acuerdo de las partes;
c. Por declaración unilateral de la Universidad, en caso de incumplimiento del contratista;
d. Por sentencia ejecutoriada que declare la resolución o la nulidad del contrato;

En definitiva, el contrato termina por el cumplimiento total de las obligaciones contractuales o en forma anticipada por causas imputables a las partes o por mutuo acuerdo.

3.2.3. Gestión de activos.

RESPONSABILIDAD SOBRE LOS ACTIVOS

A.7.1.1 Inventario de activo

Control

"Todos los activos deben ser claramente identificados y se deben elaborar y mantener un inventario de todos los activos importantes."[23]

Lista de chequeo para implantación de políticas

1. ***Verificar en los actualmente existe la política de inventarios de activos de la información.***

   Se pudo evidenciar que actualmente no cuentan con una política definida en la cual exija inventariar los activos de información. La Universidad Politécnica Salesiana sigue un estándar para el inventario de activos.

   Los tres primeros caracteres pertenecen a la sede en el cual está ubicado el activo (GYE, UIO, CUE) y luego 3 dígitos (001, 002, 003). Con este estándar de inventario que cuenta la Universidad politécnica salesiana es posible identificar fácilmente a que localidad pertenece el activo.

2. ***Documente porque es necesario un inventario de activos de la información, detalle los riesgos de no tenerlo.***

   Es necesario el inventario de activos de la información para que La universidad politécnica salesiana funcione correctamente y alcance los objetivos propuestos por su dirección. El activo esencial es la

[23] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

información que maneja el sistema; o sea los datos. Y alrededor de estos datos se pueden identificar otros activos relevantes:

- Los servicios que se pueden prestar gracias a aquellos datos, y los servicios que se necesitan para poder gestionar dichos datos.
- Las aplicaciones informáticas (software) que permiten manejar los datos.
- Los equipos informáticos (hardware) y que permiten hospedar datos, aplicaciones y servicios.
- Los soportes de información que son dispositivos de almacenamiento de datos.
- El equipamiento auxiliar que complementa el material informático.
- Las redes de comunicaciones que permiten intercambiar datos.
- Las instalaciones que acogen equipos informáticos y de comunicaciones.
- Las personas que explotan u operan todos los elementos anteriormente citados.

El riesgo fundamental de no contar con un inventario de activos de la información es que puede parar las operaciones de la institución. También sale a la vista con un pequeño análisis de riesgo, que activos van a depender de otros activos para el correcto procedimiento.

Detalle los procedimientos revisados.

- Ficha_amenazas_activos

A.7.1.2 Propiedad de los activos

Control

"Toda la información y los activos asociados con el proceso de información deben ser poseídos por una parte designada de la organización."[24]

Lista de chequeo para implantación de políticas

1. ***Verificar en los manuales actuales los controles y responsabilidades que el propietario de los activos presta.***

   No se pudo evidenciar controles que se deberían ejecutar en cuanto la asignación de activos a los colaboradores de la Universidad politécnica salesiana.

2. ***Detallar en base a los manuales las responsabilidades de los propietarios de los activos de la información.***

   No existen responsabilidades, no está documentada las responsabilidades de los propietarios de los activos de la información.

Detalle las debilidades detectadas en la lista de chequeo

- No existe un mantenimiento periódico del inventario de activos de información.
- No se evidencio responsabilidades de los propietarios de los activos.

[24] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

A.7.1.3 Uso adecuado de los activos

Control

"Las reglas para un uso aceptable de la información y de los activos asociados con las instalaciones del procesamiento de la información deben ser identificadas, documentadas e implementadas."[25]

Lista de chequeo para implantación de políticas

1. ***Verificar en los contratos con terceros si existen cláusulas que responsabilicen en uso adecuado de los activos de la universidad politécnica salesiana.***

   Se pudo constatar que en los contratos con terceros no existen clausulas del bueno uso de los activos de información de la universidad politécnica salesiana.

2. ***Documente la existencia del convenio "Uso aceptable de los activos" y verifique que abarque tanto activos físicos como activos de la información.***

   En la universidad politécnica salesiana, no se tiene como procedimiento hacerle firmar tanto al personal interno como externo un convenio de "Uso aceptable de los activos".

   No existe el convenció de responsabilidad de los activos asignados al personal por parte de la universidad politécnica salesiana.

3. ***Para el caso de correo externo e Internet verifique si se le hace firmar a los empleados y personal externos un documento donde se responsabilice a hacer buen uso del activo.***

[25] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

La Universidad Politécnica Salesiana no cuenta con un documento de las prohibiciones y uso aceptable del correo.

4. ***Para el caso de usuarios que se les otorga BlackBerry, laptops y/o token RSA que tipo documentación se le hace firmar para el uso adecuado de ese activo.***

Para la asignación de equipos tecnológicos móviles tan solo se entrega el activo al colaborador para su uso y no se le hace firmar ningún documento.

Detalle los códigos de los procedimientos revisados.

- Adquisición e implementación de subsistemas de Data Center para la Universidad Politécnica Salesiana en la ciudad de Guayaquil.

Detalle las debilidades detectadas en la lista de chequeo.

- Uso de correo electrónico externo y cual sea la herramienta de la universidad politécnica salesiana, todo el personal de Outsourcing que lo requiere y a la par de los empleados de la Universidad Politécnica Salesiana se les debe hacer firmar un compromiso de seguridad y responsabilidad de uso adecuado de los activos asignados.
- En las entregas de laptops, BlackBerry, token RSA, etc. no existe compromiso de responsabilidad y tan solo hay un acurdo de que el Outsourcing deja en buen estado el equipo.
- No cuentan con un convenio de compromiso de responsabilidad de los accesos otorgados.

CLASIFICACIÓN DE LA INFORMACIÓN

A.7.2.1 Guías de clasificación

Control

"La información debería clasificarse en función de su valor, requisitos legales, sensibilidad y criticidad para la organización."[26]

Lista de chequeo para implantación de políticas

1. ***Verificar en los actuales manuales la existencia de la clasificación de los activos***

   Actualmente no se cuenta con manuales o documentos aprobados por el consejo superior sobre la clasificación de los activos de la Universidad Politécnica Salesiana.

2. ***Detalle los motivos de clasificar la información.***

   La Universidad Politécnica Salesiana deberá clasificar la información para poder tener un control o seguridad de sus datos críticos.

3. ***Revise el actual formulario de inventario de activos y verifique que cumpla las políticas de clasificación.***

   Actualmente se cuenta con un documento en el cual detalla la clasificación de los activos por tipo. Y en el Actual Inventario de activos de información no hay un NIVEL DE CONFIDENCIALIDAD el cual deberá aplicar a todos los empleados, contratistas, terceros, etc.

[26] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

Detalle las debilidades detectadas en la lista de chequeo

- No se cuenta con una clasificación de la información por ende no se puede identificar que información puede ser pública o confidencial.

A.7.2.2 Marcado y tratamiento de la información

Control

"Es importante definir un conjunto adecuado de procedimientos para marcar y tratar la información de acuerdo con el esquema de clasificación adoptado por la organización."[27]

Lista de chequeo para implantación de políticas

1. ***Verificar en los actuales manuales existe procedimientos del tratamiento de la información según su clasificación.***

   La Universidad politécnica salesiana no cuenta con procedimiento de marcado y tratamiento de la información. Es fundamental etiquetar la información y los soportes para que la gente sepa como manipularlos. Es uno de los muchos mecanismos que tenemos para concienciar al personal.

2. ***Detalle si actualmente se cumple la política de marcado y tratamiento de la información.***

   No se cumple en la actualidad. Toda la documentación revisada no tiene ningún etiquetamiento

[27] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

Detalle los códigos de los procedimientos revisados.

- Informe de gestión.
- Proceso y registro de Capacitación.
- Correos Masivos.
- Colas de Impresión.

Detalle las debilidades detectadas en la lista de chequeo

- Actualmente no existe un procedimiento formal para el etiquetamiento de información.

3.2.4. Seguridad ligada a los recursos humanos.

ANTES DEL EMPLEO

A.8.1.1 Inclusión de la seguridad en las responsabilidades y funciones laborales

Control

"Las funciones y responsabilidades de los empleados, contratistas y terceros deben ser definidas y documentadas en concordancia con la política de seguridad de la organización."[28]

Control no aplica para el alcance del presente trabajo, sin embargo se deben establecer normas de seguridad de acuerdo con el objetivo de control.

A.8.1.2 Selección y políticas de personal

[28] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

Control

"Se deben llevar listas de verificaciones anteriores de todos los candidatos para empleo, contratistas y terceros en concordancia con las leyes, regulaciones y la ética, al igual que proporcionalmente a los requisitos del negocio, la clasificación de la información a ser acezada y los riesgos percibidos."[29]

Control no aplica para el alcance del presente trabajo, sin embargo se deben establecer normas de seguridad de acuerdo con el objetivo de control.

A.8.1.3 Términos y condiciones de contratación.

Control

"Como parte de su obligación contractual, empleados, contratista y terceros deben aceptar y firmar los términos y condiciones del contrato de empleo el cual establecerá sus obligaciones y las obligaciones de la organización para la seguridad de información."[30]

Control no aplica para el alcance del presente trabajo, sin embargo se deben establecer normas de seguridad de acuerdo con el objetivo de control.

DURANTE EL EMPLEO

A.8.2.1 Responsabilidades de gerencia

Control

[29] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >
[30] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

"El Rectorado debe requerir empleados, contratistas y usuarios de terceros para aplicar la seguridad en concordancia con las políticas y los procedimientos establecidos de la organización."[31]

Control no aplica para el alcance del presente trabajo, sin embargo se deben establecer normas de seguridad de acuerdo con el objetivo de control.

A.8.2.2 Conocimiento, educación y entrenamiento de la seguridad de información

Control

"Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deben recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo."[32]

Control no aplica para el alcance del presente trabajo, sin embargo se deben establecer normas de seguridad de acuerdo con el objetivo de control.

A.8.2.3 Proceso disciplinario

Control

[31] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >
[32] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

"Debe existir un proceso formal disciplinario para empleados que han cometido una apertura en la seguridad."[33]

Control no aplica para el alcance del presente trabajo, sin embargo se deben establecer normas de seguridad de acuerdo con el objetivo de control.

CESE DEL EMPLEADO O CAMBIO DE FUNCIONES.

A.8.3.1 Responsabilidades de finalización

Control

"Las responsabilidades para realizar la finalización de un empleo o el cambio de este deben ser claramente definidas y asignadas." [34]

Control no aplica para el alcance del presente trabajo, sin embargo se deben establecer normas de seguridad de acuerdo con el objetivo de control.

A.8.3.2 Retornos de activos

Control

"Todos los empleados, contratistas y terceros deben retornar todos los activos de la organización que estén en su posesión hasta la finalización de su empleo, contratista o acuerdo."[35]

[33] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >
[34] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >
[35] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

Control no aplica para el alcance del presente trabajo, sin embargo se deben establecer normas de seguridad de acuerdo con el objetivo de control.

A.8.3.3 Retiro de los derechos de acceso

Control

"Los derechos de acceso para todos los empleados, contratistas o usuarios de terceros a la información y a las instalaciones del procesamiento de información deben ser removidos hasta la culminación del empleado, contratista o acuerdo, o debe ser ajustada en caso de cambio."[36]

Control no aplica para el alcance del presente trabajo, sin embargo se deben establecer normas de seguridad de acuerdo con el objetivo de control.

3.2.5. Seguridad física y ambiental.

ÁREAS SEGURAS

A.9.1.1 Perímetro de seguridad física.

Control

"Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas o un puesto manual de recepción) deben ser usados

[36] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

para proteger áreas que contengan información y recursos de procesamiento de información.”[37]

Lista de chequeo para implantación de políticas

1. ***Verifique y documente de que material están constituidas las áreas de trabajo.***

   Se verifico que las paredes son de bloques y cemento a excepción del centro de cómputo que la pared interior es de aluminio, sin embargo tiene dos puertas de seguridad.

2. ***Documente si existe algún control de ingreso de personal.***

   Se pudo verificar que para el ingreso al centro de computo es restringido, se dispone de una cámara de seguridad para verificar personal que va a entrar, y una puerta con dispositivo de seguridad electromagnético, adicionalmente existe una puerta en el exterior pero esta siempre permanece sin seguro.

3. ***Documente si existen escaleras de emergencias.***

   No existen escaleras de emergencias.

4. ***Documente si existen alarmas de seguridad.***

   Actualmente no se dispone de alarmas de seguridad.

Detalle los códigos de los procedimientos revisados.

- Reunión con director del centro de cómputo.

[37] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

Detalle las debilidades detectadas en la lista de chequeo

- Se pudo verificar que no existen alarmas de seguridad en la sala de cómputo.

A.9.1.2 Controles físicos de entrada.

Control

"Las áreas de seguridad deberían estar protegidas por controles de entrada adecuados que aseguren el permiso de acceso sólo al personal autorizado." [38]

Lista de chequeo para implantación de políticas

1. ***Verificar si hay restricción al área de caja.***

   Actualmente para el ingreso al área de caja solo existe la puerta del área que no siempre permanece con seguro.

2. ***Verificar si hay restricción al centro de cómputo.***

   La puerta del centro de cómputo se encuentra asegurada con un sistema de bandas magnéticas con un lector de tarjetas en la parte exterior y un pulsador en la parte inferior. Adicionalmente se cuenta con una cámara para verificar el personal que ingresa al centro de cómputo.

3. ***Cada visitante que se dirija a todas las áreas debe estar identificado.***

   Referente al área de caja el ingreso está prohibido a personal no autorizado. Para el ingreso al centro de cómputo no se exige

[38] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

identificación porque está aislado del área administrativa, sin embargo si dispone de otros mecanismos de seguridad para el ingreso.

4. ***Revisar los movimientos de ingreso y salida.***

Personal de sistemas se encarga de entregar las tarjetas de ingreso y asignar los permisos.

Detalle los códigos de los procedimientos revisados.

- Reunión con director del centro de cómputo.

A.9.1.3 Seguridad de oficina, despacho y recursos.

Control

"La seguridad física para oficinas, despachos y recursos debe ser asignados y aplicada." [39]

Lista de chequeo para implantación de políticas

1. ***¿Existen políticas de seguridad física?***

No se encontró manuales de seguridad física.

2. ***Detallar claramente todos los lugares que se encuentran con restricciones de acceso.***

Actualmente al ingreso del área de la dirección académica se encuentra un guardia de seguridad, adicionalmente a este recurso de seguridad no existe otro.

[39] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

Detalle los códigos de los procedimientos revisados.

- Reunión con Director del centro de cómputo.

A.9.1.4 Protección contra amenazas externas y ambientales.

Control

"Se debe designar y aplicar protección física del fuego, inundación, terremoto, explosión, malestar civil y otras formas de desastres natural o humana."[40]

Lista de chequeo para implantación de políticas

1. ***Se cuenta con un sistema central de incendios.***

Se verifico que en Data Center si se dispone de un sistema central de incendios, en las oficinas de sistemas no se cuenta con este sistema. No almacenar en áreas cerradas suministro de al granel hasta que se lo necesite.

2. ***¿Se han desarrollado simulacros de evacuación con el personal?***

No se realizan simulacros de evacuación, no se cuenta con un área específica que se encargue de realizar este tipo de simulacros.

Detalle los códigos de los procedimientos revisados.

- Inspecciones realizadas en la sede de Guayaquil.
- Reunión con director del centro de cómputo.

[40] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

Detalle las debilidades detectadas en la lista de chequeo

- Se pude detectar que no se cuenta con un departamento que se encargue de la seguridad y salud ambiental.

A.9.1.5 El trabajo en las aéreas seguras.

Control

"Se debería diseñar y aplicar protección física y pautas para trabajar en áreas seguras." [41]

Lista de chequeo para implantación de políticas

1. ***¿Verifique si existen directorios públicos que especifican la ubicación de lugares restringidos?***

   No existe información publicada que revele lugares restringidos.

2. ***¿Documente que existan cámaras y monitores constantes dentro de áreas seguras?***

   En la entrada del centro de cómputo se encuentra ubicada una cámara con monitor en el lugar de trabajo del director de sistemas. En el área de caja no se hay cámaras.

3. ***¿Documente el tipo de bloqueo físico que se tiene en áreas seguras vacías?***

   No se encontró aéreas seguras vacías.

[41] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

4. ***¿Verifique si existe política de toma de foto y grabación?***

No existen políticas referentes a toma de fotos o grabación en los manuales internos.

Detalle los códigos de los procedimientos revisados.

- Inspecciones a la sede Guayaquil.

Detalle las debilidades detectadas en la lista de chequeo

- Carencia de cámaras en el área de caja.
- Carencia de políticas de toma de fotos o grabación en áreas críticas como: caja, data Center.

A.9.1.6 Acceso público, áreas de carga y descarga.

Control

"Se deberían controlar las aéreas de carga y descarga, y si es posible, aislarse de los recursos de tratamiento de información para evitar acceso no autorizado." [42]

Lista de chequeo para implantación de políticas

1. ***Hacer tour por cada piso para ver si hay acceso para algo adicional, alguna puerta abierta donde este alguna computadora apagada.***

Se verifico que actualmente la universidad se encuentra remodelando y ampliando las instalaciones.

[42] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

Detalle los códigos de los procedimientos revisados.

- Inspección de la sede Guayaquil.
- Reunión con Director de Sistemas.

SEGURIDAD DE LOS EQUIPOS

A.9.2.1 Instalación y protección de equipos.

Control

"El equipo debería situarse y protegerse para reducir el riesgo de amenazas del entorno, así como las oportunidades de accesos no autorizados." [43]

Lista de chequeo para implantación de políticas

1. ***Protección de los equipos de su uso.***

   Referente a los equipos de los laboratorios, no se encuentran con algún dispositivo de seguridad, sin embargo los laboratorios permanecen cerrados y solo son abiertos al momento de dar clases, quedando como responsable el Docente académico.

   Con respecto a los equipos de las oficinas, se encuentran en lugares seguros, ya que se necesita de autorización para su ingreso.

2. ***Equipos donde se administre información sensible.***

   Estos equipos se encuentran en el Data Center ubicados en un Rack con su respectiva seguridad.

[43] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

3. ***Revisar si existen políticas que prohíben fumar, beber,.. etc en lugares críticos.***

   No se encontró políticas referentes al tema.

4. ***Verifique si actualmente se tiene un monitoreo de temperatura y humedad en el centro de computo y que políticas internas que lo soportan.***

   Actualmente no se cuenta con estos Monitoreo, sin embargo se mantiene una temperatura fría y templada en el Data Center.

5. ***Verificar si existen políticas de seguridad industrial sobre comer, beber y fumar en las instalaciones críticas de la Institución.***

   No existen políticas referentes al tema.

Detalle las debilidades detectadas en la lista de chequeo

- Carencia de políticas sobre comer, beber o ingerir licor en la universidad.

A.9.2.2 Suministro electrónico.

Control

"Se deberían proteger los equipos contra fallos de energía u otras anomalías eléctricas en los equipos de apoyo." [44]

Lista de chequeo para implantación de políticas

[44] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

1. ***Verificar políticas de seguridad de la información donde indiquen los mantenimiento tales como: electricidad, agua, aire acondicionado.***

   Actualmente no existen políticas de seguridad referente a mantenimiento de suministros, sin embargo el director administrativo es la persona encargada de llevar un cronograma de mantenimiento de los suministros.

2. ***Verificar si está cumpliendo su función los UPS o transformadores de la universidad.***

   Efectivamente, los UPS si se encuentran en buen estado, y adicionalmente están dentro del cronograma de mantenimiento.

3. ***Verificar si los enlaces con las diferentes sedes tienen un enlace adicional de backup.***

   Actualmente no se cuenta con enlace Backup.

Detalle los códigos de los procedimientos revisados.

- Ancho de Banda Internet
- Ficha de amenaza de activos Guayaquil
- Reunión con director de Sistemas
- Inspecciones sede Guayaquil

Detalle las debilidades detectadas en la lista de chequeo

- No existen políticas de seguridad de referente a mantenimiento de suministros.

A.9.2.3 Seguridad del cableado.

Control

"Se deberían proteger contra intercepciones o daños el cableado de energía y telecomunicaciones que transporten datos o soporten servicios de información." [45]

Lista de chequeo para implantación de políticas

1. ***Verificar la existencia de algún estándar en el momento que se instale un nuevo laboratorio sobre el cableado tanto eléctrico como de datos.***

   Se tiene estándares de cableado eléctrico y de datos. Actualmente se utiliza los siguientes tipos, para cableado eléctrico, de red y de voz. Para las oficinas en la parte eléctrica se utiliza el cable No12, para datos se utiliza el cable UTP tipo 6 con conectores RJ45.

2. ***¿Se instala alguna protección para evitar que el cable sufra algún daño en su operativo o protección alterna?***

   Los cables de los computadores se cubren con protectores, cuando van por los tumbados van por unos ductos de fierro.

A.9.2.4 Mantenimientos de equipos.

Control

"Los equipos deberían mantenerse adecuadamente para asegurar su continua disponibilidad e integridad." [46]

[45] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >
[46] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

Lista de chequeo para implantación de políticas

1. ***Verificar que tipo de acuerdo hay con los proveedores con respecto a los mantenimientos.***

   No existen contratos, sin embargo el director de sistemas contrata a un proveedor para que realice mantenimientos del Data Center, llevando un cronograma de mantenimientos.

2. ***Que personal realiza los mantenimientos.***

   Los encargados de realizar los mantenimientos de los equipos es el personal del área de Sistemas, se manejan en base a cronogramas realizados por el director de sistemas.

3. ***Se lleva un historial de los registros de mantenimiento?***

   Se lleva un cronograma donde se detalla claramente los mantenimientos realizados en la sede Guayaquil.

4. ***¿Se cumplen los requisitos de las pólizas de seguros?***

   En el contrato de compra e instalación del Data Center indica la póliza que se tiene, actualmente se encuentra caducada.

Detalle los códigos de los procedimientos revisados.

- Contrato de Compra e Instalación del Data Center

Detalle las debilidades detectadas en la lista de chequeo

- No existen contratos de mantenimientos del Data Center.
- Se recomienda la contratación con un proveedor.

A.9.2.5 Seguridad de equipos fuera de los locales de la organización.

Control

"Se debe aplicar seguridad a los equipos que se encuentran fuera de los locales de la organización tomando en cuenta los diversos riesgos a los que se está expuesto." [47]

Lista de chequeo para implantación de políticas

1. ***Indagar con el Director de Sistemas, ¿Para que indique si existen seguro de equipos al momento de trasladarlos de un lugar a otro?***

   No existen seguros de traslados de equipos. Rara vez o casi nunca se trasladan equipos de una campo al otro.

2. ***Documentar las políticas y controles físicos para laptops.***

   Actualmente no existen

3. ***Consultar si se realizan respaldos de la información de los discos de las computadoras portátiles.***

   No se realizan respaldos de la información de los discos, se sugiere poner una política para que el personal que utilice un computador portátil realice respaldos antes de emprender viajes.

4. ***Consultar si se realizan encriptación de los discos de las computadoras portátiles.***

[47] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

No se realizan encriptación de la información de los discos.

Detalle los códigos de los procedimientos revisados.

- Reunión con Director de Sistemas.

Detalle las debilidades detectadas en la lista de chequeo

- Los discos duros de las computadoras portátiles no son encriptados, se recomienda su encriptación por cualquier software de encriptación.

A.9.2.6 Seguridad en el rehúso o eliminación de equipos.

Control

"Todos los elementos del equipo que contengan dispositivos de almacenamiento deben ser revisados con el fin de asegurar que cualquier dato sensible y software con licencia haya sido removido o sobrescrito con seguridad antes de la eliminación." [48]

Lista de chequeo para implantación de políticas

1. ***Revisar si existe un procedimiento establecido de almacenamiento de equipos, si es por cambios o actualización de equipos.***

No existe un procedimiento ni políticas de seguridad del mismo.

Detalle los códigos de los procedimientos revisados.

- Reunión con director de sistemas.

[48] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

A.9.2.7 Retiro de la propiedad.

Control

"El equipo, información o software no debe ser sacado fuera del local sin autorización." [49]

Lista de chequeo para implantación de políticas

1. ***Documente las políticas y procedimiento para retiro de equipos y programas instalados.***

   Control contemplado en el control 9.2.5

   Detalle los códigos de los procedimientos revisados.

   - Detalle las debilidades detectadas en la lista de chequeo

3.2.6. Gestión de comunicaciones y operaciones.

RESPONSABILIDADES Y PROCEDIMIENTOS DE OPERACIÓN

A.10.1.1 Documentación de procedimientos operativos

Control

[49] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

"Se deberían documentar y mantener los procedimientos de operación y ponerlos a disposición de todos los usuarios que lo requieran." [50]

Lista de chequeo para implantación de políticas

1. ***Documente las políticas definidas para elaboración de manuales políticas y procedimientos.***

   No existen políticas definidas para la elaboración de manuales, no obstante se tienen estándares para elaboración de los mismos.
   No se cuentan con la obligatoriedad para la elaboración de manuales de los procesos que realiza y debería documentar la Universidad Politécnica Salesiana.

2. ***Los manuales actuales están a disposición del personal involucrado***

   Los manuales solo se encuentran en poder del Director de Sistemas, no se encuentran a disposición del personal.

Detalle los códigos de los procedimientos revisados.

- Manuales internos de la Universidad Politécnica Salesiana.

Detalle las debilidades detectadas en la lista de chequeo

- Los manuales de procedimientos deberían de estar a disposición del personal involucrado.

[50] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

A.10.1.2 Gestión de cambios.

Control

"Se deberían controlar los cambios en los sistemas y recursos de tratamiento de información." [51]

1. ***Verificar si actualmente se deja constancia de alguna modificación en los manuales de procedimientos***

   Actualmente si se lleva registros de los cambios realizados en los manuales indicando el procedimiento que se modifico, se cuenta con control de versionamiento.

2. ***Revisar en políticas de la gestión de cambios.***

   Actualmente no se cuenta con políticas internas para la gestión de cambios aplicativos.

A.10.1.3 Segregación de tareas.

Control

"Se deberían segregar las tareas y las áreas de responsabilidad con el fin de reducir las oportunidades de una modificación no autorizada o no intencional, o el de un mal uso de los activos de la organización." [52]

Lista de chequeo para implantación de políticas

[51] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >
[52] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

1. ***Verificar si existen políticas de segregación de funciones***

No existen políticas de segregación de funciones. Actualmente la Universidad Politécnica Salesiana no cuenta con la implementación completa de la segregación de tareas en todos sus aplicativos.

Según nos informo el Director de Sistemas se está llevando a cabo un proyecto en el cual se quiere implementar la segregación de funciones a nivel de los sistemas aplicativos.

Detalle los códigos de los procedimientos revisados.

- Manuales de procedimientos internos

A.10.1.4 Separación de los recursos de desarrollo, prueba y operación.

Control

"La separación de los recursos para desarrollo, prueba y producción es importante para reducir los riesgos de un acceso no autorizado o de cambios al sistema operacional." [53]

Lista de chequeo para implantación de políticas:

1. ***Revisar manuales referentes a pases a producción.***

Actualmente en la Universidad Politécnica Salesiana sede Guayaquil no se realizan este tipo de procedimientos. Es poco común la realización de un pase de versión de un aplicativo. Todo está de manera centralizada en la sede de Cuenca.

[53] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

Para los desarrollos que se realizan en la sede de Guayaquil, no se cuenta con una red de desarrollo.

2. ***Documentar los controles que se tiene para pases a producción, referente a los ambientes mantenidos para desarrollo, pre-producción y producción.***

   Los controles que la Universidad Politécnica Salesiana adopta para el desarrollo es la creación de una VLAN para las pruebas.

3. ***Que controles se tienen cuando se copian datos de producción para un desarrollo.***

   Actualmente cuando los desarrolladores necesitan de una base de datos para realizar pruebas las puede solicitar la base de datos. Toda esa información es entregada tal y cual sin ningún cambio.

GESTIÓN DE LA PROVISIÓN DE SERVICIOS POR TERCEROS.

A.10.2.1 Provisión de servicios.

Control

"Debemos asegurarnos que todos los controles de seguridad, definiciones de servicios y niveles de entregas incluidas en el acuerdo de entrega de servicio externo sean implementados, operados." [54]

Todo el control y guía de implementación, está incluido en la política, 6.2.3, 8.3.2.

[54] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

A.10.2.2 Monitoreo y revisión de los servicios externos

Control

"Los servicios, reportes y registros provistos por terceros deben ser monitoreados y revisados regularmente, y las auditorias deben ser llevadas a cabo regularmente." [55]

Lista de chequeo para implantación de políticas

1. ***Verificar si existe un monitoreo de personal externo y la revisión de los servicios entregados por terceros para garantizar el cumplimiento de los términos y condiciones del contrato.***

   Actualmente si existe un control de estas actividades, sin embargo no existe ninguna política que lo indique, se recomienda publicar una política referente al tema.

A.10.2.3 Gestión del cambio en los servicios prestados por terceros.

Control

"Los cambios en la provisión del servicio, incluyendo mantenimiento y mejoras en las políticas de seguridad de información existentes, en los procedimientos y los controles se deberían gestionar teniendo en cuenta la importancia de los sistemas y procesos del negocio involucrados, así como la reevaluación de los riesgos." [56]

Lista de chequeo para implantación de políticas

[55] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >
[56] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

1. ***Indagar, cuando se hace cambios en el contrato de los proveedores que se es tomado en cuenta:***

   Actualmente al momento de actualizar un contrato de un proveedor se toman las siguientes recomendaciones:

   - Mejoras en los servicios actuales ofrecidos
   - Cambios que se hayan dado en la Universidad.
   - Incorporación de controles nuevos para resolver incidentes de seguridad de la información o mejorar la seguridad.

PLANIFICACIÓN Y ACEPTACIÓN DEL SISTEMA.

A.10.3.1 Gestión de capacidades.

Control

"El uso de recursos deben ser monitoreados y las proyecciones hechas de requisitos de capacidad adecuadas futuras para asegurar el sistema de funcionamiento requerido." [57]

Lista de chequeo para implantación de políticas

1. ***Detalle si existe una política, que especifique que antes de implantación de una actividad nueva (Sistema, servidor, producto nuevo), hay un proceso de establecimiento donde mide la capacidad futura.***

   Personal del área de Sistemas mantiene un monitoreo constante del rendimientos de los servidores y servicios de la Universidad Politécnica

[57] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

Salesiana sede Guayaquil. En caso de que sea de un proyecto nuevo se realiza laboratorios para verificar si el rendimiento es óptimo.

A.10.3.2 Aceptación del sistema.

Control

"Se deberían establecer criterios de aceptación para nuevos sistemas de información y versiones nuevas o mejoras y se deberían desarrollar con ellos las pruebas adecuadas antes de su aceptación." [58]

Lista de chequeo para implantación de políticas.

1. ***Una vez que se pase el sistema a producción, se debe haber establecido un procedimiento de atención de errores.***

   No se cuenta con un procedimiento de atención de errores, en caso de que se

2. ***Antes de pases a producción que tipo de validación realiza o cual se sugiere.***

   Se realizan las pruebas antes de la solicitud del pase a producción.

   Se sugiere que el área de Sistemas, esté presente en las pruebas de certificación efectiva y documentada para:

   - Verificar que los roles y/o transacciones creadas por Seguridad de la Información, realicen los procesos por el cual fue creado.
   - Verificar los controles de seguridad que estén implementados correctamente.

[58] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

- Definir qué tipos de accesos deberán contar cada colaborador según su cargo y/o función; para contar con una base de conocimientos en el momento de otorgarle los roles o atributos.

Importante:

Es importante debido a que se deben establecer criterios de aceptación para sistemas de información nuevos, actualizaciones y nuevas versiones, también se debe llevar a cabo las pruebas adecuadas del sistema antes de su aceptación.

PROTECCIÓN CONTRA EL CÓDIGO MALICIOSO Y DESCARGABLE.

A.10.4.1 Controles contra el código malicioso.

Control

"Se deberían implementar controles para detectar el software malicioso y prevenirse contra él, junto a procedimientos adecuados para concientizar a los usuarios." [59]

Lista de chequeo para implantación de políticas

1. ***Verificar si existe una política formal que requiera el cumplimiento de las licencias de software y la prohibición del uso de software no autorizado***

   Se verificaron los manuales existentes y no se encontró política referente al tema, se recomienda la publicación de una política de antivirus.

[59] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

El Director de Sistemas controla el licenciamiento del antivirus, para proteger el prestigio de la Institución.

La instalación y actualización de la herramienta de monitoreo de virus informático; las revisiones deberá incluir:

- Verificación de archivos electrónicos de origen incierto o no autorizado, o recibidos a través de redes no fiables, para comprobar la existencia de virus antes de usarlos.

- Verificación de todo archivo adjunto a un correo electrónico o de toda descarga para buscar software malicioso antes de usarlo. Esta comprobación se hará en distintos lugares, por ejemplo, en los servidores de correo, en los computadores personales o a la entrada en la red de la universidad.

- Verificación de códigos maliciosos en las páginas WEB.

Detalle las debilidades detectadas en la lista de chequeo

- Se recomienda la creación de un manual de procedimientos de prevención contra código maliciosa.

A.10.4.2 Controles contra el código descargado en el cliente.

Control

"Donde el uso de código móvil es autorizado, la configuración debe asegurar que dicho código móvil opera de acuerdo a una política de seguridad definida y que se debe prevenir que este sea ejecutado." [60]

[60] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

Lista de chequeo para implantación de políticas

1. ***Verificar si existe una política formal que requiera el cumplimiento de las licencias de software y la prohibición del uso de software no autorizado en los dispositivos móviles.***

   Se verificaron los manuales existentes y no se encontró política referente al tema, se recomienda la publicación de una política de antivirus.

COPIAS DE SEGURIDAD.

A.10.5.1 Copias de seguridad de la información.

Control

"Se deben de realizar copias de respaldo de la información y del software, y se deben poner a prueba con regularidad de acuerdo con la política de respaldo acordada." [61]

Lista de chequeo para implantación de políticas

1. ***Documente el esquema de respaldos que actualmente se utiliza.***

   La Universidad Politécnica Salesiana cuanta con un manual de procedimientos en la cual detalla los esquemas de respaldos que utiliza. El Director de Sistemas tiene políticas internas sobre los tiempos de permanencia de los respaldos.

[61] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

2. ***Donde se mantiene los registros exactos y completos de las copias de respaldo y existen procedimientos documentados de su restauración por solicitud del usuario.***

   La Universidad Politécnica Salesiana mantiene sus raspados en cintas magnéticas en el departamento de Sistemas. Se tiene como contingencia tapes de respaldos en un sitio alterno.

3. ***Los respaldos se los debe de mantener con controles físicos y ambientales que aseguren que estos no se perderán o deteriorarán.***

   En el sitio alterno donde se guardan los tapes de respaldos de la Universidad Politécnica Salesiana existen controles físicos y lógicos para impedir el acceso no autorizado. Además cuanta con un ambiente adecuado para la protección de la integridad de los tapes.

GESTIÓN DE LA SEGURIDAD DE LAS REDES.

A.10.6.1 Controles de red.

Control

"Las redes deben ser manejadas y controladas adecuadamente para proteger de amenazas y para mantener las seguridades en los sistemas y aplicaciones usando las redes, incluyendo información en tránsito." [62]

Lista de chequeo para implantación de políticas

1. ***Existe una segregación de responsabilidades en el departamento de Sistemas.***

[62] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

Se verifico el manual de responsabilidades, actividades y servicios y se pudo verificar que existe segregación de funciones en las responsabilidades del personal.

2. ***Indagar con el Director de Sistemas y consultar que controles especiales se tiene para que los datos transmitidos a través de la LAN y WAN, estén protegidos su confidencialidad e integridad, por ejemplo uso de criptografía.***

   Para prevenir cualquier situación de riesgo, existen varias VLAN, adicionalmente existe un Firewall perimetral.

3. ***Indague con el Director de Sistemas y consultar que monitoreos se tiene o se van a implementar en muy corto plazo para revisar el intento de ataques o actividades no autorizadas en la red.***

   Si se realizan monitoreos, la persona responsable es el Director de Sistemas.

Detalle los códigos de los procedimientos revisados.

- Responsabilidades, actividades y/o servicios

Detalle las debilidades detectadas en la lista de chequeo

- Se recomienda que exista una segregación funcional adecuada para que la persona que administra la red, sea independiente al responsable que administra la estructura de la base de datos y operaciones del centro de cómputo.

A.10.6.2 Seguridad de los servicios de red.

Control

"Las características de seguridad, niveles de servicio y los requisitos de gestión de todos los servicios de red deben ser identificadas e incluidos en cualquier acuerdo de servicio de red, así estos servicios sean provistos dentro o fuera de la organización." [63]

Lista de chequeo para implantación de políticas

1. ***Obtenga el contrato de Enlaces y extraiga las clausulas que indiquen los compromisos acordados para gestionar de forma segura la red (Integridad, disponibilidad y confidencialidad).***

   No se pudo obtener el contrato debido a que es manejado en la sede principal (Cuenca), sin embargo se implantarán políticas referentes al tema.

MANIPULACIÓN DE LOS SOPORTES.

A.10.7.1 Gestión de soportes extraíbles.

Control

"Debería haber procedimientos para la gestión de los medios informáticos removibles." [64]

Lista de chequeo para implantación de políticas

[63] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >
[64] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

1. ***En caso de que se quiere realizar una destrucción de medios (cintas, discos, memorias flash (USB, SD etc.), discos duros removibles, CD, DVD, medios impresos y cualquier otro dispositivo en el cual se pueda almacenar información para ser transportada), investigue que proceso se tiene para su ejecución segura.***

   En el departamento de Sistemas realiza los respaldos en Tape estos no son destruidos, caso contrario siempre los están reutilizando.

2. ***Verificar que se realice la identificación de medios removibles. (etiquetado)***

   Todos los medios de respaldos están codificados de manera que el personal de Sistemas de la Universidad Politécnica Salesiana pueda identificarlos fácilmente.

3. ***Documente si existen controles al momento de habilitar nuevas estaciones para dejar inhabilitado el lector de CD y puertos USB (Las unidades de medios removibles solo se podrían habilitar si existen razones para hacerlo).***

   Actualmente la Universidad Politécnica Salesiana al momento de habilitar una estación para un colaborador no se les inhabilita los puertos USB o la unidad de CD. No se tiene como buenas prácticas de seguridad restringir el acceso a los medios extraíbles.

4. ***Indague si existe controles criptográficos para información a respaldar sensitiva.***

   Todos los respaldos de la Universidad Politécnica Salesiana cuentan con encriptación de sus datos,

Control a implementar

Los archivos de información de respaldos tendrán programada una encriptación y autenticación para resguardar la integridad y seguridad de la información.

Detalle los códigos de los procedimientos revisados.

- Manual de respaldos de la Universidad Politécnica Salesiana.

A.10.7.2 Retirada de soportes.

Control

"Se deberían eliminar los medios de forma segura y sin peligro cuando no se necesiten más, utilizando procedimientos formales." [65]

Lista de chequeo para implantación de políticas

1. ***Verificar como es el proceso de destrucción de la información de la Universidad Politécnica Salesiana.***

   Se pudo evidenciar que en todos los departamentos de la Universidad Politécnica Salesiana que no existe un proceso definido para la destrucción de la información generada en cada departamento.

   No se cuenta con las herramientas necesarias para destruir la información impresa o en CD.

[65] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

A.10.7.3 Procedimientos de manipulación de la información.

Control

"Los procedimientos para la manipulación y almacenamientos de la información deben ser establecidos para proteger esta información de divulgaciones o usos no autorizados." [66]

Control contemplado en el control 10.7.1, 10.7.2, 10.5.1 y 7.2

A.10.7.4 Seguridad de la documentación del sistema.

Control

"La documentación de sistemas debe ser protegida contra acceso no autorizado." [67]

Lista de chequeo para implantación de políticas

1. ***Que procedimiento se tiene para no publicación de procesos sensibles, se debe de considerar los siguientes aspectos:***

   Actualmente no se publican los manual de procedimientos, los manual de procedimientos de Sistemas son custodiados por ellos mismo. No se cuenta con ocultamiento de información sensible.

[66] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >
[67] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

INTERCAMBIO DE INFORMACIÓN.

A.10.8.1 Políticas y procedimientos de intercambio de información.

Control

"Se deberían establecer políticas, procedimientos y controles formales de intercambio con el fin de proteger la información a través de todos los tipos de instalaciones de comunicación." [68]

Lista de chequeo para implantación de políticas

1. ***Investigar en los manuales internos qué políticas de seguridad especifican intercambio de información.***

   Actualmente no existen políticas referentes al intercambio de información.

2. ***Intercambio de información electrónica***

   Las transmisiones a los bancos sobre las recaudaciones realizadas día a día, esta transmisión se la realiza por medio del protocolo https y viaja encriptado.

3. ***En caso de que se intercambie información sensitiva por correo electrónico, este también debe de estar encriptado.***

   Actualmente esa información no es encriptado, no se ve la necesidad por el momento de encriptar la información de correo electrónico porque no es enviada información confidencial.

[68] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

A.10.8.2 Acuerdos de intercambio.

Control

"Los acuerdos deben ser establecidos para el intercambio de información y software entre la organización y terceros." [69]

Lista de chequeo para implantación de políticas

1. ***Analice si existe una política que especifique que deberá existir un acuerdo de confidencialidad y buen uso de los recursos de procesamiento de la información, antes de otorgar acceso a un externo.***

   Actualmente no se cuenta con esta política, se recomienda incorporarla. No se cuenta con convenios de confidencialidad.

A.10.8.3 Soportes físicos en tránsito.

Control

"Los medios conteniendo información deben ser protegidos contra acceso no autorizado, mal uso o corrupción durante el transporte fuera de los límites físicos de la organización." [70]

Control contemplado en el control 10.8.1 y 10.8.2

[69] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >
[70] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

A.10.8.4 Mensajería electrónica.

Control

"La información implicada con la mensajería electrónica debe ser protegida apropiadamente." [71]

Lista de chequeo para implantación de políticas

1. ***Documente todas las políticas contenidas en manuales, así como también de medios tecnológicos que correspondan a controles sobre correo electrónico. (políticas ya sean administrativas o técnica).***

   Actualmente solo existe un manual de configuración de correo electrónico, no existen políticas del buen uso del correo electrónico.

2. ***En lo referente a mensajería electrónica enviada a clientes, verifique que controles existen***

   El departamento de Sistemas para garantizar la disponibilidad del servicio, permanentemente realiza monitoreo del servicio para verificar su correcto funcionamiento.
   Garantizar que la dirección del mensaje es correcta, garantiza la disponibilidad del servicio de entrega de mensajes a los clientes.

3. ***Política del personal que está autorizado a utilizar mensajería instantánea para clientes.***

   Actualmente solo existe la firma en la que solicitan la creación o configuración del correo electrónico, se recomienda crear un formulario específico de correo electrónico y adicionalmente exigir que se firme una carta de responsabilidad del buen uso de la información.

[71] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

Detalle los códigos de los procedimientos revisados.

- Manual de documentación de correos masivos.
- Instructivo del personal para llenar formularios.

A.10.8.5 Sistemas de información empresariales.

Control

"Se deberían desarrollar e implementar políticas y procedimientos con el fin de proteger la información asociada con la interconexión de sistemas de información de negocios." [72]

Control no aplica para la Universidad Politécnica Salesiana sede Guayaquil.

SERVICIOS DE COMERCIO ELECTRÓNICO.

A.10.9.1 Comercio electrónico.

Control

"La información envuelta en el comercio electrónico pasando a través de redes públicas, debe ser protegida de actividades fraudulentas, dispuesta de contratos y de acceso y modificación no autorizada." [73]

Control no aplica para la Universidad Politécnica Salesiana sede Guayaquil.

[72] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >
[73] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

A.10.9.2 Transacciones en línea.

Control

"La información implícita en las transacciones en líneas debe ser protegida para prevenir la transmisión incompleta, ruta equivocada, alteración no autorizada de mensajes, acceso no autorizado, duplicado no autorizado del mensaje o reproducción." [74]

Control no aplica para la Universidad Politécnica Salesiana sede Guayaquil.

A.10.9.3 Información públicamente disponible.

Control

"La integridad de la información que se ha hecho disponible en un sistema público debe ser protegido para prevenir modificaciones no autorizadas." [75]

Lista de chequeo para implantación de políticas

1. ***Se requiere saber el cuál es el proceso de autorización, para validar la información pública de la empresa antes de que esté disponible a externos.***

   Este requerimiento no se pudo llevar a cabo debido a que todo este tipo de información es manejado en la sede principal cuenca, sin embargo se incorporaran políticas referentes al tema.

[74] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >
[75] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

Detalle los códigos de los procedimientos revisados.

- Pagina web de la Universidad.

SUPERVISIÓN.

A.10.10.1 Registros de auditoría.

Control

"Los registros de auditoría grabando actividades de los usuarios, excepciones y eventos de la seguridad de información deben ser producidos y guardados para un periodo acordado con el fin de que asistan en investigaciones futuras y en el monitoreo de los controles de acceso." [76]

Lista de chequeo para implantación de políticas

1. ***Cuando un usuario se logonea en una máquina, donde y que tiempo queda grabado el evento.***

   Actualmente existen varios Domain Controler en cada sede, la estación para poder logonearse buscará los Domain Controler según su configuración, por lo general buscarán los de la misma sede.

   La capacidad configurada para los registro de actividad es la que viene por default (128MB) por lo general la capacidad se llenan aproximadamente en una semana, luego de este tiempo se sobrescriben.

2. ***Qué tipo de información se guarda (que tiene el log).***

[76] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

Se almacenan todo tipo de evento, desde que el usuario se logoneo hasta que apago el equipo.

3. ***Para cambio de clave de red, donde se guarda los registros de log.***

   Este tipo de eventos es guardado en el evento de seguridad del Domain Controler que fue logoneado.

4. ***Indagar como se podría desactivar el grabado de los log's y quién tiene acceso para realizar esta tarea.***

   Se podría desactivar con un usuario administrador desde uno de los domain controler.

Detalle los códigos de los procedimientos revisados.

- Reunión con director de Sistemas

A.10.10.2 Supervisión del uso del sistema.

Control

"Los procedimientos para el uso del monitoreo de las instalaciones de procesamiento de información deben ser establecidos y los resultados de las actividades de monitoreo deben ser revisadas regularmente." [77]

Lista de chequeo para implantación de políticas

1. ***Verificar si existe monitoreo de acceso a red.***

   Si se realizan Monitoreos de la red desde cada sede.

[77] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

2. ***Monitoreo de uso de cuentas privilegiadas como Domain Admin***

   Actualmente no se realizan estos tipos de Monitoreos, sin embargo se adicionará una política que referencie esta recomendación.

3. ***Monitoreo a los firewalls.***

   Este tipo de Monitoreos son realizados en la sede principal.

A.10.10.3 Protección de la información de los registros.

Control

"Las instalaciones de información de registro deben ser protegidas contra acciones forzosas u accesos no autorizados." [78]

Se incluyó política referente al tema en el dominio 10.10.1

A.10.10.4 Registros de administración y operación.

Control

"Actividades del administrador y de los operadores del sistema deben ser registradas." [79]

Lista de chequeo para implantación de políticas

[78] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >
[79] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

1. ***Para los usuarios que son Domain Admin, debe existir un monitoreo de sus actividades, que incluya hora de registro, acción que realizó.***

   Actualmente no existe un control referente al tema, se recomienda que se cree un procedimiento de monitoreo de actividades.

   Detalle las debilidades detectadas en la lista de chequeo

   Se recomienda que se cree un procedimiento de monitoreo de actividades de los usuarios administradores.

A.10.10.5 Registro de fallos.

Control

"Las averías deben ser registradas, analizadas y se debe tomar acciones apropiadas." [80]

Lista de chequeo para implantación de políticas

1. ***Verificar si hay un registro de averías con el procesamiento o comunicación de la información.***

   Con respecto al procesamiento de datos no existe un registro de averías, todo queda registrado en el visor de eventos.
   Por el lado de averías de comunicación tampoco existen datos.
   Se recomienda la centralización de los visores de eventos de los servidores principales.

2. ***Documente políticas sobre la atención de requerimientos que hablen sobre registros de errores.***

[80] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

No se encontraron políticas referentes al tema.

3. ***Verifique si son revisadas los registros de errores.***

Solo son verificados cuando surge una falla en algún aplicativo, sin embargo no existe un procedimiento de monitoreo frecuente de los mismos.

10.10.6 Sincronización del reloj.

Control

"Los relojes de todos los sistemas de procesamiento de información dentro de la organización o en el dominio de seguridad deben ser sincronizados con una fuente acordada y exacta de tiempo." [81]

Lista de chequeo para implantación de políticas

1. ***Verificar si las computadoras de la universidad disponen de la misma hora.***

Las computadoras de la universidad no se encuentran con una sincronización de hora, se recomienda crear un proceso que al momento de logonearse al dominio se actualice la hora.

[81] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

3.2.7. Control de acceso.

REQUISITOS DEL NEGOCIO PARA EL CONTROL DE ACCESO.

A.11.1.1 Políticas de control de acceso

Control

"Una política de control de acceso debe ser establecida, documentada y revisada y debe estar basada en los requisitos de seguridad y del negocio." [82]

Lista de chequeo para implantación de políticas

1. ***Documente los requisitos de seguridad para las aplicaciones de la Institución, por ejemplo: Toda aplicación deberá contar con un usuario y clave de acceso, no se permitirán sesiones concurrentes, etc.***

   En la reunión mantenida con el Coordinador de Tecnología de Información de la sede Guayaquil, nos detallo que se han realizado proyectos en cuanto las aplicaciones para que se puedan logonear con su propio usuario, actualmente se encuentran en un proceso de integración de aplicaciones ya que actualmente son pocos los sistemas integrados.

   Según lo documentado con el responsable del Área de Sistemas se está estandarizando que todas las aplicaciones en producción de la Universidad Politécnica Salesiana sede Guayaquil deben contar con un nivel de autenticación, es decir, que para usar cualquier aplicación deberá contar con un usuario y una contraseña

[82] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

2. ***Verifique la existencia de una política que obligue a mantener perfiles de acceso a los usuarios estandarizados según su labor en la Universidad.***

   Actualmente la Universidad Politécnica Salesiana no cuenta con perfiles de usuarios, tan solo se tienen ciertos roles para los accesos. Con la integración de las aplicaciones se está creando perfiles de usuarios según sus funciones y responsabilidades.

3. ***Verificar si con los actuales procedimientos y políticas de acceso a los diferentes aplicativos o recursos, existe una segregación de funciones en lo que se refiere a solicitud, autorización y administración de accesos***

   Como se tiene en proyecto estandarizar las aplicaciones, en la actualidad no se cuenta con segregación de tareas, un mismo usuario puede solicitar, aprobar y autorizar una transacción. Se deber regularizar lo más pronto posible ya que esto causaría un riesgo de alto nivel.

4. ***Documente las políticas y procedimientos existentes que respalde el retiro de los derechos.***

   No se tiene normas para reportar las desvinculaciones de los empleados. El responsable de control de accesos de la Universidad Politécnica Salesiana retira los accesos cuando se entera por casualidad de la desvinculación de un empleado, en pocos casos es el área de Recursos Humanos quien notifica la salida del colaborador.

   No se ha evidenciado manuales de procedimiento que detallen políticas de accesos, recientemente la gran mayoría de las aplicaciones de la Universidad Politécnica Salesiana ha incorporado controles para la segregación de tareas en los aplicativos. Anteriormente cualquier

usuario podía realizar la mayoría de las transacciones que la aplicación poseía, tan solo ciertas transacciones estaban segregadas.

Detalle las debilidades detectadas en la lista de chequeo

- No se tienen definidos perfiles de usuarios, según el cargo o función que desempeña el colaborador en la institución.
- Claves de usuarios administradores no han sido cambiadas después de la desvinculación de personal clave.
- No se cuenta con segregación de tareas.

GESTIÓN DE ACCESO DE USUARIO.

A.11.2.1 Registro de usuarios

Control

"Se debería formalizar un procedimiento de registro de altas y bajas de usuarios para garantizar el acceso a los sistemas y servicios de información multiusuario." [83]

Lista de chequeo para implantación de políticas

1. ***Documente el proceso que se utiliza para que los empleados comprendan las condiciones de acceso. (**compromiso de responsabilidad y hacer referencia donde lo estamos nombrando**)***

   Actualmente la Universidad Politécnica Salesiana no ha realizado concientización de los empleados sobre las responsabilidades o condiciones al otorgarle accesos a la red y aplicativos en general.

[83] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

La Universidad Politécnica Salesiana deberá implementar y legalizar un documento de compromisos de responsabilidades que los empleados internos y externos deberán cumplir para poder asegurar el buen uso de los recursos.

2. ***Comprobar la existencia de documentos de compromiso antes de otorgar acceso a los diferentes entornos (empleado Internos y externos).***

   En la actualidad la Universidad Politécnica Salesiana no cuenta con un documento de compromiso de responsabilidad.

Detalle las debilidades detectadas en la lista de chequeo

- No se cuentan con documentos formales que impida la creación de usuarios genéricos, o controlar dicha creación.
- No existe documentos de responsabilidad del empleado interno o externo antes de otorgarle acceso a los recursos.

A.11.2.2 Gestión de privilegios

Control

"Debería restringir y controlarse el uso y asignación de privilegios." [84]

Lista de chequeo para implantación de políticas

Control contemplado en el control 11.1 y 11.2

[84] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

A.11.2.3 Gestión de contraseñas de usuario

Control

"Se deberían controlar la asignación de contraseñas por medio de un proceso de gestión formal." [85]

Lista de chequeo para implantación de políticas

1. ***Documente las políticas que obligan al usuario la firma del compromiso de responsabilidad del empleado antes de concederles acceso a la red.***

   En la actualidad la Universidad Politécnica Salesiana no cuenta con un documento de compromiso de responsabilidad. Ref.: control 11.2.1 Registro de usuarios literal 3

2. ***Documente la política que exige que cada vez que se le otorgue una contraseña a un usuario para acceso a cualquier recurso, esta debe nacer expirada.***

   La Universidad Politécnica Salesiana no cuenta con documentación formal aprobada por el alto Directorio. Se tiene como buenas prácticas de seguridad, que al momento de otorgar una nueva clave a cualquier usuario para acceso a cualquier recurso de la institución, esta clave debe nacer expirada.

3. ***Verifique procedimientos que se tiene actualmente para verificar la identidad de un usuario antes de proporcionarle una contraseña temporal o reemplazo a la nueva.***

[85] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

Los empleados internos y externos de la Universidad Politécnica Salesiana realizan una llamada al personal responsable del procedimiento para otorgar nueva clave, antes de concederle la nueva clave al usuario este debe de confirmar algunos datos personales para poder proporcionarle la contraseña nueva o en reemplazo, además deberán ser entregarlas caducadas para poder ser cambiada por el usuario y solo el conocerla

4. ***Documente la existencia de un procedimiento donde no se permita enviar contraseñas temporales vía correo o sin protección.***

   Personal responsable de la administración de los usuarios de dominio de la Universidad Politécnica Salesiana, son los comprometidos a otorgar esta contraseña de forma personalizada, evitando el riesgo de intersección de esta y poder realizar acciones fraudulentas.

5. ***Documente si existe la política de que las contraseñas predeterminadas por el proveedor deben de cambiarse inmediatamente después de la instalación de los sistemas o software.***

   El Director del área de Sistemas de la Universidad Politécnica Salesiana tiene como buena práctica de seguridad de la información, cambiar las claves por default del producto una vez que el proveedor haya terminado la implementación de este.

A.11.2.4 Revisión de los derechos de acceso de los usuarios

Control

"El Rectorado debería establecer un proceso formal de revisión periódica de los derechos de acceso de los usuarios." [86]

[86] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

Lista de chequeo para implantación de políticas

1. ***Verificar la constancia de una herramienta en la cual el administrador de control de acceso este actualizado o informado de los cambios de área o funciones en su labor para restringir acceso a los aplicativos anteriores.***

   La Universidad Politécnica Salesiana no tiene un sistema para la administración de accesos a los diferentes aplicativos. Además no se cuenta con un procedimiento para la notificación del estado de los empleados, entiéndase por:

   - Cambio de área
   - Vacaciones
   - Licencia por maternidad o enfermedad
   - Calamidad domestica.

RESPONSABILIDAD DEL USUARIO

A.11.3.1 Uso de contraseñas

Control

"Los usuarios deberían seguir buenas políticas de seguridad para la selección y uso de sus contraseñas." [87]

Lista de chequeo para implantación de políticas

[87] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

1. ***Detallar las obligaciones y responsabilidades de los usuarios en mantener la confidencialidad de sus claves y los controle que debe tener.***

   En la Universidad Politécnica Salesiana no se tiene normas sobre la confidencialidad de sus claves de acceso. No se ha realizado campañas de concientización sobre la seguridad de la información.

2. ***Detallar las políticas de la seguridad que deberá tener las contraseñas por parte de los usuarios.***

   No se cuentan con normas de seguridad formales, se han adoptado buenas prácticas de seguridad de la información para las contraseñas de acceso a la red.

   Estas normas son;

   - Nacen expiradas
   - Caracteres mínimos y máximos, etc.

A.11.3.2 Equipo informático de usuario desatendido

Control

"Los usuarios deberían asegurar que los equipos informáticos desatendidos estén debidamente protegidos." [88]

Lista de chequeo para implantación de políticas

[88] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

1. ***Verificar si existen políticas o procedimientos que detallen la protección de sus equipos en su ausencia (Protector de pantalla con clave, desconectarse de las aplicaciones, etc.).***

   No se cuentan con políticas de dominio de inactivación de la estación por equipo desatendido.

   Se debe incluir una política de que todos los equipos al finalizar el día deben de estar apagados.

A.11.3.3 Política de pantalla y escritorio limpio

Control

"Se deberían adoptar una política de escritorio para papeles y medios removibles de almacenamiento así como una política de pantalla limpia instalaciones de procesamiento de información." [89]

Lista de chequeo para implantación de políticas

1. ***Detallar las políticas de seguridad sobre pantallas y escritorios limpios.***

   No se cuenta con las buenas prácticas de seguridad para escritorios limpios.

2. ***Detallar las políticas de puntos de impresión.***

   No se cuenta con las buenas prácticas de seguridad para impresiones desatendidas.

[89] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

CONTROL DE ACCESO A LA RED

A.11.4.1 Política de uso de los servicios de la red

Control

"Los usuarios sólo deberían tener acceso directo a los servicios para los que estén autorizados de una forma específica." [90]

Lista de chequeo para implantación de políticas

1. ***Verifique en los actuales procedimientos, si existe una política especificando quien puede autorizar el acceso a qué red o que servicio de red.***

   No se cuentan con políticas formales, pero la responsabilidad de autorizar el acceso a la red o al servicio de red es el Director del área de sistemas.

A.11.4.2 Autenticación de usuario para conexiones externas

Control

"Se deben utilizar métodos apropiados de autentificación para controlar el acceso de usuarios remotos." [91]

Control no aplica para la Universidad Politécnica Salesiana sede Guayaquil, sin embargo se deben establecer normas de seguridad de acuerdo con el objetivo de control en caso de que se implemente.

[90] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >
[91] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

A.11.4.3 Identificación de equipos en las redes

Control

"Las identificaciones automáticas de equipo deben ser consideradas como medios para autentificar conexiones desde locales y equipos específicos." [92]

Lista de chequeo para implantación de políticas

1. ***Documente si existe actualmente un control automático de red, que identifique a equipos que no son de la Institución conectarse a la Red y no permita acceso a ningún tipo de recursos basándose en registro de estaciones.***

   La Universidad Politécnica Salesiana no cuenta con registros de estaciones, cualquier PC que se quiera conectar a la red de la institución sin ningún tipo de restricción.

A.11.4.4 Diagnostico remoto y configuración de protección de puertos

Control

"Se debería controlar el acceso físico y logístico para diagnosticar y configurar puertos." [93]

Lista de chequeo para implantación de políticas

[92] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >
[93] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

1. ***Verificar si en la Universidad Politécnica Salesiana se cuenta con diagnósticos remotos y configuración de puertos.***

   Este tipo de servicio es lo aplica muy rara vez, el soporte de algún servicio normalmente se lo realiza en las mismas instalaciones de la Universidad Politécnica Salesiana.

A.11.4.5 Segregación en las redes

Control

"Los grupos de servicios de información, usuarios y sistemas de información deben ser segregados en las redes." [94]

Lista de chequeo para implantación de políticas

1. ***Identifique dentro de la Universidad Politécnica Salesiana la existencia de segmentación o separación de la red y los controles (firewall).***

   Se cuenta con un control de firewall perimetral, de esta manera se puede controlar los accesos no autorizados a la red interna de la Universidad Politécnica Salesiana.

A.11.4.6 Control de conexión a las redes

Control

"Los requisitos de la política de control de accesos para redes compartidas, sobre todos para las que atraviesan las fronteras de la

[94] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

organización, se deberían basar en los requisitos de las aplicaciones del negocio." [95]

Control no aplica para la Universidad Politécnica Salesiana sede Guayaquil, sin embargo se deben establecer normas de seguridad de acuerdo con el objetivo de control

A.11.4.7 Control de enrutamiento en la red

Control

"Se deberían implementar controles de enrutamiento que garanticen que las conexiones entre computadores y los flujos de información no incumplan la política de control de acceso a las aplicaciones." [96]

Lista de chequeo para implantación de políticas

1. ***Verificar si existen políticas de enrutamiento de información.***

La Universidad Politécnica Salesiana no cuenta con normas de seguridad para el enrutamiento de la información.

[95] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >
[96] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

CONTROL DE ACCESO AL SISTEMA OPERATIVO

A.11.5.1 Procedimiento de registros de inicio seguro

Control

"El acceso a los sistemas operativos se debería controlar mediante un procedimiento de registro de inicio seguro." [97]

Lista de chequeo para implantación de políticas

1. ***Verificar las políticas de dominio del Directorio Activo, con el fin de confirmar los siguientes datos:***

- ☐ Max número de intentos fallidos
- ☐ Proceso de desbloqueo de clave en caso de que se bloquee.
- ☐ Longitud de la contraseña
- ☐ Nunca mostrar la contraseña en claro.

- Registro de intentos exitosos y fallidos.
- Guardar Registro de Fecha, Hora de inicio exitoso y que el usuario final sea de fácil acceso a esta información.
- Logs, con el detalle de intentos fallidos de registro de inicio desde el último registro exitoso. No se deberá transmitir la contraseña en texto claro a través de la red. Todas estas seguridades expuestas se cumplen cuando el usuario inicia una sesión.

[97] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

A.11.5.2 Identificación y autenticación de usuarios

Control

"Todos los usuarios deberían disponer de un identificador único para su uso personal y debería ser escogida una técnica de autenticación adecuada para verificar la identidad de estos." [98]

Control contemplado en el control 11.5.1

A.11.5.3 Sistema de gestión de contraseñas

Control

"Los sistemas de gestión de contraseñas deberían proporcionar un medio eficaz e interactivo para asegurar la calidad de las mismas." [99]

Lista de chequeo para implantación de políticas

1. ***Verifique que exista normas para cambio periódico de contraseñas.***

   Por norma interna de la Universidad Politécnica Salesiana sede Guayaquil, se tiene como buenas prácticas de seguridad que la contraseña del usuario se la cambie cada 60 días.

2. ***Verifique que exista políticas de complejidad en la contraseña.***

   En las directrices / políticas de contraseñas se tienen activa la opción de complejidad de la contraseña, esto da lugar que el usuario pueda usar números, letras (mayúsculas y minúsculas) y caracteres especiales.

[98] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >
[99] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

Con esta buena práctica se puede reducir el riesgo de accesos no autorizados mediante el descubrimiento de claves de accesos de los colaboradores de la institución.

3. ***Verifique que exista normas para forzar cambio de contraseñas temporales.***

   Todas las claves proporcionadas por primera vez naces de forma expirada, el personal responsable de realizar el proceso de entrega de clave para los usuarios está en la obligación por norma interna de proporcionarla con el estado de expirada para que el usuarios estén forzados a cambiar inmediatamente la clave de acceso.

4. ***Verifique que exista política sobre la reutilización de las contraseñas.***

   Por norma interna la Universidad Politécnica Salesiana sede Guayaquil, no se puede reutilizar las contraseñas de acceso, en las directrices o políticas de contraseña que maneja el administrador de la red se registra las últimas 30 contraseñas

5. ***Verifique que exista políticas formales en la que se especifique que no se debe de mostrar las contraseñas al momento del ingreso.***

   Por buenas prácticas de seguridad de la información, en las directrices de políticas de contraseña se tiene establecido que la momento del ingreso de una contraseña no se la muestre en texto claro sino en forma de asteriscos (****)

Detalle los códigos de los procedimientos revisados.

- Relevamiento de información con el Coordinador de Tecnologías de Información.

Detalle las debilidades detectadas en la lista de chequeo

- No se cuentan con procedimientos formales.

A.11.5.4 Utilización de las facilidades del sistema

Control

"La mayoría de las instalaciones informáticas disponen de programas del sistema capaces de eludir las medidas de control del sistema o de las aplicaciones. Es fundamental que su uso se restrinja y se mantenga fuertemente controlado." [100]

Lista de chequeo para implantación de políticas

1. ***Documente la política que especifique que no se podrá ser administrador de las estaciones.***

   Ningún usuario es administrador de su estación de trabajo, se crean perfiles de usuarios de tal manera que se pueda controlar la administración de estaciones de trabajo.

2. ***Documente la política que especifique que no se puedan instalar programas no autorizados en las estaciones.***

   Para la protección de la imagen de la universidad, esta por políticas interna que ningún usuario pueda instalar programas en sus estaciones de trabajo, para ello se lo tienen que solicitar al área de Sistemas.

[100] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

A.11.5.5 Tiempo de inactividad de la sesión

Control

"Las sesiones se deberían desactivar tras un periodo definido de inactividad." [101]

Lista de chequeo para implantación de políticas.

1. ***Documente las políticas internas sobre el bloqueo de estaciones y aplicaciones después de un periodo de inactividad.***

La Universidad Politécnica Salesiana tiene como políticas que todas las estaciones de los colaboradores de la institución se bloqueen con un periodo de inactividad de 10 minutos, después de este tiempo el usuario deberá colocar su usuario y clave para poder seguir realizando sus tareas pertinentes.

A.11.5.6 Limitaciones del Tiempo de conexión

Control

"Las restricciones en los tiempos de conexión ofrecen seguridad adicional para aplicaciones de alto riesgo." [102]

Control contemplado en el control 11.5.1

[101] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >
[102] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

CONTROL DE ACCESO A LAS APLICACIONES Y LA INFORMACIÓN

A.11.6.1 Restricción de acceso a la información

Control

"Se debería dar acceso a la información y a las funciones del sistema de aplicaciones solo a los usuarios de este, incluido el personal de apoyo, de acuerdo con una política de control de accesos definida." [103]

Control contemplado en el control 11.2.2

A.11.6.2 Aislamiento de sistemas sensibles

Control

"Los sistemas sensibles pueden necesitar entornos informáticos dedicados (aislados)." [104]

Control contemplado en el control 11.4.5

[103] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >
[104] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

ORDENADORES PORTÁTILES Y TELETRABAJO.

A.11.7.1 Informática móvil y comunicaciones

Control

"Se debería adoptar una política formal y medidas de seguridad apropiadas con el fin de protegernos contra los riesgos cuando se usan dispositivos de informática." [105]

Lista de chequeo para implantación de políticas

1. ***Verifique la existencia de políticas internas para computación móvil:***

   No se cuentan con buenas prácticas de seguridad para los equipos móviles, los empleados docentes en su gran mayoría tienen estaciones de trabajo portátiles y no cuentan con las seguridades respectivas.

A.11.7.2 Teletrabajo

Control

"Se deberían desarrollar e implementar una política, planes operacionales y procedimientos para las actividades de teletrabajo." [106]

Lista de chequeo para implantación de políticas

1. ***Detalle los controles y políticas que se tiene para evitar que utilizando la VPN se pueda contagiar de virus la red.***

[105] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >
[106] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

La Universidad Politécnica Salesiana No se cuenta con accesos remotos mediante VPN. Es importante mantener políticas de seguridad respecto a la conexión remota mediante VPN.

3.2.8. Adquisición, desarrollo y mantenimiento de los sistemas.

REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN.

A.12.1.1 Análisis y especificación de los requisitos de seguridad

Control

"Los enunciados de los requisitos de negocios para sistemas nuevos o mejoras a sistemas existentes deberían especificar los requisitos de control." [107]

Lista de chequeo para implantación de políticas

1. ***Detallar si existen políticas de la adquisición o desarrollo de SW según las necesidades de la Universidad Politécnica Salesiana.***

   Políticas de la adquisición o desarrollo de SW de la Universidad Politécnica Salesiana formales no existen.

   Se tiene como buenas prácticas de seguridad que solo el área de Sistemas pueda realizar la adquisición de algún software. En caso de que personal docente o administrativo requiera algún aplicativo este se lo canaliza por medio del Director de Sistemas.

2. ***Documentar si existen políticas de pruebas antes de la adquisición o desarrollo de un software.***

   En la Universidad Politécnica Salesiana no se cuenta con segregación de las redes, como por ejemplo: red de desarrollo y pruebas. Solo tienen la red de producción. Al momento del desarrollo de un aplicativo en el

[107] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

departamento de Sistemas de la sede Guayaquil las pruebas son realizadas en maquinas virtuales.

3. ***Verificar que se cuente con estándares para el desarrollo de software.***

   No se cuenta con estándares para el desarrollo de software.

4. ***Documentar la existencia de los controles que deberán incluir para la seguridad de la información en los aplicativos de la Universidad Politécnica Salesiana.***

   Los controles que deberían incluir en todas las aplicaciones de Universidad Politécnica Salesiana para la seguridad de la información serian:

- Single Sign On
- Perfiles de usuarios
- Para acceso directo a las bases de datos serán atreves de las interfaces aplicativas.
- El token o ticket de sesión
- Identificación única de la sesión del usuario

Detalle las debilidades detectadas en la lista de chequeo

- No se especifican los controles de seguridad necesarios para nuevos sistemas o mejoras de los actuales, por ejemplo adquisición o desarrollo de nuevo software.
- En qué momento del ciclo de vida de desarrollo y adquisición de SW debería estar verificar las seguridades que cuenta el aplicativo.
- Donde se deberían definir los estándares aplicativos referentes de seguridad. Pienso que es el los procedimientos a elaborarse de pases a producción.

TRATAMIENTO CORRECTO DE LAS APLICACIONES.

A.12.2.1 Validación de los datos de entrada

Control

"Se deberían validar los datos de entrada a las aplicaciones del sistema para garantizar que son correctas y apropiadas." [108]

Lista de chequeo para implantación de políticas

1. ***Documentar la existencia de políticas de registro de actividad en los aplicativos.***

   Los aplicativos nuevos de la Universidad Politécnica Salesiana constan de registros de actividad, con esta facilidad, ante un problema de ingresos incorrectos en el sistema se puede verificar los datos ingresados.

   Importante:
   Validar estos datos para asegurar que son correctos y apropiados.

A.12.2.2 Control del proceso interno

Control

"Se deberían incorporar a los sistemas comprobaciones de validación para detectar cualquier tipo de corrupción de información a través de errores del proceso o por actos deliberados." [109]

[108] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >
[109] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

Control contemplado en el control 12.2.1

Importante:

Para evitar que los datos introducidos correctamente puedan comprometerse por errores de procesamiento deberían incorporarse a los sistema comprobadores o validadores que detecten dicha corrupción; los controles requeridos dependerán de la naturaleza de la aplicación y del impacto de la corrupción.

A.12.2.3 Integridad de mensajes

Control

"Se debería identificar los requerimientos para asegurar la autenticación y protección de la integridad de los mensajes en aplicaciones y se deberían de identificar e implementar controles apropiados." [110]

Lista de chequeo para implantación de políticas

Importante:

Se debería establecer mecanismos para controlar la integridad de los mensajes para así detectar cambios no autorizados o corrupción del contenido de un mensaje transmitido, estos controles pueden ser implementados mediante hardware o software.

[110] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

A.12.2.4 Validación de los datos de salida

Control

"Se debería validar los datos de salida de un sistema de aplicación para garantizar que el proceso de la información ha sido correcto y apropiado a las circunstancias." [111]

Lista de chequeo para implantación de políticas

1. ***Documentar las políticas para el desarrollo de aplicaciones referente a la verificación de los datos de salida.***

   El personal dedicado al desarrollo de las aplicaciones de la Universidad Politécnica Salesiana al momento del desarrollo toma las medidas de precaución para no mostrar información más de la necesaria al momento de un error y los datos de salida.

2. ***Documentar la existencia de políticas de registro de actividad como control de las aplicaciones.***

   Los aplicativos nuevos de la Universidad Politécnica Salesiana constan de registros de actividad, con esta facilidad, ante un problema de ingresos incorrectos en el sistema se puede verificar los datos ingresados.

Importante.

Este punto es importante para garantizar que el procesamiento de la información almacenada sea correcto y apropiado, este control puede incluir tareas de validación, verificación y pruebas adecuadas.

[111] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

CONTROLES CRIPTOGRÁFICAS

A.12.3.1 Política de uso de los controles criptográficos

Control

"La organización debería desarrollar e implementar una política de uso de las medidas criptográficas para proteger la información." [112]

Lista de chequeo para implantación de políticas

1. ***Verifique en los actuales procedimientos, si existe una política especificando controles criptográficos para información sensitiva.***

La Universidad Politécnica Salesiana no cuenta con controles criptográficos, es importante tener políticas que sustente este control.

Los controles criptográficos deberán incluir:

- Información transmitida por internet
- Información transportada por medios móviles
- Basada en el interés del negocio
- Basada en la evaluación de riesgos

A.12.3.2 Gestión de claves

Control

"La gestión de claves debe criptográficas debe apoyar el uso de las técnicas criptográficas en la organización." [113]

[112] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

La Universidad Politécnica Salesiana no cuenta con controles criptográficos, es importante tener políticas que sustente este control.

Importante.

Este control es importante para el buen uso de las técnicas criptográficas, un problema de este control puede llevar a debilitar la autenticidad, confidencialidad o integridad de la información, por esta razón es necesario instalar un sistema de administración que de soporte al uso de claves.

SEGURIDAD DE LOS ARCHIVOS DE SISTEMAS.

A.12.4.1 Control del Software en producción

Control

"Deberían existir procedimientos para controlar la instalación del software en sistemas operacionales." [114]

Lista de chequeo para implantación de políticas

1. ***Verificar en los actuales manuales si existe la política de restringir la instalación de software no autorizado y la desinstalación de aplicaciones.***

   Actualmente la Universidad Politécnica Salesiana tienen implementado en las estaciones de laboratorio que al apagarse la PC realiza un resteo,

[113] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >
[114] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

es decir que al encender la estación esta borra toda la documentación, programas ejecutados e instalados.

Esto no quiere decir que se puede instalar cualquier programa, se tienen sesiones con perfiles bajos, no son administradores.

2. ***Detallar las políticas sobre pases de programas a producción.***

En el departamento de Sistemas de la ciudad de Guayaquil, se realiza desarrollos de aplicaciones pero es en la ciudad de Cuenca en la que se realiza el pase a producción.

A.12.4.2 Protección de los datos de prueba del Sistema

Control

"Los datos de prueba deben ser seleccionados cuidadosamente, así como protegidos y controlados." [115]

Lista de chequeo para implantación de políticas

1. ***Verificar en los actuales manuales si existe la política para evitar el uso de datos reales para las pruebas del sistema.***

En el área de Sistemas al momento del desarrollo que requiere la utilización de las bases de datos estas son tomadas de los respaldos antiguos, es decir que se trabaja con las bases de datos de producción desactualizadas.

2. ***Documentar restricciones para el acceso a usuarios en los diferentes ambientes para la realización de pruebas.***

[115] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

Para este caso, como no se cuenta con redes aisladas a la de producción, los usuarios tienen acceso a toda la red interna de la Universidad Politécnica Salesiana.

A.12.4.3 Control de acceso a los códigos de programas fuente

Control

"El acceso a los códigos de programas fuentes debe ser restringido." [116]

Lista de chequeo para implantación de políticas

1. ***Verificar en los actuales manuales sobre la existencia de políticas de transportación y manipulación de código fuente***

   Los códigos fuentes de los desarrollos tanto internos como externos de la Universidad Politécnica Salesiana son custodiados en el mismo departamento. Se tiene respaldos en otro edificio. No se cuentan con políticas para la transportación de los medios.

[116] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE.

A.12.5.1 Procedimiento de control de cambios

Control

"La implementación de cambios debe ser controlada usando procedimientos formales de cambio." [117]

Lista de chequeo para implantación de políticas

1. ***Detallar las políticas existentes sobre control de cambios en las aplicaciones de la Universidad Politécnica Salesiana.***

   La Universidad Politécnica Salesiana no cuenta con políticas de control de cambios formales, se tiene como buenas prácticas de seguridad realizar versionamientos de los aplicativos desarrollados, además documentan los cambios realizados.

2. ***Verificar la existencia de procedimientos eficaces de control de cambios.***

   La Universidad Politécnica Salesiana cuenta con formatos estándares para la solicitud de desarrollo y aceptación del aplicativo creado o mejorado.

[117] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

A.12.5.2 Revisión técnica de los cambios en el sistema operativo

Control

"Se deberían revisar y probar las aplicaciones del sistema cuando se efectúen cambios, para asegurar que no impactan adversamente en el funcionamiento o en la seguridad." [118]

Control contemplado en el control 11.2.2

A.12.5.3 Restricciones en los cambios a los paquetes de software

Control

"No se recomiendan modificar a los paquetes de software. Se deberían limitar a cambios necesarios y todos estos deben ser estrictamente controlados." [119]

Lista de chequeo para implantación de políticas

1. ***Paquetes estándar, preferiblemente no hacer modificaciones, y que en caso de que se requieran que controles se deben aplicar.***

   En caso de que la Universidad Politécnica Salesiana adquiera un paquete de software estándar y requiera la modificación para adaptarlo a las necesidades, se deberá incluir en el contrato un clausula para el mejoramiento interno por parte de la Institución. El proveedor del paquete estándar al momento de la liberación de actualizaciones notificarnos.

[118] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >
[119] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

A.12.5.4 Fuga de información

Control

"Las oportunidades de fuga de información deben ser prevenidas." [120]

Lista de chequeo para implantación de políticas

1. ***Existen políticas sobre el uso no autorizado de la información.***

La Universidad Politécnica Salesiana no cuenta con controles para la protección de la información, en estos casos es muy fácil extraerse la información de la Institución sin que existan alertas de accesos no autorizados. Este control se complementa con los acuerdos de confidencialidad y etiquetado de la información.

Controles a implementar:

- Restringir el almacenamiento de datos en dispositivos removibles no autorizados (Memorias USB, Discos Duros externos, iPods, etc.).
- Restringir la funcionalidad de escritura en unidades CD/DVD.
- Restringir la conexión de impresoras USB.
- Encriptar los datos almacenados en dispositivos removibles.

Detalle las debilidades detectadas en la lista de chequeo

- No existe una clasificación de la Información.
- Actualmente la gran mayoría de los colaboradores no tienen deshabilitado los puertos USB y es por esta vía que se extrae información valiosa de la Universidad Politécnica Salesiana.

[120] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

- Actualmente no se puede controlar la información que es transmitida por correos electrónicos.

A.12.5.5 Desarrollo externo del Software

Control

"El desarrollo externo del software debe ser supervisado y monitoreado por la organización." [121]

Lista de chequeo para implantación de políticas

1. ***Documentar políticas de Desarrollo externo del Software.***

El desarrollo de software para la Universidad Politécnica Salesiana normalmente se lo realiza en sitio. En caso de que se el desarrollo es por personal externo, no se tiene controles de derecho de autor.

GESTIÓN DE LA VULNERABILIDAD TÉCNICA

A.12.6.1 Control de las Vulnerabilidades técnicas.

Control

"Se debe obtener a tiempo la información sobre las vulnerabilidades técnicas de los sistemas de información utilizadas. Igualmente, se debe evaluar la exposición de la organización a tales vulnerabilidades y las medidas apropiadas para tratar los riesgos asociados." [122]

[121] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >
[122] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

Lista de chequeo para implantación de políticas

1. ***Proceso de parches de la Universidad Politécnica Salesiana.***

El proceso operativo de "Security Advisory Patch Management" es administrado a través de la herramienta Microsoft Windows Server Update Services (WSUS) el cual permite a los administradores de las TI implantar las últimas actualizaciones de productos de Microsoft en los sistemas operativos:

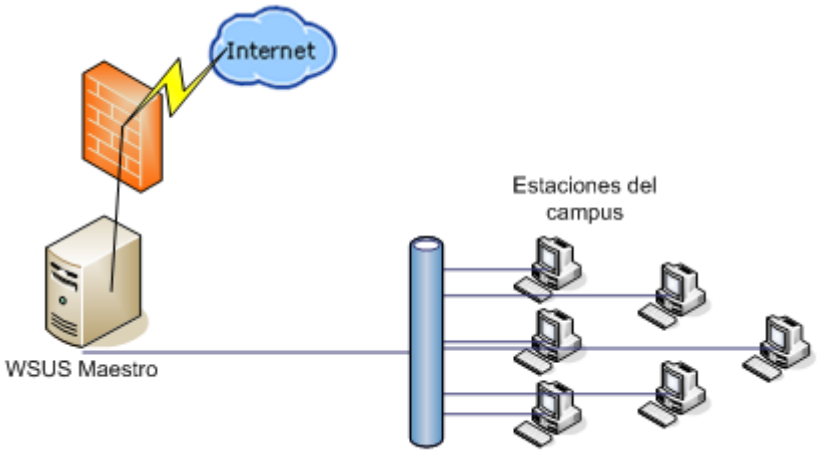
- Microsoft Windows Server 2000
- Windows Server 2003
- Windows XP
- Windows Vista.

Mediante el uso de WSUS se puede gestionar la distribución de actualizaciones que se publican en Microsoft Update a los equipos de su red corporativa.

- Microsoft Update.
- Windows Server Update Service Server - WSUS.
- Automatic Updates.

Gráfico #8

Proceso de actualización de parches



Fuente: Universidad Politécnica Salesiana

Elaborado por: Daniel Romo y Joffre Valarezo

3.2.9. Gestión de incidentes en la Seguridad de la Información.

NOTIFICACIÓN DE EVENTOS Y PUNTOS DÉBILES DE SEGURIDAD DE LA INFORMACIÓN.

A.13.1.1 Reportando los eventos de Seguridad de Información

Control

"Los eventos en la seguridad de información deben ser reportados lo más rápido posible a través de una gestión de canales apropiada." [123]

Lista de chequeo para implantación de políticas

1. ***Verificar si en las herramientas tecnológicas existen reportes automáticos de reportes de incidentes de seguridad.***

   Según la entrevista con el Director del área de sistemas no solo existe alarmas de alerta para intrusos o cambio de políticas en el firewall.

2. ***Verificar la existencia de manuales políticas de reporte de incidentes de seguridad.***

   La Universidad Politécnica Salesiana no cuenta con políticas y procedimientos de reporte de incidentes.

Controles a implementar.

- Monitorear actividades y generar reportes permanentemente.
- Exportar registros a sistemas externos de análisis y generación de reportes.

[123] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

Detalle las debilidades detectadas en la lista de chequeo

- Falta realizar procesos de concienciación sobre la seguridad de la información y de reportar tales eventos, ya que no saben a quién mismo notificar estos problemas.
- No comunican a contratistas y terceros sobre la responsabilidad de informar un incidente de seguridad.

A.13.1.2 Reportando debilidades en la Seguridad de Información

Control

"Todos los empleados, contratistas y terceros que son usuarios de los sistemas y servicios de información deben anotar y reportar cualquier debilidad observada o sospechada en la seguridad de estos." [124]

Lista de chequeo para implantación de políticas

1. ***Detallar las políticas existentes sobre reporte de debilidades.***

   La incitación no cuenta con políticas ni buenas prácticas para reporte de debilidades.

[124] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

GESTIÓN DE INCIDENTES Y MEJORAS DE SEGURIDAD DE LA INFORMACIÓN.

A.13.2.1 Responsabilidades y procedimientos

Control

"Las responsabilidades y procedimientos de la gerencia deben ser establecidas para asegurar una rápida, efectiva y ordenada respuesta a los incidentes en la seguridad de información." [125]

Lista de chequeo para implantación de políticas

1. ***Documentar, de existir un procedimiento formal en el cual debe de estar establecido las responsabilidades ante un incidente de seguridad de la información.***

   La Universidad Politécnica Salesiana no cuenta con procedimientos formales para que los colaboradores de la institución actúen ante un evento de incidente de seguridad de la información.

2. ***Verificar en los actuales manuales las responsabilidades de los colaboradores ante un incidente de seguridad de la información.***

   Actualmente el personal de la Universidad Politécnica Salesiana no tiene conocimiento de cómo actuar ante un incidente de seguridad, no se tienen definidas las responsabilidades ante un evento de seguridad.

[125] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

A.13.2.2 Aprendiendo de los incidentes en la seguridad de información.

Control

"Debe existir un mecanismo que permita que los tipos, volúmenes y costos de los incidentes en la seguridad de información sean cuantificados y monitoreados." [126]

Lista de chequeo para implantación de políticas

1. ***Documentar si existen registros de incidentes de seguridad, con su respectivo informe.***

   Estos informes deberán incluir:

   - Detalle de incidente.
   - En que afecto el incidente, cual fue el impacto que causo a la Universidad Politécnica Salesiana.
   - Informe de cómo resolvieron el incidente.

   De acuerdo a lo investigado, no se tienen registros de los incidentes de seguridad, tan solo se tiene las experiencias y conocimientos de algunos casos de incidentes de seguridad que cuando exista uno en un futuro dicho personal aplicará sus conocimientos para salvaguardas la integridad de la Universidad Politécnica Salesiana.

2. ***Después del incidente, se realiza alguna evaluación para identificar futuros incidentes de seguridad y poder neutralizarlos antes de su ocurrencia.***

[126] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

Al momento de resolver alguna anomalía de seguridad aplican los controles para aislar el incidente, y si en la investigación de estos controles observan alguna vulnerabilidad realizan una evaluación para descartar futuros incidentes, y aplicar las medidas de seguridad.

Detalle las debilidades detectadas en la lista de chequeo

- No se tienen registros de los incidentes de seguridad.
- No se tiene una base de conocimientos estable para gestionar incidentes futuros.

A.13.2.3 Recolección de evidencia.

Control

"Cuando una acción de seguimiento contra una persona u organización, después de un incidente en la seguridad de información, implique acción legal (civil o criminal), la evidencia debe ser recolectada, retenida y presentada para estar conforme con las reglas para la colocación de evidencia en la jurisdicción relevante." [127]

Lista de chequeo para implantación de políticas

1. ***Documentar donde Seguridad de la información custodia y el tratamiento de las evidencias de los incidentes de seguridad de la información.***

Actualmente el área de Sistemas, no custodia ninguna evidencia de los incidentes de seguridad, tan solo se tiene como forma de custodiar las evidencias que llegan por correo electrónico.

[127] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

Detalle las debilidades detectadas en la lista de chequeo

- El área de Sistemas no cuenta con un proceso para el tratamiento y custodia de las evidencias ante un incidente de seguridad.
- No se tiene registros de las evidencias.

3.2.10. Gestión de la continuidad del negocio.

ASPECTOS DE LA SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.

14.1.1 Inclusión de la seguridad de información en el proceso de gestión de la continuidad del negocio

Control

"Se debería instalar en toda la organización un proceso de gestión para el desarrollo y el mantenimiento de la continuidad del negocio a través de la organización que trate los requerimientos en la seguridad de información necesarios para la continuidad del negocio." [128]

Control no aplica para el alcance del presente trabajo, sin embargo se deben establecer normas de seguridad de acuerdo con el objetivo de control.

[128] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

14.1.2 Continuidad del negocio y evaluación de riesgos

Control

"Los eventos que pueden causar interrupciones a los procesos de negocio deben ser identificados, junto con la probabilidad e impacto de dichas interrupciones y sus consecuencias para la seguridad de información." [129]

Control no aplica para el alcance del presente trabajo, sin embargo se deben establecer normas de seguridad de acuerdo con el objetivo de control.

14.1.3 Redacción e implantación de planes de continuidad que incluyen la seguridad de información

Control

"Se deberían desarrollar planes de mantenimiento y recuperación de las operaciones del negocio, para asegurar la disponibilidad de información al nivel y en las escalas de tiempo requeridas, tras la interrupción o la falla de sus procesos críticos." [130]

Control no aplica para el alcance del presente trabajo, sin embargo se deben establecer normas de seguridad de acuerdo con el objetivo de control.

[129] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >
[130] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

14.1.4 Marco de planificación para la continuidad del negocio

Control

"Se debería mantener un esquema único de planes de continuidad del negocio para asegurar que dichos planes son consistentes, para tratar los requisitos de seguridad y para identificar las prioridades de prueba y mantenimiento." [131]

Control no aplica para el alcance del presente trabajo, sin embargo se deben establecer normas de seguridad de acuerdo con el objetivo de control.

14.1.5 Prueba, mantenimiento y reevaluación de los planes de continuidad

Control

"Los planes de continuidad del negocio se deberían probar regularmente para asegurarse de su actualización y eficacia." [132]

Control no aplica para el alcance del presente trabajo, sin embargo se deben establecer normas de seguridad de acuerdo con el objetivo de control.

[131] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >
[132] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

3.2.11. Cumplimiento.

CUMPLIMIENTO CON LOS REQUISITOS LEGALES

A. 15.1.5 Prevención en el mal uso de los recursos de tratamiento de la información

Control

"El personal debe ser disuadido de utilizar los recursos de tratamiento de la información para propósitos no autorizados." [133]

Control no aplica para el alcance del presente trabajo, sin embargo se deben establecer normas de seguridad de acuerdo con el objetivo de control.

A. 15.1.2 Derechos de propiedad intelectual (DPI)

Control

"Se deberían implantar los procedimientos apropiados para asegurar el cumplimiento de las restricciones legales, reguladoras y contractuales sobre el uso del material protegido por derechos de propiedad intelectual y sobre el uso de productos de software propietario." [134]

Control no aplica para el alcance del presente trabajo, sin embargo se deben establecer normas de seguridad de acuerdo con el objetivo de control.

[133] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >
[134] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

A. 15.1.3 Salvaguarda de los registros de la organización

Control

"Se deberían proteger los registros importantes de la organización frente a su pérdida, destrucción y falsificación en concordancia con los requisitos regulatorios, contractuales y de negocio." [135]

Control no aplica para el alcance del presente trabajo, sin embargo se deben establecer normas de seguridad de acuerdo con el objetivo de control.

A. 15.1.4 Protección de los datos y de la privacidad de la información personal

Control

"La protección de datos y la privacidad debe ser asegurada como se requiere en la legislación, las regulaciones y, si es aplicable, en las cláusulas contractuales." [136]

Control no aplica para el alcance del presente trabajo, sin embargo se deben establecer normas de seguridad de acuerdo con el objetivo de control.

[135] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >
[136] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

A. 15.1.5 Prevención en el mal uso de los recursos de tratamiento de la información

Control

"El personal debe ser disuadido de utilizar los recursos de tratamiento de la información para propósitos no autorizados." [137]

Control no aplica para el alcance del presente trabajo, sin embargo se deben establecer normas de seguridad de acuerdo con el objetivo de control.

A. 15.1.6 Regulación de los controles criptográficos

Control

"Los controles criptográficos deben ser utilizados en conformidad con todos los acuerdos, leyes y regulaciones." [138]

Control no aplica para el alcance del presente trabajo, sin embargo se deben establecer normas de seguridad de acuerdo con el objetivo de control.

[137] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >
[138] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

CUMPLIMIENTO DE LAS POLÍTICAS Y NORMAS DE SEGURIDAD Y CUMPLIMIENTO TÉCNICO.

A. 15.2.1 Conformidad con la política de seguridad y los estándares

Control

"Los gerentes deberían asegurarse que se cumplan correctamente todos los procedimientos de seguridad dentro de su área de responsabilidad cumpliendo las políticas y estándares de seguridad." [139]

Control no aplica para el alcance del presente trabajo, sin embargo se deben establecer normas de seguridad de acuerdo con el objetivo de control.

A. 15.2.2 Comprobación de la conformidad técnica

Control

"Se debería comprobar regularmente la conformidad con las normas de implantación de la seguridad en los sistemas de información." [140]

Control no aplica para el alcance del presente trabajo, sin embargo se deben establecer normas de seguridad de acuerdo con el objetivo de control.

[139] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >
[140] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

CONSIDERACIONES SOBRE LAS AUDITORÍAS DE LOS SISTEM. DE INFORMACIÓN.

A. 15.3.1 Controles de auditoría de sistemas

Control

"Se deberían planificar cuidadosamente y acordarse los requisitos y actividades de auditoría que impliquen comprobaciones en los sistemas operativos, para minimizar el riesgo de interrupción de los procesos de negocio." [141]

Control no aplica para el alcance del presente trabajo, sin embargo se deben establecer normas de seguridad de acuerdo con el objetivo de control.

A. 15.3.2 Protección de las herramientas de auditoría de sistemas

Control

"Se deberían proteger los accesos a las herramientas de auditoría de sistemas con el fin de prever cualquier posible mal uso o daño." [142]

Control no aplica para el alcance del presente trabajo, sin embargo se deben establecer normas de seguridad de acuerdo con el objetivo de control.

[141] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >
[142] ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002. Dirección URL: < http://iso27002.wiki.zoho.com >

CAPITULO 4

4. CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

Luego del estudio, análisis e implementación de la norma ISO 27002 para el departamento de Sistemas de la Universidad Politécnica Salesiana sede Guayaquil se pudo detectar muchas deficiencias en la parte de seguridad de la información. Como consecuencia, la información en todas sus formas y estados

Es importante recalcar que si se cumple al 100% con las políticas desarrolladas para la Universidad Politécnica Salesiana sede Guayaquil, no se garantiza que no tengan problemas de seguridad ya que no existe la seguridad al 100%; con el manual de políticas de seguridad de la información y con el cumplimiento de las mismas da lugar a minimizar los riesgos asociados a los activos reduciendo impactos, fuga de información y pérdidas económicas originados por la carencia de las normas y políticas de seguridad de la información.

Con el manual de políticas de seguridad de la información diseñado para la Universidad Politécnica Salesiana sede Guayaquil, proporcionara una guía a seguir para trabajar en los aspectos de seguridad.

El departamento de Sistemas de la Universidad Politécnica Salesiana sede Guayaquil, debe afrontar con las deficiencias de seguridad de la información, para lo cual debe tomar seriedad sobre lo documentado y realizar proyectos de enmendadura basados en las políticas de seguridad y por ultimo debe realizar campañas de concientización sobre los temas abordados.

4.2. Recomendaciones

- Se recomienda realizar las campañas concientización sobre la importancia de la seguridad de la información, esta campaña será dirigida al personal docente, administrativo y de servicio.

- Se debe realizar difusiones de las políticas de seguridad de la información a todo el personal de la Universidad Politécnica Salesiana.

- Se recomienda contar con controles de prohibiciones de los activos de información asignados a personal.

- Se recomienda contar con un documento formalmente aprobado por el Consejo superior en el cual conste las responsabilidades que tiene que cumplir el colaborador con respecto a los activos asignados a él.

- Se debe elaborar convenios sobre el buen uso de los activos y compromiso de responsabilidad de los activos de información.

- Este convenció debería ser firmado por todos los empleados de la Universidad Politécnica Salesiana al ingreso de la institución.

- Se recomienda que en la Universidad Politécnica Salesiana sede Guayaquil se tenga como política que se cambie la contraseña cada 30 días.

- Es necesario controlar la implementación de software en los sistemas operativos para minimizar el riesgo de corrupción de la información.

- Es importante que la información utilizada en las pruebas del sistema se acerquen a la realidad, pero al mismo tiempo se debe evitar el uso de la base de datos real de la Universidad Politécnica Salesiana.

- Se debe mantener un control estricto del acceso al código fuente de los programas, para así evitar copia, modificación o divulgación de los mismos.

- Se debe controlar estrictamente los cambios realizados en el software para minimizar la corrupción de los sistemas. Los programadores deberán tener acceso únicamente a la información que necesiten, todo cambio provendrá de un acuerdo y aprobación previa.

BIBLIOGRAFIA

- Information technology -- Security techniques -- Information security risk management, de http://www.iso.org/iso/search.htm?qt=iso+27002&sort=rel&type=simple&published=on
- ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002, de http://iso27002.wiki.zoho.com
- Tipos de estudios, de http://www.ophismkt.com/estudios.html
- El objetivo principal del uso de una política de seguridad, de http://www.pac.com.ve/index.php?option=com_content&view=article&id=8034: politicas -de-seguridad&catid=67:seguridad-y-proteccion&Itemid=90
- BEST PRACTICES FOR SECURITY - http://www.sisteseg.com/files/Microsoft_PowerPoint_-_ISO_17799.pdf
- Universidad de Oriente UNIVO, Manual de Normas y Políticas de Seguridad Informática
- Código de Practica para la administración de la Seguridad de la Información. IDAM, Instituto Argentino de Normalización (2002) - ISO/IEC 17799:2005
- National Information Systems Security (INFOSEC) Glossary, NSTISSI No. 4009, January 2000
- Irwin Valera Romero, Auditorias de Sistemas
- Segu-Info, Seguridad de la Información - www.cfbsoft.com.ar
- CERT, Software Engineering Institute - www.cert.org
- Guía Para la Elaboración de Políticas de Seguridad. Universidad Nacional de Colombia. 2003.
- El portal de ISO 27001 en Español - http://www.iso27000.es
- Universidad Politécnica Salesiana - http://www.ups.edu.ec

- ISO/IEC 27002:2005 Information technology — Security techniques — Code of practice for information security management - http://www.iso27001security.com/html/27002.html
- NORMAS TECNICAS SOBRE SISTEMAS DE GESTION DE LA SEGURIDAD DE LA INFROMACION, Instituto colombiano de normas técnicas y certificación INCONTEC, 2005
- Los pilares de la seguridad Informática - http://seguridaddeinformacion.bligoo.com/los-pilares-de-la-seguridad-informatica

ANEXOS

- Manual de Políticas de Seguridad de la Información de la Universidad Politécnica Salesiana sede Guayaquil. Anexo_1. El anexo 1 tiene carácter confidencial, por lo tanto este lo custodia el Departamento de Sistemas de la Universidad Politécnica Salesiana sede Guayaquil.

- Convenio de confidencialidad para personal interno y externo. Anexo_2.