ESCUELA POLITÉCNICA DEL EJÉRCITO
VICERRECTORADO DE INVESTIGACIÓN Y VINCULACIÓN CON LA COLECTIVIDAD

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

MAESTRÍA EN GERENCIA DE SISTEMAS

PLAN MAESTRO DE SEGURIDAD INFORMÁTICA PARA LA UTIC DE LA ESPE CON LINEAMIENTOS DE LA NORMA ISO/IEC 27002

Tesis de grado

Autores: Ing. Mauricio Javier Baldeón Garzón
Ing. Christian Alfredo Coronel Guerrero

Sangolquí, 2012

ESCUELA POLITÉCNICA DEL EJÉRCITO

MAESTRÍA EN GERENCIA DE SISTEMAS

CERTIFICO

Que el trabajo titulado “PLAN MAESTRO DE SEGURIDAD INFORMÁTICA PARA LA UTIC DE LA ESPE CON LINEAMIENTOS DE LA NORMA ISO/IEC 27002”, realizado por el Ing. Mauricio Javier Baldeón Garzón y el Ing. Christian Alfredo Coronel Guerrero, ha sido guiado y revisado periódicamente y cumple normas estatutarias establecidas por la ESPE, en el reglamento de estudiantes de la Escuela Politécnica del Ejército.

Sangolquí, 22 de octubre de 2012

_____

ING. FAUSTO GRANDA MsC.

DIRECTOR

ESCUELA POLITÉCNICA DEL EJÉRCITO

MAESTRÍA EN GERENCIA DE SISTEMAS

DECLARACIÓN DE RESPONSABILIDAD

Nosotros, **ING. MAURICIO JAVIER BALDEÓN GARZÓN** e **ING. CHRISTIAN ALFREDO CORONEL GUERRERO**

DECLARAMOS QUE:

El proyecto de grado denominado "PLAN MAESTRO DE SEGURIDAD INFORMÁTICA PARA LA UTIC DE LA ESPE CON LINEAMIENTOS DE LA NORMA ISO/IEC 27002", ha sido desarrollado con base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme las citas que constan en el pie de las páginas correspondientes, cuyas fuentes se incorporan en la bibliografía. Consecuentemente este trabajo es de nuestra autoría.

En virtud de esta declaración, nos responsabilizo del contenido, veracidad y alcance científico del proyecto de grado en mención.

Sangolquí, 22 de octubre de 2012

Ing. Mauricio Baldeón Garzón

Ing. Christian Coronel Guerrero

ESCUELA POLITÉCNICA DEL EJÉRCITO

MAESTRÍA EN GERENCIA DE SISTEMAS

AUTORIZACIÓN

Nosotros, **ING. MAURICIO JAVIER BALDEÓN GARZÓN** e **ING. CHRISTIAN ALFREDO CORONEL GUERRERO**

Autorizamos a la Escuela Politécnica del Ejército, la publicación, en la Biblioteca Virtual de la Institución del trabajo "PLAN MAESTRO DE SEGURIDAD INFORMÁTICA PARA LA UTIC DE LA ESPE CON LINEAMIENTOS DE LA NORMA ISO/IEC 27002", cuyo contenido, ideas y criterio son de nuestra exclusiva responsabilidad y autoría.

Sangolquí, 22 de octubre de 2012

Ing. Mauricio Baldeón Garzón	Ing. Christian Coronel Guerrero

AGRADECIMIENTO

A Dios, por darme la sabiduría y fortaleza para culminar este objetivo planteado.
A mi esposa, Johanna, por el incondicional apoyo y amor, fuente de energía en mi vida.
A mis padres y hermanos, por ser el orgullo que llevo día a día en mi corazón.
Al ingeniero y amigo, Fausto Granda, quien con su apoyo y conocimiento nos supo guiar durante todo el desarrollo de esta tesis, hasta hoy su culminación.
A todos los profesionales que laboran en la Unidad de Tecnologías de Información y Comunicaciones y que cada día ponen su mayor esfuerzo en beneficio de la institución.
A mi amigo de tesis, Ing. Christian Coronel, por todo el esfuerzo puesto en la culminación de esta tesis.

Ing. Mauricio Baldeón Garzón

Para mi esposa Adriana y mi hija Liz, por su amoroso apoyo y su formidable contribución durante todo el programa de mi maestría.

Ing. Christian Coronel Guerrero

DEDICATORIA

Primeramente, dedico este logro a Dios por darme el conocimiento y la fortaleza para culminar una etapa más de mi vida.

A mi esposa, amiga y compañera Johanna, por ser la persona que comparte mis ilusiones, mis alegrías, mis tristezas y mis triunfos, ahora juntos terminamos la maestría, TE AMO MI AMOR.

A mi madre, por ser la persona que me enseño toda la vida a terminar lo empezado, el carácter y la perseverancia para cumplir los objetivos que me proponga en la vida. A mi padre, por que una vez mas me dio un ejemplo de vida: “por mas complicada que sea la situación, siempre hay que levantarse y caminar”. Gracias a Dios por permitir que mis padres estén siempre junto a mí. LOS AMO.

A mis hermanos, espero ser una fuente inspiración y orgullo para ustedes. Siempre se puede alcanzar lo que uno se propone, no importa el tiempo ni lo complicado que sea.

Una dedicatoria especial a todas y cada una de las personas que contribuyeron de una u otra forma para que hoy alcance una meta más.

Ing. Mauricio Baldeón Garzón

A mis padres, a quienes admiro intensamente por su fortaleza y amor incondicional, quienes me han impulsado y permitido ser quien soy.

Ing. Christian Coronel Guerrero

ÍNDICE DEL CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE ANEXOS

Resumen

La Seguridad de la Información (S-I) es algo más que un antivirus, cortafuego o cifrado de datos, la S-I es el resultado de operaciones realizadas por personas y que son soportadas por la tecnología (Gonzalo Álvarez Marañon, Pedro Pablo Pérez García, 2004); bajo este contexto, la Escuela Politécnica del Ejército (ESPE) desde el año 2010 ha realizado adquisiciones considerables de equipamiento de seguridad perimetral y software de altas prestaciones, requiriéndose definir políticas, normas, procedimientos y controles que permitan gestionar correctamente los principios de la S-I (integridad, disponibilidad y confiabilidad).

El objetivo principal de esta investigación es presentar una propuesta formal para implementar políticas y controles de buenas prácticas que recomienda la Norma ISO/IEC 27002 enfocado a dos procesos de la UTIC: Base de Datos y Redes y Comunicaciones. Se pretende entregar una guía flexible, coherente e integral que permitirá minimizar o eliminar los ataques, vulnerabilidades, desastres naturales o disturbios sociales que destruyan la información, poniendo en peligro inminente a la Institución. Se propone un acercamiento a la metodología OCTAVE para gestionar el riesgo y a la norma de seguridad ISO/IEC 27002.

Se realizó un estudio real de las políticas, procesos, controles, planes y manuales existentes en la UTIC, para culminar con el Plan Maestro de Seguridad Informática con lineamientos de la norma ISO/IEC 27002. La utilización de estas políticas y controles permitirán ofrecer servicios de tecnología de calidad acorde a las exigencias Institucionales y tendencias Mundiales

Abstract

Information Security (I-S) is more than one antivirus, firewall and data encryption, the I-S is the result of operations carried out by people and that are supported by technology (Gonzalo Álvarez Marañón, Pedro Pablo Pérez García, 2004), in this context, the Army Polytechnic School (ESPE) since 2010 has made substantial purchases of perimeter security equipment and high-performance software, requiring define policies, standards, procedures and controls to manage properly the principles of SI (integrity, availability and reliability).

The main objective of this research is to present a formal proposal to implement policies and controls best practices recommended by the ISO/IEC 27002 to two processes UTIC: Database and Networking and Communications. It attempts to provide a flexible, consistent and comprehensive which will minimize or eliminate attacks, vulnerabilities, natural disasters or civil unrest destroy information, imminently endangering the institution. We propose an approach to the OCTAVE methodology for managing risk and safety standard ISO / IEC 27002.

Secondly, a real study of the policies, processes, controls, plans and manuals in UTIC, culminating in the Master Plan guidelines I-S with ISO/IEC 27002. The use of these policies and controls allow technology to offer quality services in line with Institutional requirements and Global trends.

“Decir imposible equivale a no intentarlo” ***Vladimir Lenin***

1. CAPÍTULO I – INTRODUCCIÓN

1.1. Generalidades

La seguridad informática es algo más que un cortafuego, un antivirus y el cifrado de datos. La seguridad informática es el resultado de operaciones realizadas por personas que son soportadas por la tecnología. (Gonzalo Álvarez Marañon, Pedro Pablo Pérez García, 2004)

El internet ha tenido un crecimiento muy relevante en el desarrollo de las actividades de los seres humanos, lamentablemente es una herramienta que ha crecido paralelamente con factores negativos tales como amenazas y vulnerabilidades que atentan contra la seguridad informática de las organizaciones, entre ellas la Escuela Politécnica del Ejército.

La finalidad del presente documento se enfoca en el uso de los controles de buenas prácticas que recomienda la Norma ISO/IEC 27000. Muchas de las actividades que se realizan de forma cotidiana en la ESPE[1] dependen en mayor o menor medida de las Tecnologías de la Información, esto se da porque obedecemos directamente a una sociedad moderna.

Es por eso que, un plan maestro de Seguridad Informática para una Universidad Clase "A"[2], como es la Escuela Politécnica del Ejército, será una guía flexible, coherente e integral que permitirá, que la ejecución de sus operaciones no se vean afectadas o comprometidas por ataques, vulnerabilidades, desastres naturales o disturbios sociales que destruyan la información, poniendo en peligro inminente a la institución.

[1] Escuela Politécnica del Ejército
[2] http://www.senescyt.gob.ec/c/document_library/get_file?uuid=5abcdec7-071b-4c34-a26f-7222773334ba&groupId=10156

1.2. Planteamiento del Problema

La falta de un Plan Maestro de Seguridad Informática en la UTIC[3] de la ESPE puede afectar negativamente el desarrollo de las actividades Académicas, Administrativas y de Vinculación con la Colectividad, pudiéndose detectar algunos problemas como:

- Duplicidad de trabajo, en la reparación y reconfiguración de equipos informáticos existentes en la ESPE.
- Incremento de gastos al utilizar inadecuadamente los recursos y aplicaciones informáticas.
- Robo de información confidencial y su revelación a terceros.
- Filtración de datos personales de usuarios registrados en los sistemas, diseños de proyectos, estrategias competitivas, programas académicos y financieros.
- Pérdida de la imagen corporativa y de la reputación ante otras universidades y organizaciones públicas o privadas, además la reducción de la confianza de clientes y proveedores
- Retrasos en los procesos académicos, financieros, estratégicos, investigativos, entre otros, maximizando el impacto en la calidad del servicio.
- Afrontar demandas legales y civiles que finalizan en el pago de indemnizaciones por daños y perjuicios a terceros. (Vieites, 2007)

1.2.1. Descripción del Problema

La Escuela Politécnica del Ejército (ESPE) es una institución de educación superior, con domicilio en la ciudad de Quito y sede principal en la ciudad de Sangolquí, actualmente se encuentra reconocida por el Sistema Nacional de

[3] UTIC: Unidad de Tecnologías de la Información

Educación Superior. (ESPE). Cuenta con un total de 25000 estudiantes, distribuidos en modalidad presencial y distancia.

Dentro de sus procesos cuenta con la Gestión de Tecnologías de la Información y Comunicaciones (UTIC), la misma que tiene como objetivo asegurar la disponibilidad, actualización tecnológica, innovación y operación de los recursos y servicios de TIC´s, para alcanzar un alto nivel de Tecnología y estándares de calidad acorde con las exigencias institucionales (SGC). La gestión de UTIC, se divide en 5 ítems:

a) Gestión Estratégica de Tecnologías de Información y Comunicaciones
b) Gestión de Soporte Técnico
c) Administración de Servicios de Redes y Comunicaciones
d) Desarrollo, Implantación y Mantenimiento de Aplicativos
e) Administración de Aplicativos y Base de Datos

Bajo este contexto, la UTIC ha sido gestor de proyectos estratégicos ambiciosos que han logrado alcanzar una adecuada infraestructura tecnológica, la cual permite que el interés institucional y de la comunidad politécnica estén a la vanguardia del país.

A la presente, no se dispone de un cuerpo debidamente estructurado de normas reguladoras, procedimientos, reglas y buenas prácticas que garanticen plenamente la disponibilidad, integridad y confiabilidad de la Información. Se dispone de información dispersa referente a seguridad informática entre las diferentes unidades, en un esfuerzo por minimizar el impacto tecnológico ante la falta de una política institucional.

1.3. Justificación e Importancia

La presente investigación se la realiza con la finalidad de presentar una propuesta formal de seguridad de información para la ESPE, que permita ofrecer servicios informáticos de calidad a sus clientes. La seguridad de la información es más que la administración o implementación de un determinado equipo o sistema de seguridad. Durante el año 2011, la institución realizó una adquisición considerable de equipamiento de seguridad perimetral, sin embargo por las múltiples actividades que mantienen los especialistas de TI no se han definido políticas, normas y procedimientos para gestionar correctamente la seguridad de la información. La falta de políticas en materia de seguridad informática, ha sido principalmente la causa de:

a) Duplicidad de trabajo, debido a la reparación y reconfiguración de equipos y/o sistemas informáticos.
b) Sub utilización del recurso humano, “apagando incendios” por pérdida o inestabilidad de informaciones o configuraciones de las diferentes aplicaciones.
c) Baja disponibilidad de los servicios, causada por errores de hardware o software. No se ha puesto en práctica una estrategia de copias de seguridad.
d) Afectación a la privacidad, ya que los equipos informáticos se encuentran compartiendo los recursos de red y no se mantiene una cultura de administración de contraseñas.
e) Instalación compulsiva de aplicaciones que están disponibles en el Internet, a modo de prueba. Como consecuencia, el rendimiento de los equipos informáticos se ve negativamente afectado.

De esta forma, se justifica el diseño de un plan maestro de seguridad de la información con lineamientos en la Norma Internacional ISO/IEC 27002 para la UTIC, de tal manera que se mantenga alineado a las tendencias globales relacionadas a la tecnología de la información, digno de una Universidad clasificada en la categoría “A”.

1.4. Objetivo general

Diseñar un plan maestro de seguridad informática para la Unidad de Tecnologías de la Información y Comunicación de la ESPE, considerando como referencia el estándar ISO/IEC 27002, a fin de impulsar una política institucional referente a esta temática.

1.5. Objetivos específicos

a) Documentar el estado del arte de seguridad informática relacionado con la norma ISO/IEC 27002.
b) Describir el estado de la situación actual de seguridad informática de la UTIC utilizando herramientas como Matriz de Riesgos e investigación de campo.
c) Elaborar una propuesta de seguridad informática en base a la cadena de valor de los servicios que ofrece la UTIC referenciando la norma ISO/IEC 27002.

1.6. Alcance

Esta investigación cubre las necesidades que tiene la UTIC sobre la elaboración de políticas de seguridad sobre 2 de sus subprocesos internos. De acuerdo a la criticidad, se realizará el estudio sobre:

a) Administración de Aplicativos y Base de Datos
b) Administración de Servicios de Redes y Comunicaciones

El diagnóstico, evaluación y el diseño de recomendaciones comprende los siguientes aspectos:

a) Políticas de seguridad
b) Seguridad ligada a los recursos humanos
c) Control de acceso
d) Gestión de comunicaciones y operaciones
e) Gestión de la continuidad del negocio

Los resultados de esta tesis, servirán para que los usuarios de los servicios de red y de los sistemas de información de la ESPE, se encuentren en la capacidad de aplicar esta norma internacional de seguridad de una manera confiable, segura y oportuna.

“Las organizaciones gastan millones en firewalls y dispositivos de seguridad, pero tiran el dinero, porque ninguna de estas medidas cubre el eslabón más débil de la cadena de seguridad: la gente que usa y administra los ordenadores.” ***Kevin Mitnick***

2. CAPÍTULO II – FUNDAMENTO TEÓRICO

2.1. Definición de seguridad información

La seguridad informática concierne a la protección de la información que se encuentra en una computadora o en una red de ellas y también a la protección del acceso a todos los recursos del sistema. (CYBSEC S.A., 2011)

La seguridad de la información es enmarcada por 3 principios fundamentales, que son un conjunto de políticas y mecanismos que permiten garantizar los recursos de los sistemas, estos se muestran a continuación:

Figura 1: Principios de la Seguridad de la Información

Integridad.- Es el principio que busca mantener los datos libres de modificaciones no autorizadas.

Confidencialidad.- Es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados.

Disponibilidad.- La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. A groso modo, la disponibilidad es el

acceso a la información y a los sistemas por personas autorizadas en el momento que lo requieran.

a. Misión de la seguridad de la información

La misión de Seguridad de la Información es garantizar la protección de sus activos y su información sensible y crítica, que la integran e interactúan para ofrecer servicios que permiten la Gestión del Negocio y las operaciones de una manera oportuna, confiable y segura, y que redunda en Calidad para sus clientes, proveedores y empleados.

b. Realidad de la seguridad de la información

Actualmente, los problemas experimentados por motivos de seguridad van desde ataques externos, hasta incidencias en el interior de la propia organización, como aquellas provocadas por empleados que borran archivos críticos o acceden a información confidencial.

En ese contexto, la seguridad información resulta vital en las organizaciones, mientras que la materialización de los riesgos y vulnerabilidades pueden significar millonarias pérdidas y comprometer su continuidad.

Aparentemente, la gente no reacciona ante los problemas de seguridad informática, vulnerabilidades básicas siguen apareciendo en los programas, los administradores todavía no realizan actualizaciones de los sistemas y no los aplican parches, y los usuarios siguen accediendo sobre los archivos adjuntos enviados por correo electrónico.

Las empresas no pueden solucionar los problemas de seguridad porque si lo hacen, las aplicaciones críticas que están en producción entran en crisis y los

proveedores siguen tratando de explicar que requieren permisos habilitados para todo el mundo, utilizar usuarios contraseñas, no es tan inseguro.

A través del sitio web: www.zone-h.org se realiza una investigación estadística que muestra un total de 308 de ataques exitoso realizados páginas web de instituciones académicas desde el 2002. Como objeto de este estudio, en la siguiente figura se visualiza que la ESPE ha sido atacada el 15 de Abril del presente año:

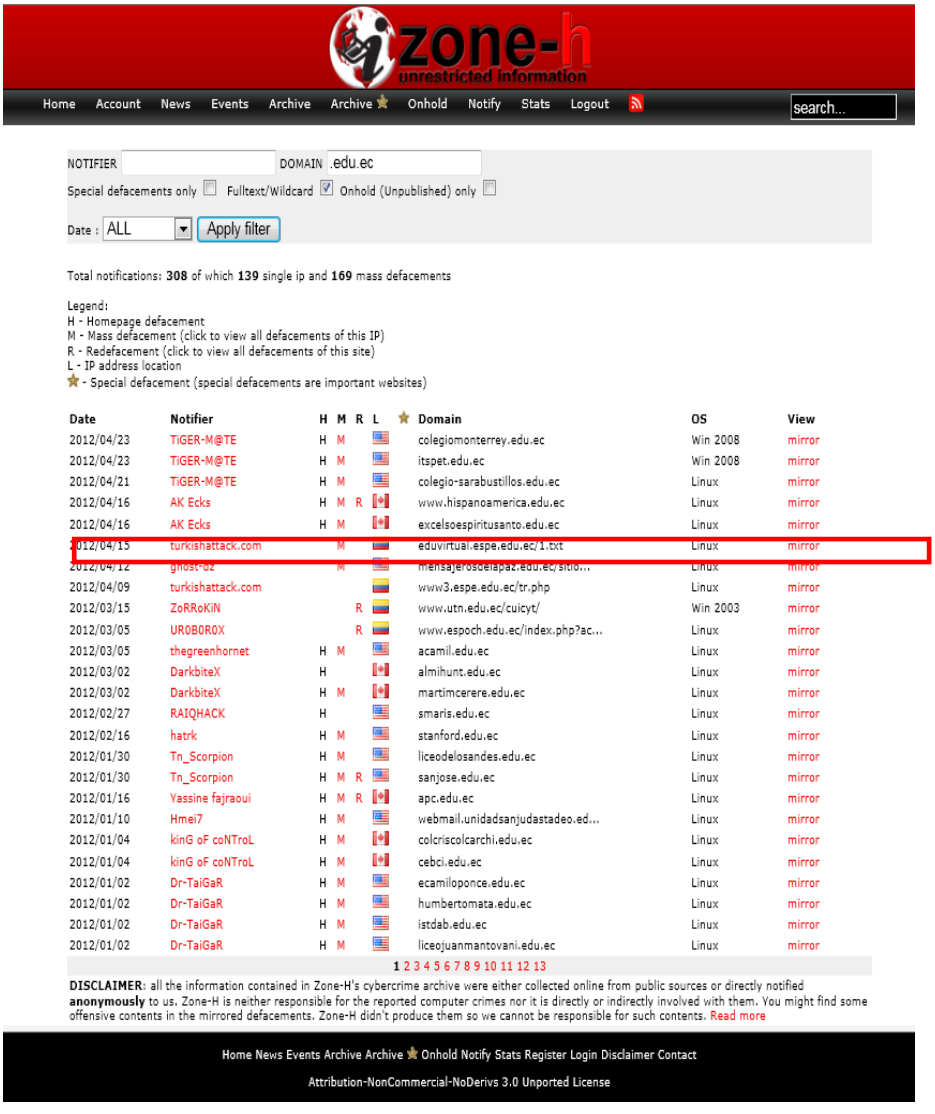


Figura 2: Paginas Educativas del Ecuador Atacadas (www.zone-h.org)

c. ¿QUÉ ES UN HACKER?

Es una persona que disfruta: explorar los detalles internos de los sistemas informáticos y cómo extender sus capacidades más allá de lo normal, la programación de sistemas y es entusiasta en una determinada área. Es considerada una persona no malintencionada.

d. ¿QUÉ ES UN INTRUSO?

Simplemente es una persona que accede en forma no autorizada a un determinado Sistema Informático con intenciones de provocar daño.

Las organizaciones, ¿De quiénes se protegen?:

- Intrusos Informáticos
- Extorsionadores
- Espías Industriales
- Usuarios del sistema
- Ex empleados
- Cien millones de adolescentes.

Las organizaciones, ¿De qué se protegen?:

- Robo de información confidencial
- Fraude Informático
- Daño a la imagen
- Modificación de archivos
- Indisponibilidad de servicios críticos
- Destrucción del Sistema Informático

- Sabotaje Corporativo

e. NIVELES DE CONOCIMIENTOS DE LOS INTRUSOS

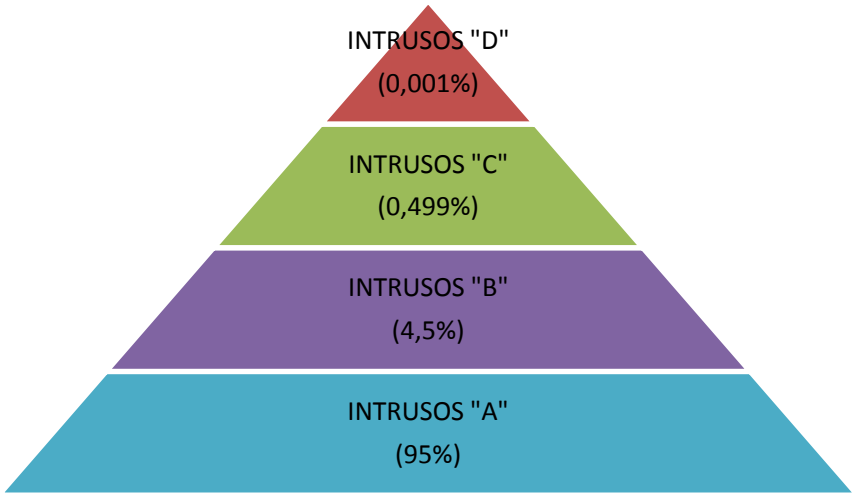


Figura 3: Niveles de conocimiento de los intrusos

Siendo así; para las organizaciones, los intrusos “A” son los intrusos más peligrosos, debido a que este segmento es al más numeroso y se encuentran personas que por “hobby” buscan la manera de acceder a información no autorizada, no necesariamente con el objetivo de causar daño. En este grupo se considera que se encuentran los adolescentes y estudiantes.

2.2. Definición del riesgo

Para COSO (Comitee of Sponsoring Organizations of the Treadway Commission), riesgo es un “Factor identificado que podría afectar a la consecución de un objetivo, como:

- Efectividad de las operaciones
- Confiabilidad de la información
- Cumplimiento de leyes y regulaciones

De la misma manera COSO, define al riesgo como: “La posibilidad de que un evento ocurrirá y afecte adversamente el cumplimiento de los objetivos”[4].

Para la norma ISO/IEC TR 13335-1, define: “Riesgo es el potencial de que una amenaza dada explote las vulnerabilidades causando pérdida o daño a un activo o grupos de activos, y en consecuencia de esto directa o indirectamente a la organización”[5].

Riesgo también puede considerarse como “la posibilidad de sufrir daño o pérdida; el potencial para comprender las consecuencias negativas de un evento. El Riesgo refiere a una situación en la cual tanto una persona puede hacer al indeseable o una ocurrencia natural puede causar un resultado indeseado, teniendo un impacto negativo o consecuencia”[6].

a. Componentes del riesgo

1. Procesos y/o activos

Son todos y cada uno de los componentes sobre los cuales se gestiona el normal funcionamiento de una empresa o institución. Se incluyen en estos todos los activos, tantos físicos como de información. Estos componen elementos como los siguientes:

- Activos Físicos (Fijos): Edificio, planta, infraestructura, maquinarias, equipos de oficina, entre otros.

[4] COSO: Enterprise Risk Managment Framework. Apéndice E, página 4
[5] ISO/IEC TR 13335-1: Information technology – Guidelines for the managment of TI Security – Part 1: Concepts and models for LT Security, página 13.
[6] Alberts C., Dorofee A.: Managing Information Security Risks: The OCTAVE Approach. Glosario de Términos.

- Activos de Información: Bases de Datos, aplicaciones, sistemas de gestión, sistemas de monitoreo en línea, archivos de datos, entre otros.

b. Riesgos en tecnología de información

Los riesgos dentro de las TI están ligados a la exposición de los activos que conforman la unidad de TIC en la ESPE, a una actividad que represente una amenaza para los mismos. Dentro de este ambiente se podría catalogar las siguientes categorías de riesgos para TI:

- Riesgos asociados a catástrofes

Son aquellos eventos asociados a fuerzas naturales de destrucción, por ejemplo terremotos, maremotos, inundaciones.

- Riesgos por variaciones y pérdida del flujo eléctrico

Son aquellos ligados al suministro eléctrico del que la institución dispone a través de un servicio público o privado.

- Riesgos de mal uso o mala configuración de equipos

Son aquellos que tienen que ver con una errónea manipulación o uso de los equipos que forman parte de los activos de información, por ejemplo una configuración descuidada de un equipo, borrado de registros de una base de datos por un mal uso de aplicaciones, entre otras.

- Riesgos de pérdida de la información

Son aquellos asociados al desvanecimiento de la información almacenada en medios magnéticos, debido a daños de las fuentes de almacenamiento o incursión deliberada de procesos que generen actividades de supresión de registros y/o archivos de datos.

- Riesgos de caídas de sistemas

Son aquellos que involucran pérdidas tanto de datos como económicas por el deceso o fallo del o los sistemas de información que soporten actividades o procesos considerados como críticos o importantes para la organización. Por ejemplo la caída de un sistema bancario de transacciones en línea podría representar pérdidas tanto de datos como económicas para la institución.

- Riesgos por vandalismos

Son aquellos que están ligados a la destrucción física y/o lógica de la integridad de los equipos, de los cuales depende el funcionamiento de las aplicaciones/servicios que ofrece la unidad informática de la institución

- Riesgos por pérdidas de equipos o partes

Estos están vinculados al hurto o pérdida involuntaria de equipos o partes de los mismos, como consecuencia de delitos o accidentes, respectivamente.

- Riesgos de pérdida e confidencialidad de la información

Esta clase de riesgos están netamente vinculados al robo de la información de la institución para su posterior divulgación a terceras pares que no deberían

obtener tales datos. En esta parte tiene que ver mucho el robo o filtración de información tanto por agentes internos a la organización, así como por agentes externos a la misma.

- Riesgos de Autenticación

Están vinculados a la violación del sistema de autenticación que tiene una organización para dar acceso a usuarios autorizados a cierta información o roles administrativos inherentes al cargo que este individuo ocupa en la institución. Adicionalmente, están relacionados con la posibilidad de un robo de la identidad electrónica de un usuario de un sistema, de modo que se logre un acceso autorizado dentro del medio a una persona que simula ser un ente permitido para alcanzar datos al hurtar la identidad de un usuarios permitido.

- Riesgos de violación de la integridad

Estos riesgos están vinculados a la posibilidad de alteración de los datos de un archivo o una base de datos, modificándolos voluntaria o involuntariamente por un sujeto o una situación inesperada, de modo que añada, supriman o actualice información de manera deliberada o accidental dentro de las fuentes que contienen dichas referencias, poniendo en peligro la confiabilidad de la información almacenada.

Este tipo de riesgos son típicos de las bases de datos y archivos que contienen información sensible y modificable.

- Riesgos económicos

Es la posibilidad de que una institución o empresa sufra pérdidas económicas asociadas a cualquier evento nocivo para el logro de sus objetivos.

Estas pérdidas pueden ser tanto materiales, económicas y/o humanas, expresadas en cantidades de dinero que representan una merma para la organización.

- Riesgos de pérdida de prestigio

Están asociados netamente a la pérdida de la confiabilidad, prestigio o veracidad de una institución. Esta clase de riesgos podría representar un altísimo impacto económico en instituciones que basen sus operaciones en la confiabilidad de sus productos/servicios, por ejemplo instituciones del sector financiero, organizaciones comerciales, servicios gubernamentales, entre otros. (Pazmiño, 2007)

2.3. Análisis de riesgos

La Administración del Riesgo es utilizado para minimizar el riesgo aplicando efectivamente medidas de seguridad según las:

- Amenazas
- Vulnerabilidades y,
- El valor de los activos a ser protegidos

El análisis de riesgo es el método para:

- Identificar los riesgos
- Evaluar el posible daño que estos pueden causar a una organización
- Justificar las medidas de seguridad que deben implementarse en la misma

a. Objetivo del análisis del riesgo

El objetivo principal del análisis de riesgo es:

- Cuantificar el impacto de las amenazas potenciales.
- Asignar un precio o valor del costo de la pérdidas de un negocio por la manifestación de un riesgo:
- Incluye la identificación de los riesgos y
- El costo/beneficio que justifica la seguridad y control, lo cual es de vital importancia en la creación de una arquitectura de seguridad que mitiga los riesgos de un negocio.

b. Características del análisis de riesgo

- Permite considerar el costo de los sistemas automatizados y controles; respecto al impacto de la pérdida o modificación de los recursos e información de manera inadecuada, asociándolo a su vez al impacto en la organización.
- Permite establecer un método por el cual las vulnerabilidades individuales se comparan para identificar escenarios actuales de amenazas de la seguridad y determinar la probabilidad en la que compromete la información protegida.
- Permite definir e implementar requerimientos de seguridad.
- Evaluación de las amenazas y vulnerabilidades conocidas y postuladas, con la finalidad de determinar la pérdida esperada y establecer el grado de aceptabilidad para la operación de sistemas.

Bajo este contexto, el análisis de riesgo es entonces una herramienta que permite ayudar a los directivos de negocio a obtener un entendimiento de los riesgos y las vulnerabilidades asociadas a la información y la tecnología que la

habilita, y a partir de ello establecer una arquitectura que reduzca el nivel de riesgo a grados de impacto que la organización pueda soportar. Sin embargo actualmente los gerentes de negocio siguen inhabilitados a usar el análisis de riesgo; ya que las técnicas disponibles son difíciles de entender, producen resultados que son inciertos y requieren de personal altamente capacitado y con experiencia que es difícil de encontrar.

2.4. Gestión de riesgos

¿Cómo se maneja o administra un riesgo?

Para gestionar un riesgo, se puede tomar varias alternativas:

- Aceptarlo
- Transferirlo
- Mitigarlo (Implementar políticas de seguridad)
- Evitarlo (Eventualmente)

Las alternativas serán determinadas por la relación COSTO/RIESGO. El proceso total de la gestión de riesgo, se muestra en la siguiente figura.

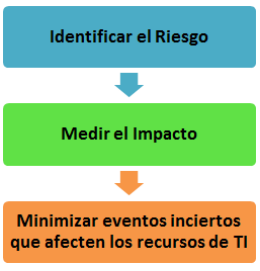


Figura 4: Proceso de Gestión de Riesgos

Este proceso incluye:

- El análisis de riesgo
- El análisis de costo beneficio

- La selección de protecciones
- El desarrollo de la estrategia de seguridad
- La prueba de la seguridad y su evaluación
- La implementación de las protecciones
- La revisión del sistema

2.5. Metodología para el análisis de riesgos

El método OCTAVE fue desarrollado bajo un enfoque para el análisis de riesgos en las grandes empresas (mas de 300 empleados), sin embargo el tamaño no fue la única consideración. Por ejemplo, las grandes organizaciones suelen tener una estructura organizacional jerárquica de varios niveles y es probable que mantengan su propia infraestructura tecnológica para ejecutar las herramientas evaluación de la vulnerabilidad e interpretar los resultados en relación con los activos críticos.

Es una metodología para la búsqueda de seguridad informática, basada en el análisis estratégico del riesgo y la planeación de una técnica para su implementación. OCTAVE está integrado en un compendio de criterios que definen los elementos esenciales para la evaluación de riesgos en la seguridad informática.

El Método OCTAVE utiliza un enfoque de tres fases para examinar aspectos organizacionales y de tecnología. Se compone de una serie de talleres que lo llevan a su ejecución un equipo de análisis interdisciplinario de tres a cinco personas que trabajen en la organización. El método aprovecha el conocimiento de múltiples niveles de la organización, centrándose en:

- Identificar los elementos críticos y las amenazas a los activos
- Identificar vulnerabilidades, tanto organizativas como tecnológicas.

- Desarrollar una estrategia de protección basada en la práctica y los planes de mitigación de riesgo para apoyar la misión de la organización y las prioridades.

Estas actividades son apoyadas por un catálogo de buenas prácticas o conocidas, así como en encuestas y hojas de trabajo que pueden ser utilizados para obtener y captar la información durante los debates y entrevistas con el personal experto de la organización. (CERT, 2008)

Entre los aspectos importantes de OCTAVE se destaca lo siguiente:

- Asegura la continuidad de la operación de la Institución
- Identifica y define los riesgos
- Establece estrategias para mitigar el riesgo
- Se enfoca en la conservación de la información no de los activos
- Toma en cuenta todos los departamentos o secciones de la empresa

a. Objetivo de OCTAVE

OCTAVE, busca que las organizaciones se encuentre en la capacidad de:

- Tomar las decisiones adecuadas, basadas en el análisis de sus riesgos
- Evaluar y Controlar los riesgos en la seguridad de la información, por si mismos.
- Enfocarse en el aseguramiento de sus activos tecnológicos principales
- Manipular y preservar información clasificada. (Palma, 2011)

b. Guía de implementación de OCTAVE

La Guía de Implementación del Método OCTAVE ofrece todo lo que un equipo de análisis tiene que utilizar a fin de llevar a cabo una evaluación en su organización. Incluye un conjunto completo de procesos detallados, hojas de cálculo y las instrucciones para su implementación “paso a paso”, así como material de apoyo y orientación para la adaptación.

2.6. Descripción de las fases de implementación de OCTAVE

a. Fase Startup

- Obtener apoyo de los altos mandos en todas las áreas para los trabajos del grupo de análisis y evaluación
- Seleccionar el equipo de trabajo
  - ✓ Líderes
  - ✓ Habilitantes
- Determinar los alcances del análisis
- Determinar el equipo de apoyo. (Palma, 2011)

b. Fase 1

Determinar cuales son los activos informáticos críticos para la operación de la empresa e identificar que se hace actualmente para protegerlos.

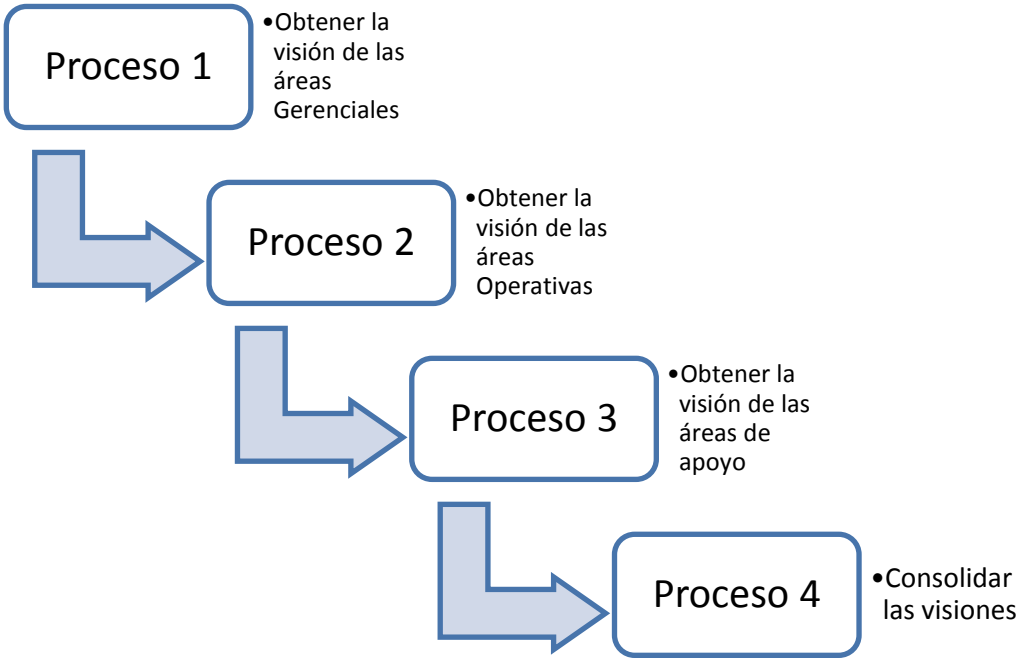


Figura 5: OCTAVE - Fase 1

c. Fase 2

- Identificar las vulnerabilidades de la infraestructura informática

  - ✓ Red
  - ✓ Arquitectura
  - ✓ Sistema Operativo
  - ✓ Aplicaciones

- Identificar vías de acceso no autorizado a elementos críticos

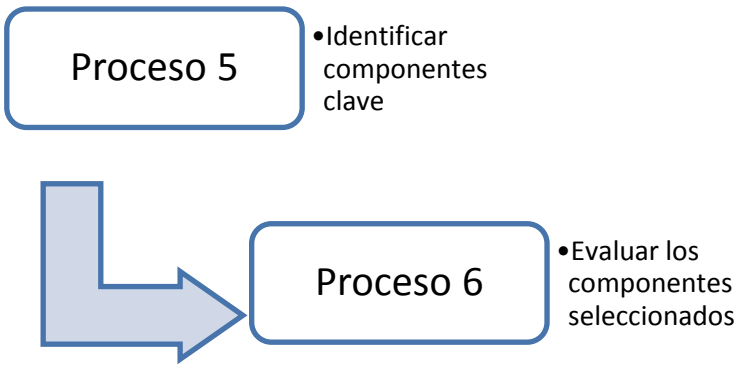


Figura 6: OCTAVE - Fase 2

d. <u>Fase 3</u>

- Desarrollar planes y estrategias de seguridad

  ✓ Analizar riesgos específicos
  ✓ Pruebas

- Decidir acciones e implementaciones de protección
- Decidir acciones e implementaciones de contingencia (Palma, 2011)

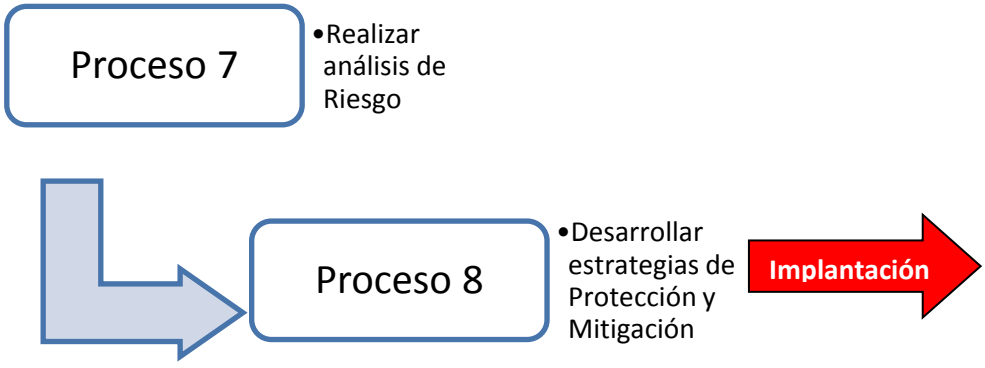


Figura 7: OCTAVE - Fase 3

2.7. Serie ISO/IEC 27000

Muchas organizaciones no han podido definir o no han podido implementar de forma eficaz adecuadas políticas y procedimientos de Seguridad Informática de acuerdo con sus necesidades de seguridad de la información. La Seguridad Informática, establece controles de operación a todos los sistemas de información desde todas sus operaciones y procesos, tratando únicamente de prevenir, minimizar el riesgo de problemas informáticos y atacar las vulnerabilidades existentes en los sistemas informáticos, teniendo como principios fundamentales la integridad, la disponibilidad y la confidencialidad de la información. Por tanto, para una adecuada gestión de la seguridad de la información en la ESPE, es necesario implementar un sistema que aborde estas tareas de una forma metódica, documentada y basada en objetivos claros de seguridad a los que está sometida la información de la Institución.

ISO/IEC 27000 es un conjunto de estándares desarrollados por ISO[7] e IEC[8] que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización o institución.

- ISO (International Organization for Standardization) - Organización Internacional para la Estandarización, es un organismo que promueve el desarrollo de normas voluntarias internacionales de fabricación, comercio y comunicación para todas las ramas industriales menos las del campo de la eléctrica y la electrónica. Su sede principal se encuentra en la ciudad de Ginebra-Suiza y su objetivo principal es la de estandarizar normas, productos y seguridad para organizaciones y empresas de todo el mundo.

[7] http://www.iso.org/iso/home.html
[8] http://www.iec.ch

- IEC (International Electrotechnical Commission) - Comisión Electrónica Internacional, es una organización que se encarga de la normalización en el campo eléctrico, electrónico y en todas las tecnologías que se encuentren relacionadas. Desde el año 1.906 IEC es la organización líder a nivel mundial que prepara y publica normas internacionales para todas las tecnologías eléctricas, electrónicas y relacionadas con el fin de trabajar con seguridad en todos los niveles. Ecuador es un país afiliado a IEC mediante el Instituto Ecuatoriano de normalización (INEN).

- Estándar: Es un modelo o conjunto de reglas, normas, técnicas y procedimientos documentados que se siguen con la finalidad de cumplir un objetivo de superación.

- Norma: Es un documento de aplicación voluntaria que contiene especificaciones técnicas específicas basadas en los resultados de la experiencia y del desarrollo tecnológico. Las normas son consecuencia del consenso entre todas las partes involucradas e interesadas en la actividad objeto de la misma. Además, deben aprobarse por un Organismo de Normalización internacional. Tanto los estándares como las normas garantizan niveles de calidad y seguridad que permiten a cualquier empresa posicionarse de mejor manera en el mercado.

La serie ISO/IEC 27000 contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI).[9].

[9] http://www.iso.org/iso/store.htm

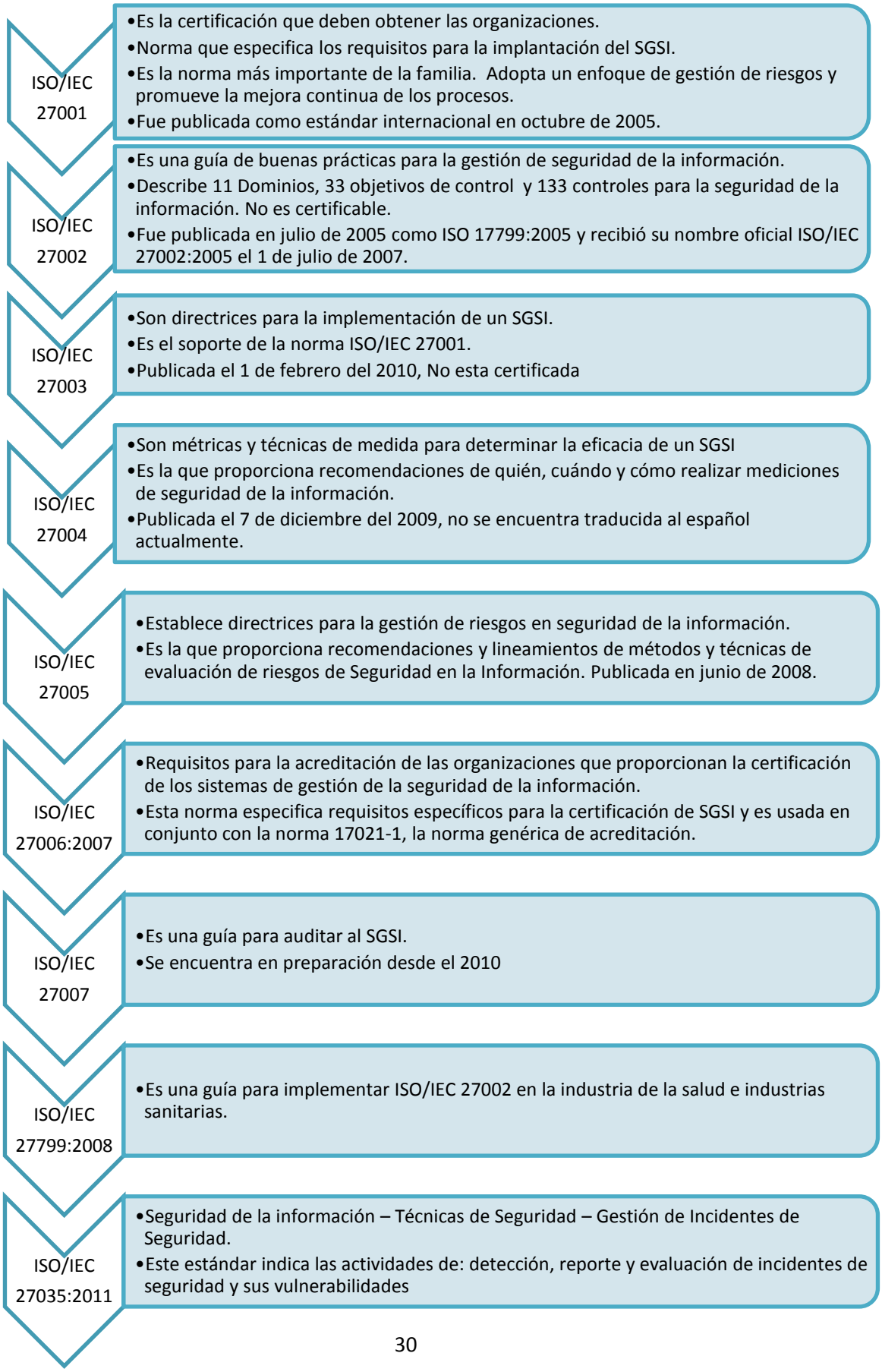


Figura 8: Resumen de la Serie ISO 27000

2.8. Estándar ISO/IEC 27002

ISO/IEC 17799 (llamada también ISO 27002) es un estándar para la seguridad de la información publicado por primera vez como ISO/IEC 17799:2000 en el año 2000, con el título de Information technology - Security techniques - Code of practice for information security management. Tras un periodo de revisión y actualización de los contenidos del estándar, se publicó en el año 2005 el documento actualizado denominado ISO/IEC 17799:2005.

Desde el 1 de Julio de 2007, adoptó el nombre de 27002:2005, siendo; 2005 el año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Desde 2006, está traducida en Colombia (como ISO 17799) y desde 2007 en Perú (como ISO 17799 descarga gratuita). El original esta en inglés y su traducción al francés o al español pueden adquirirse en ISO.org a un costo aproximado de $200.

2.9. Propósito de la ISO/IEC 27002

Proporcionar recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener un SGSI. La seguridad de la información se define en el estándar como la preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de procesamiento sean exactos y completos) y la disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran).

La versión del 2005 del estándar incluye las siguientes once secciones principales:

1) Política de Seguridad de la Información.
2) Organización de la Seguridad de la Información.
3) Gestión de Activos de Información.
4) Seguridad de los Recursos Humanos.
5) Seguridad Física y Ambiental.
6) Gestión de las Comunicaciones y Operaciones.
7) Control de Accesos.
8) Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.
9) Gestión de Incidentes en la Seguridad de la Información.
10) Gestión de Continuidad del Negocio.
11) Cumplimiento.

Dentro de cada sección, se especifican los objetivos de los distintos controles para la seguridad de la información y para cada uno de los controles se indica asimismo una guía para su implantación. El número total de controles son 133 y cada organización debe considerar previamente cuántos serán realmente los aplicables según sus propias necesidades.

2.10. ¿Cómo implementar la norma ISO/IEC 27002?

Para realizar una implementación exitosa de cualquier estándar internacional es preferible contar con la ayuda de una consultora externa que conozca a profundidad la norma y que supervise todos los pasos para que la certificación se obtenga sin problemas, en los plazos y términos establecidos. Solo de esta manera se podrán alcanzar los máximos parámetros de seguridad en los sistemas. Sin embargo, en un contexto general, para poder implementar el estándar el proceso resumido puede ser el siguiente:

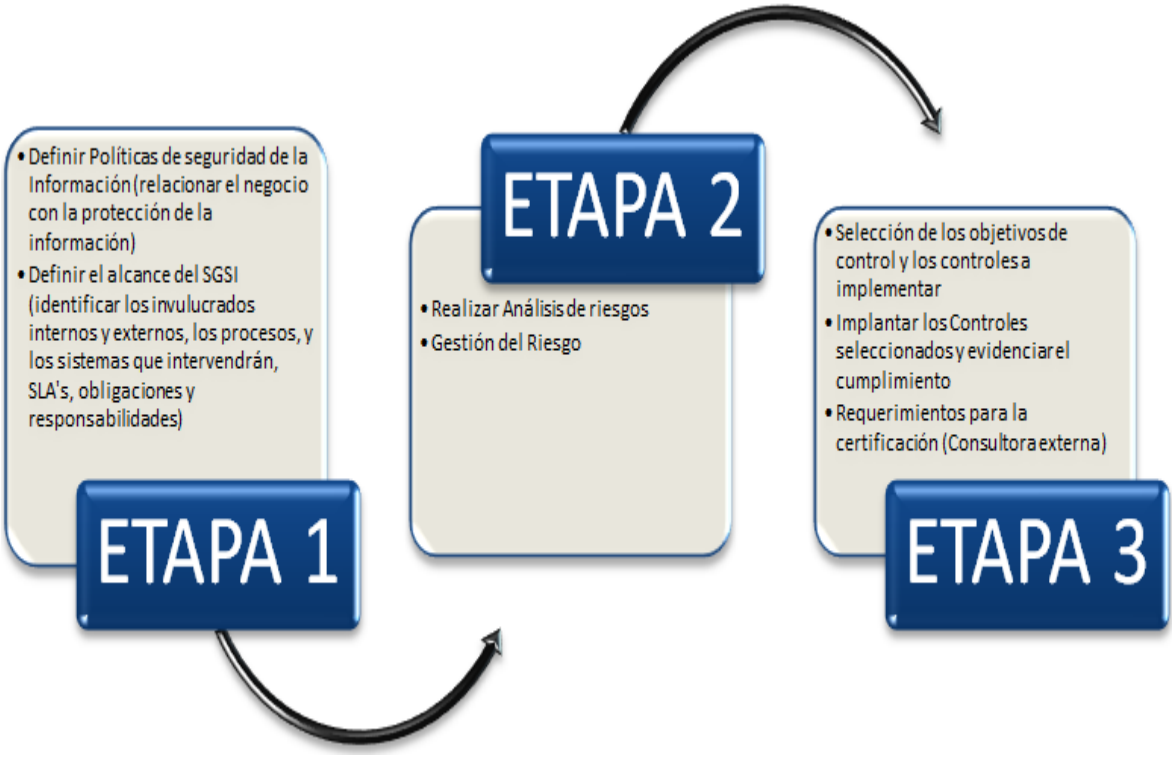


Figura 9: Resumen de Implementación de ISO 27001

2.11. Resumen de la norma ISO/IEC 27002 (Dominios, Objetivos de Control Y Controles)

ISO/IEC 27002:2005 Dominios (11) - Objetivos de Control (39) - Controles (133)

1. POLÍTICA DE SEGURIDAD
   - 1.1. Política de seguridad de la información: (1)
     - 1.1.1. Documento de política de seguridad de la información. (1)
     - 1.1.2. Revisión de la política de seguridad de la información. (2)
2. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN
   - 2.1. Organización Interna: (2)
     - 2.1.1. Compromiso de la Dirección con la seguridad de la información. (3)
     - 2.1.2. Coordinación de la seguridad de la información. (4)
     - 2.1.3. Asignación de responsabilidades relativas a la seguridad de la información. (5)
     - 2.1.4. Proceso de autorización de recursos para el tratamiento de la información. (6)
     - 2.1.5. Contacto con las autoridades. (7)
     - 2.1.6. Contacto con grupos de especial interés. (8)
     - 2.1.7. Revisión independiente de la seguridad de la información. (9)
   - 2.2. Terceros: (3)
     - 2.2.1. Identificación de los riesgos derivados del acceso de terceros. (10)
     - 2.2.2. Tratamiento de la seguridad en la relación con los clientes. (11)
     - 2.2.3. Tratamiento de la seguridad en contacto con terceros. (12)
3. GESTIÓN DE ACTIVOS
   - 3.1. Responsabilidad sobre los activos: (4)
     - 3.1.1. Inventario de activos. (13)
     - 3.1.2. Propiedad de los activos. (14)
     - 3.1.3. Uso aceptable de los activos. (15)
   - 3.2. Clasificación de la información: (5)
     - 3.2.1. Directrices de clasificación. (17)
     - 3.2.2. Etiquetado y manipulado de la información. (18)
4. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS
   - 4.1. Antes del empleo: (6)
     - 4.1.1. Funciones y responsabilidades. (19)
     - 4.1.2. Investigación de antecedentes. (20)
     - 4.1.3. Términos y condiciones de contratación. (21)
   - 4.2. Durante el empleo: (7)
     - 4.2.1. Responsabilidades de la Dirección. (22)
     - 4.2.2. Concienciación, formación y capacitación en seguridad de la información. (23)
     - 4.2.3. Proceso disciplinario. (24)
   - 4.3. Cese del empleo o cambio de puesto de trabajo: (8)
     - 4.3.1. Responsabilidad del cese o cambio. (25)
     - 4.3.2. Devolución de activos. (26)
     - 4.3.3. Retirada de los derechos de acceso. (27)
5. SEGURIDAD FÍSICA Y DEL ENTORNO:
   - 5.1. Áreas seguras: (9)
     - 5.1.1. Perímetro de seguridad física. (28)
     - 5.1.2. Controles físicos de entrada. (29)
     - 5.1.3. Seguridad de oficinas, despachos e instalaciones. (30)
     - 5.1.4. Protección contra las amenazas externas y de origen ambiental. (31)
     - 5.1.5. Trabajo en áreas seguras. (32)
     - 5.1.6. Áreas de acceso público y de carga y descarga. (33)
   - 5.2. Seguridad de los equipos: (10)
     - 5.2.1. Emplazamiento y protección de los equipos. (34)
     - 5.2.2. Instalaciones de suministros. (35)
     - 5.2.3. Seguridad del cableado. (36)
     - 5.2.4. Mantenimiento de los equipos. (37)
     - 5.2.5. Seguridad de los equipos fuera de las instalaciones. (38)
     - 5.2.6. Reutilización o retirada segura de equipos. (39)
     - 5.2.7. Retirada de materiales propiedad de la empresa. (40)
6. GESTIÓN DE COMUNICACIONES Y OPERACIONES
   - 6.1. Responsabilidades y procedimientos de operación: (11)
     - 6.1.1. Documentación de los procedimientos de operación. (41)
     - 6.1.2. Gestión de cambios. (42)
     - 6.1.3. Segregación de tareas. (43)
     - 6.1.4. Separación de los recursos de desarrollo, prueba y operación. (44)
   - 6.2. Gestión de la provisión de servicios por terceros: (12)
     - 6.2.1. Provisión de servicios. (45)
     - 6.2.2. Supervisión y revisión de los servicios prestados por terceros. (46)
     - 6.2.3. Gestión del cambio en los servicios prestados por terceros. (47)
   - 6.3. Planificación y aceptación del sistema: (13)
     - 6.3.1. Gestión de capacidades. (48)
     - 6.3.2. Aceptación del sistema. (49)
   - 6.4. Protección contra el código malicioso y descargable: (14)
     - 6.4.1. Controles contra el código malicioso. (50)
     - 6.4.2. Controles contra el código descargado en el cliente. (51)
   - 6.5. Copias de seguridad: (15)
     - 6.5.1. Copias de seguridad de la información. (52)
   - 6.6. Gestión de la seguridad de redes: (16)
     - 6.6.1. Controles de red. (53)
     - 6.6.2. Seguridad de los servicios de red. (54)
   - 6.7. Manipulación de los soportes: (17)
     - 6.7.1. Gestión de soportes extraíbles. (55)
     - 6.7.2. Retirada de soportes. (56)
     - 6.7.3. Procedimientos de manipulación de la información. (57)
     - 6.7.4. Seguridad de la documentación del sistema. (58)
   - 6.8. Intercambio de información: (18)
     - 6.8.1. Políticas y procedimientos del intercambio de información. (59)
     - 6.8.2. Acuerdos de intercambio. (60)
     - 6.8.3. Soportes físicos en tránsito. (61)
     - 6.8.4. Mensajería electrónica. (62)
     - 6.8.5. Sistemas de información empresariales. (63)
   - 6.9. Servicios de comercio electrónico: (19)
     - 6.9.1. Comercio electrónico. (64)
     - 6.9.2. Transacciones en línea. (65)
     - 6.9.3. Información públicamente disponible. (66)
   - 6.10. Supervisión: (20)
     - 6.10.1. Registros de auditoría. (67)
     - 6.10.2. Supervisión del uso del sistema. (68)
     - 6.10.3. Protección de la información de los registros. (69)
     - 6.10.4. Registros de administración y operación. (70)
     - 6.10.5. Registro de fallos. (71)
     - 6.10.6. Sincronización del reloj. (72)
7. CONTROL DE ACCESO

Tabla 1: Dominio (1): Política de Seguridad de la Información

DOMINIO (1): POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN		
OBJETIVOS DE CONTROL	**CONTROLES**	**EXTRACTO DEL CONTROL**
Política de S-I Dirigir y dar soporte a la gestión de la S-I. La gerencia debería establecer la actuación, apoyo y compromiso a la SI, publicando y manteniendo una política de seguridad en la organización.	**Documento de política de S-I**	La gerencia debería **APROBAR-PUBLICAR-COMUNICAR a todos los empleados un documento de política de S-I**.
	Revisión de la política de S-I	**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.

Tabla 2: Dominio (2): Aspectos Organizativos para la S-I

DOMINIO (2): ASPECTOS ORGANIZATIVOS PARA LA S-I		
OBJETIVOS DE CONTROL	**CONTROLES**	**EXTRACTO DEL CONTROL**
Organización Interna Gestionar la S-I dentro de la organización. Establecer una estructura de gestión para iniciar y controlar la implantación de la S-I, organizar foros de gestión con la gerencia para aprobar la política de S-I, asignar roles de seguridad, si fuera necesario consultar a especialistas o consultores externos en S-I para mantenerse actulizado en las tendencias de la industria, evolución de la norma y los métodos de evaluación	**Compromiso de la Dirección con la S-I (comité de gestión de la S-I)**	**La gerencia debe apoyar activamente la S-I** dentro de la organización a través de direcciones claras demostrando **compromiso, asignaciones explicitas y reconocimiento de responsabilidades**
	Coordinación de la S-I	**La información de las actividades de S-I deben ser coordinadas por representantes de diferentes partes** de la organización con roles relevantes y funciones de trabajo
	Asignación de responsabilidades sobre S-I	Deberían **definirse claramente las responsabilidades**
	Proceso de autorización de recursos para el tratamiento de la información	Debería **establecerse un proceso de autorización para la gestión de cada nuevo recurso** de tratamiento de la información
	Acuerdos de Confidencialidad	**Requerimientos de confidencialidad o de no-acceso o acuerdos de no divulgación** de las necesidades de la organización para la protección de la información **deben ser identificadas y revisadas regularmente**
	Contacto con las autoridades	Debe existir **contacto apropiado con autoridades relevantes o proveedores si se sospecha que las leyes han sido rotas**
	Contacto con grupos de especial interés	Debe existir **contacto apropiado con grupos de interés especial o especialistas en foros de seguridad** y asociaciones profesionales
	Revisión independiente de la S-I	Para gestionar la S-I y su implementación **(controles, políticas, procesos y procedimientos) deben ser revisados independientemente en intervalos planificados**
Seguridad en los accesos a Terceros Mantener la seguridad de los recursos de tratamiento de la información y de los activos de información cuando sean accesibles por terceros. Se debe controlar el acceso de terceros a los dispositivos de tratamiento de la información de la organización. Se deben definir medidas de control en un contrato con la tercera parte dependiendo del riesgo que represente para la S-I	**Identificación de los riesgos derivados del acceso de terceros**	**Los riesgos a la información** y a las instalaciones del procesamiento de la información **que impliquen a terceros deben ser identificados y se debe implementar controles antes de conceder el acceso**
	Requisitos de seguridad en la relación con los clientes	**Todos los requisitos identificados de seguridad deben ser anexados antes de dar a los clientes acceso a la información** o a los activos de la organización
	Requisitos de seguridad en contratos con terceros (Outsourcing)	**Los acuerdos con terceras partes que implican el acceso, proceso, comunicación o gestión de la información** o de los activos de la organización, adición de productos o servicios adicionales **debe cubrir todos los requisitos de seguridad relevantes**

Tabla 3: Dominio (3): Gestión de Activos

DOMINIO (3): GESTIÓN DE ACTIVOS (CLASIFICACIÓN Y CONTROL)		
OBJETIVOS DE CONTROL	**CONTROLES**	**EXTRACTO DEL CONTROL**
Responsabilidad sobre los activos Mantener una protección adecuada sobre los activos de la organización. Todos los activos deben ser considerados y tener un propietario asignado. Se debe Identificar los propietarios para todos los activos importantes y asignar la responsabilidad del mantenimiento de los controles apropiados	**Inventario de activos**	**Todos los activos deben ser claramente identificados** y se debe **elaborar y mantener un inventario de todos los activos importantes**
	Propiedad de los activos	Toda la información y los activos deben ser poseídos por una parte designada de la organización, **el propietario del servicio es responsable por la entrega del servicio incluyendo la funcionalidad de los activos**
	Uso adecuado de los activos	**Las reglas para un uso adecuado de la información y de los activos asociados deben ser identificados, documentados e implementados**
Clasificación de la información Asegurar un nivel de protección adecuado a los activos de información. La información debe clasificarse para indicar la necesidad, prioridad y grado de protección dependiendo del grado de sensibilidad y criticidad de la misma. Algunos elementos de información pueden requerir un nivel	**Directrices de clasificación**	**La información debe clasificarse en función de su valor, requisitos legales, sensibilidad y criticidad** para la organización
	Etiquetado y tratamiento de la información	Definir un conjunto adecuado de **procedimientos para etiquetar y tratar la información de acuerdo a su clasificación** adoptada (manipulación, copias, almacenamiento, transmición, clasificación y destrucción)

Tabla 4: Dominio (4): Seguridad Ligada a los Recursos Humanos

DOMINIO (4): SEGURIDAD LIGADA A LOS RECURSOS HUMANOS		
OBJETIVOS DE CONTROL	**CONTROLES**	**EXTRACTO DEL CONTROL**
Seguridad antes del empleo Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades y que sean adecuados para los roles para los que han sido considerados, reduciendo el riesgo de hurto, fraude o mal uso de las instalaciones. Empleados, contratistas y terceros deben firmar un acuerdo de confidencialidad	**Inclusión de la seguridad en las funciones y responsabilidades laborales**	**Las funciones y responsabilidades de los empleados**, contratistas y terceros **deben ser definidas y documentadas en concordancia con la política de S-I**
	Investigación de antecedentes (selección de personal)	**Se debe llevar listas de verificación anteriores de todos los candidatos para empleo en concordancia con las leyes, regulaciones y la ética**. Realizar una comprobación mas detallada de la persona, contratista, terceros, personal temporal cuando accedan a su empleo
	Acuerdos de confidencialidad	**Como parte de su obligación contractual, empleados, contratistas y terceros deben aceptar y firmar los términos y condiciones** del contrato de empleo el cual establece sus obligaciones y las obligaciones de la organización **para la S-I**
Durante el empleo Asegurar que los empleados, contratistas y terceros esten consientes de las amenazas y riesgos en el ámbito de la S-I, y que están preparados para sostener la política de S-I en el curso normal de su trabajo y de reducir el riesgo de error humano. Un nivel adecuado de conocimiento, educación y entrenamiento en procedimientos de seguridad debe ser provista a todos los empleados	**Responsabilidades de la Gerencia**	La gerencia debe requerir a los empleados, contratistas y terceros aplicar la seguridad en concordancia con las políticas y procedimientos establecidos en la organización. **Asegurarse de que los empleados tengan en claro sus responsabilidades, roles, motivados y capacitados en S-I**
	Concienciación, formación y capacitación en seguridad de la información	**Todos los empleados de la organización deben recibir entrenamiento apropiado en políticas y procedimientos organizacionales para la función de su trabajo**
	Proceso disciplinario	**Debe existir un proceso formal disciplinario para empleados** que han cometido una apertura en la seguridad o **han violado alguna política de seguridad**
Finalización del empleo o cambio de puesto de trabajo Asegurar que los empleados, contratistas o terceros salgan de la organización de una forma ordenada, cambios en las responsabilidades y que el retiro de todo derecho de acceso este completada	**Responsabilidad del cese o cambio (finalización)**	Las responsabilidades para realizar **la finalización de un empleo o el cambio de este deben ser claramente definidas y asignadas.** Deben incluir requisitos de seguridad, responsabilidades legales y acuerdos de confidencialidad
	Devolución o retorno de activos	**Todos los empleados,** contratistas y terceros **deben retornar todos los activos de la organización** (software, documentos corporativos, equipos, tarjetas de acceso, manuales, respaldos digitales) **que estén en su posesión hasta la finalización de su empleo**, contrato o acuerdo
	Retiro de los derechos de acceso	**Los derechos de acceso (físico y lógico) para todos los empleados,** contratistas y terceros **deben ser removidos hasta la culminación del empleo, contrato o acuerdo, o debe ser ajustada en caso de cambio**

Tabla 5: Dominio (5): Seguridad Física y del Entorno

DOMINIO (5): SEGURIDAD FÍSICA Y DEL ENTORNO		
OBJETIVOS DE CONTROL	**CONTROLES**	**EXTRACTO DEL CONTROL**
Áreas seguras Evitar accesos no autorizados, daños e interferencias contra los locales y la información de la organización. Los recursos críticos y sensibles para la organización deben ubicarse en áreas seguras protegidas por un perímetro de seguridad definida, con barreras de seguridad y controles de entrada, siendo estos proporcionales a los riesgos definidos	**Perímetro de seguridad física**	**Los perímetros de seguridad como paredes, tarjetas de control de entrada a puertas, alarmas o un puesto de recepción, deben ser usados para proteger áreas que contengan información** o recursos de procesamiento de información
	Controles físicos de entrada	**Las áreas de seguridad deben estar protegidas por controles de entrada adecuados que aseguren el permiso de acceso sólo al personal autorizado.** Se deben supervisar las visitas, registrar fechas de entrada y de salida, utilizar controles de autenticación, rastros auditables de acceso y utilizar formas de identificación de todo el personal
	Seguridad de oficinas, despachos e instalaciones	**La seguridad física para oficinas, despachos e instalaciones debe ser asignada y aplicada**. Se debe tomar en cuenta estándares de seguridad y salud, instalar equipos con claves de acceso o no mostrar mucha identificación de los activos sensibles
	Protección contra las amenazas externas y de origen ambiental	**Se debe designar y aplicar protección física del fuego, inundación, terremoto, explosión, malestar civil, goteo de agua en tuberías y otras formas de desastre natural o humana**
	Trabajo en áreas seguras	**Se debe diseñar y aplicar protección física y pautas para trabajar en áreas seguras**. Estas áreas deben estar cerradas y controladas cuando estén vacías, además **no se debe permitir equipos de fotografía, video o cualquier método de grabación** sin autorización
	Áreas de acceso público, áreas de carga y descarga	**Se deben controlar las áreas de carga y descarga para evitar accesos no autorizados. El material entrante y saliente se debería supervisar y registrar** de acuerdo a políticas establecidas
Seguridad de los equipos Evitar pérdidas, daños o comprometer los activos así como la interrupción de las actividades de la organización. El equipo debe estar físicamente protegido de amenazas y se debería considerar su instalación fuera del local en caso de emergencia. También se deben considerar controles para la alimentación eléctrica y el cableado	**Instalación y protección de los equipos**	**El equipo debe situarse y protegerse para reducir el riesgo de amenazas del entorno y de accesos no autorizados.** Establecer controles para minimizar riesgos de robo, incendio, humo, agua, polvo, vibraciones, efectos químicos, interferencias eléctricas, radiaciones electromagnéticas y vandalismo, humedad, así como no fumar, comer o beber cerca de estos equipos.
	Suministro eléctrico	**Se debe proteger los equipos contra fallos de energía y otras anomalías eléctricas en los equipos de apoyo como son los generadores, UPS, suministros de agua, aires acondicionados.** Estos deben ser inspeccionados regularmente y probados apropiadamente para asegurar su funcionamiento
	Seguridad del cableado	**Se debe proteger contra daños o interceptaciones el cableado de energía y telecomunicaciones que transporten datos o soporten servicios de información**. Utilizar conductos blindados subterráneos, cables identificados, separar cables de energía con los de datos
	Mantenimiento de los equipos	**Los equipos deben mantenerse adecuadamente para asegurar su continua disponibilidad e integridad**. Solo el personal de mantenimiento debidamente autorizado debe realizar la reparación y servicio de los equipos, registrar documentalmente todos los fallos reales o sospechosos, así como el mantenimiento preventivo y correctivo
	Seguridad de los equipos fuera de las instalaciones	**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 esta expuest**o. Implementar controles cuando se trabaja desde la casa y solo la gerencia autoriza el retiro de los equipos de su entorno habitual
	Seguridad en el rehúso o eliminación de equipos	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. **Los dispositivos de almacenamiento dañados con información sensible deben ser destruidos físicamente y la información debe ser destruida evitando ser recuperable**
	Retirada de materiales propiedad de la empresa	**El equipo, información o software no debe ser sacado fuera del local sin autorización**. Si existe el permiso, el equipo debe ser registrado cuando sale y cuando entra, así como el tiempo límite para el retiro y el retorno.

Tabla 6: Dominio (6): Gestión de Comunicaciones y Operaciones

DOMINIO (6): GESTIÓN DE COMUNICACIONES Y OPERACIONES		
OBJETIVOS DE CONTROL	**CONTROLES**	**EXTRACTO DEL CONTROL**
Procedimientos y responsabilidades de operación Asegurar la operación correcta y segura de los recursos de tratamiento de la información. Se deben establecer responsabilidades y procedimientos para la gestión y operación de todos los recursos de tratamiento de información, incluyendo instrucciones apropiadas de operación y procedimientos de respuesta ante incidencias. Además se implantará la segregación de tareas para reducir el riesgo de un mal uso del sistema o por negligencia	**Documentación de los procedimientos de operación**	**Se deben documentar y mantener los procedimientos de operación y ponerlos a disposición de todos los usuarios que lo requieran**. Establecer procedimientos documentados para actividades de sistemas de información y los recursos de comunicación, como prendido y apagado de equipos, bakups, mantenimiento de equipos, manejo de errores, manipulación de medios, ambientes de computo, contactos de apoyo técnico, manipulación de correos y seguridad
	Gestión de cambios	**Se debe controlar estrictamente los cambios en los sistemas y recursos de tratamiento de la información.** Esto es la identificación y registro del cambio, el planeamiento y pruebas del cambio, la evaluación del posible impacto, la comunicación de los detalles de cambio a todas las personas que corresponda, la responsabilidad de abortar y recuperarse de los cambios sin éxito y de acontecimientos imprevistos
	Segregación de tareas	**Se debe 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.** Es importante que la auditoria de seguridad permanezca independiente
	Separación de los recursos de desarrollo, prueba y operación	**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.** Las reglas de transferencia del software desde el desarrollo al de producción deben ser definidos y documentados, además el entorno de prueba del sistema debe emular el entorno del sistema operacional lo mas cercano posible utilizando otros procesadores, dominios o directorios distintos
Gestión de servicios externos Implementar y mantener un nivel apropiado de seguridad y de entrega de servicio en línea con los acuerdos con terceros. Se debe verificar la implementación de acuerdos y monitorear la conformidad con los acuerdos con el fin de asegurar que todos los servicios entregados cumplen con todos los requerimientos acordados con terceros	**Servicio de entrega**	**Asegurarse que todos los controles de seguridad, definiciones de servicio, acuerdos de servicio y niveles de entrega incluidas en el acuerdo de entrega de servicio externo sean implementados, operados y mantenidos por la parte externa**
	Supervisión y revisión de los servicios prestados por terceros	**Los servicios, reportes, reuniones, incidentes y registros provistos por terceros deben ser monitoreados y revisados regularmente, y las auditorias deben ser llevadas a cabo regularmente.** La responsabilidad para manejar las relaciones con un tercero debe ser asignada a un individuo designado y se deben tomar acciones apropiadas cuando se observen deficiencias en el servicio entregado
	Gestión del cambio para los servicios externos	Se debe **gestionar los cambios en la provisión del servicio, incluyendo mantenimiento y mejoras en las políticas de seguridad de información existentes**, como realces en el actual servicio ofrecido, modificaciones o actualizaciones de los procedimientos organizacionales, **controles nuevos para resolver incidentes, uso de nuevas tecnologías, nuevas versiones lanzadas, cambios en la localización física de los recursos de servicio**
Planificación y aceptación del sistema Minimizar el riesgo de fallos de los sistemas. Se debe planificar y realizar proyecciones de los requisitos futuros de capacidad para reducir el riesgo de sobrecarga del sistema. Se debe también establecer, documentar y probar antes de su aceptación los requisitos operacionales de los sistemas nuevos	**Planificación de la capacidad**	**El uso de recursos y las proyecciones hechas de requisitos de capacidades adecuadas futuras para asegurar el sistema de funcionamiento requerido debe ser monitoreado, para mejorar la disponibilidad y la eficiencia de los sistemas.** Controles de detección deben ser instalados para detectar los problemas en un tiempo debido, tomando en cuenta los nuevos requisitos, tendencia actual, cuellos de botella que representen una amenaza a la seguridad y proyección del tratamiento de la información en la organización
	Aceptación del sistema	**Se deben establecer criterios de aceptación para nuevos sistemas de información o versiones nuevas mejoradas y se debe desarrollar con ellos las pruebas adecuadas antes de su aceptación**. Los administradores deben asegurar que los requisitos y criterios de aceptación de los nuevos sistemas estén definidos, acordados, documentados y probados, y deben salir a producción solamente después de una aceptación formal tomando en cuenta requisitos de rendimiento, procesos de recuperación de errores y reinicio, planes de contingencia, controles de seguridad, manual de procedimientos, plan de continuidad, la facilidad de empleo (como esta afecta el funcionamiento del usuario y evita errores humanos)
Protección contra software malicioso Proteger la integridad del software y de la información. Establecer precauciones para prevenir, detectar y evitar la introducción de software malicioso como virus informático, gusanos de red, caballos de Troya, bombas lógicas	**Medidas y controles contra el software malicioso**	**Se deben implantar controles para detectar el software malicioso y prevenirse contra él, junto a procedimientos adecuados para concientizar a los usuarios.** Crear políticas contra el software no licenciado o no autorizado, obtención de archivos o software de otras redes, instalación y actualización de antivirus, planes de continuidad del negocio para recuperarse de los ataques de virus, capacitación sobre nuevos virus creados, realizar boletines de información de alerta de ataques
	Medidas y controles contra el código descargado en el cliente (código móvil)	**Donde el uso de código descargable o móvil es autorizado, la configuración debe asegurar que dicho código opera de acuerdo a una política de seguridad definida y que se debe prevenir que este sea ejecutado**. Se pueden crear ambientes lógicos aislados para la ejecución de los códigos descargados
Gestión de respaldo y recuperación Mantener la integridad y la disponibilidad de los servicios de tratamiento de información y comunicación.	**Recuperación de la información**	**Se debe hacer regularmente copias de seguridad de toda la información esencial del negocio y del software, en concordancia con la política acordada de recuperación.** Establecer procedimientos rutinarios haciendo copias de seguridad y ensayando su oportuna recuperación
Gestión de la seguridad de redes Asegurar la salvaguarda de la información en las redes y la protección de su infraestructura de apoyo. La gestión de la seguridad de las redes que cruzan las fronteras de la organización requiere controles y medidas adicionales para proteger los datos sensibles que circulan por las redes públicas	**Controles de red**	**Las redes deben ser manejadas y controladas adecuadamente para protegerse de amenazas y para mantener la seguridad en los sistemas y aplicaciones usando las redes, incluyendo información en transito**. Los administradores de redes deben implantar controles para conservar la seguridad de los datos y protección de los servicios, controles como: responsabilidades para la gestión de equipos remotos, salvaguardar la confidencialidad e integridad de los datos en redes públicas, registro y monitoreo de acciones de seguridad
	Seguridad de los servicios de red	**Las características de seguridad, niveles de servicio y los requisitos de gestión de todos los servicios de red deben ser identificados, monitoreados, auditados e incluidos en cualquier acuerdo de servicio de red, sean estos provistos dentro o fuera de la organización**. Las características de los servicios de seguridad de redes pueden ser: autenticación, encriptado y controles de conexión de red, parámetros requeridos de conexiones seguras, restricción de accesos a servicios o aplicaciones

Tabla 7: Dominio (6): Gestión de Comunicaciones y Operaciones

DOMINIO (6): GESTIÓN DE COMUNICACIONES Y OPERACIONES		
OBJETIVOS DE CONTROL	**CONTROLES**	**EXTRACTO DEL CONTROL**
Utilización de los medios de información Prevenir acceso no autorizado, modificaciones, robos, evitar daños a los activos e interrupciones de las actividades de la organización. Los medios deben ser controlados y físicamente protegidos. Establecer procedimientos operativos adecuados para proteger documentos, discos, cintas, CDs, DVDs, datos de entrada/salida y documentación del sistema, comunicaciones móviles, correo, multimedia	**Gestión de medios removibles (extraíbles)**	Debe haber **procedimientos para la gestión de los medios informáticos extraíbles** como: **borrarlos cuando no se requieren más, todo medio desechado por la organización requiere autorización para destruirlo y se debe guardar registro de su remoción para guardar pistas de auditoría, llevar un control de la vida útil del medio a utilizar, el registro de los medios extraíbles debe ser considerado para limitar la perdida de datos**
	Eliminación de medios extraíbles	**Se deben eliminar los medios de forma segura y sin peligro cuando no se necesiten más, utilizando procedimientos formales.**
	Procedimientos de manipulación de la información	**Los procedimientos para la manipulación y almacenamiento de la información deben ser establecidos para proteger esta información de divulgaciones o usos no autorizados. Se debe controlar el etiquetado de todos los medios, restricciones de acceso**, mantenimiento de un registro formal de recipientes autorizados de datos, aseguramiento de que los datos de entrada, su proceso y la validación de la salida están completos, almacenamiento de los medios en un entorno acorde con las especificaciones del fabricante
	Seguridad de la documentación del sistema	**La documentación de sistemas debe ser protegida contra acceso no autorizado, para esto se debe almacenarla con seguridad, la lista de acceso a la documentación se debe limitar al máximo y ser autorizada por el propietario de la aplicación**
Intercambio de información Evitar la pérdida, modificación o mal uso de la información intercambiada entre organizaciones. Se debe realizar intercambios sobre la base de acuerdos formales, controlando y cumpliendo con toda la legislación correspondiente y protegiendo la información de los medios en tránsito	**Políticas y procedimientos para el intercambio de información y software**	**Se deben 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.** Procedimientos designados para proteger la información intercambiada de una intercepción, copiado, modificación, cambio de ruta, eliminación, código malicioso que circula en la red, información electrónica que esta en forma de archivos adjuntos, comunicaciones inalámbricas, conversaciones en los pasillos, responsabilidad de los usuarios al comunicarse entre si, uso de técnicas criptográficas, respeto a la legislación y regulación nacional y local
	Acuerdos de intercambio	**Los acuerdos deben ser establecidos para el intercambio de información y software entre la organización y terceros**. Implementar condiciones de seguridad como: las responsabilidades de la gerencia para controlar y notificar la transmisión, despacho y recibo, estándares técnicos para empacado y transmisión, acuerdos de fideicomiso, identificación de mensajería, responsabilidad en los incidentes como pérdida de datos, copyright, licenciamiento
	Medios físicos en tránsito	**Los medios físicos conteniendo información deben ser protegidos contra acceso no autorizado, mal uso o corrupción durante el transporte fuera de los limites físicos de la organización**. Se debe usar transporte o mensajeros fiables y convenirse entre las gerencias una lista de mensajeros autorizados
	Seguridad en la mensajería electrónica	L**a información implicada con la mensajería electrónica debe ser protegida apropiadamente. Consideraciones como protección de mensajes de accesos no autorizados, modificaciones o negación del servicio, asegurar una dirección y un transporte correcto del mensaje, confiabilidad y disponibilidad**, consideraciones legales como firmas electrónicas, autentificación del acceso en redes públicas
	Sistemas de información empresariales	**Se debe desarrollar e implementar políticas y procedimientos con el fin de proteger la información asociada con la interconexión de sistemas de información de negocios.** Las consideraciones de seguridad al interconectar organizaciones deben incluir vulnerabilidades en sistemas de administración y contabilidad, vulnerabilidad en sistemas de comunicación como el grabado de llamadas telefónicas, conferencias, almacenamiento de faxes, correo abierto, archivos compartidos
Servicios de comercio electrónico Asegurar la seguridad de los servicios de comercio electrónico y de su uso seguro. Seguridades como transacciones en línea o información electrónica publicada a través de sistemas disponibles de publicidad.	**Comercio electrónico**	**La información envuelta en el comercio electrónico pasando a través de redes públicas, deben ser protegidas de actividad fraudulenta, disputas de contratos y de acceso y modificación no autorizada**. Consideraciones como el nivel de confidencialidad, procesos de autorización para designar los precios, ediciones o firmas en los documentos de negocio, que los socios de negocio estén totalmente informados, pruebas de despacho y recepción de documentos, ordenes de transacciones, información de pagos, evitar pérdidas o duplicidad de la información
	Transacciones en línea	**La información implicada en las transacciones en línea 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.** Se deben usar firmas electrónicas y credenciales de usuario por cada una de las partes envueltas en la transacción, medios de comunicación cifradas, protocolos seguros, almacenamiento de las transacciones en repositorios seguros sin acceso al internet
	Información publica disponible	**La integridad de la información que se ha hecho disponible en un sistema público deber ser protegida para prevenir modificaciones no autorizadas. Se debe usar firmas digitales para aquella información sensible que se requiere sea pública**

Tabla 8: Dominio (6): Gestión de Comunicaciones y Operaciones

DOMINIO (6): GESTIÓN DE COMUNICACIONES Y OPERACIONES		
OBJETIVOS DE CONTROL	**CONTROLES**	**EXTRACTO DEL CONTROL**
Monitoreo Detectar las actividades de procesamiento de información no autorizadas. Los sistemas deben ser monitoreados y los eventos de la seguridad de información deben ser grabados cumpliendo con todos los requerimientos legales aplicables para el monitoreo y el registro de actividades. El monitoreo debe ser utilizado para verificar la efectividad de los controles adoptados y para verificar la conformidad de un acceso a un modelo de política	**Registros de auditoria**	**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. **Los registros de auditoría deben incluir identificación de usuarios, fecha y hora de conexión y desconexión, identidad de la terminal de acceso, registro de éxito y fracaso de accesos al sistema, cambios de configuración del sistema, uso de privilegios, direcciones de red, alarmas realizadas**
	Monitoreando el uso del sistema	**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.** Monitoreos al acceso autorizado incluyendo detalles como la identificación del usuario, fecha y hora de eventos claves, archivos y programas utilizados, el uso de cuentas privilegiadas como supervisores, puesta en marcha y parada de los sistemas, conexión o desconexión de un recurso, accesos no autorizados, violaciones a las políticas de acceso, alertas de los sistemas de detección de intrusos, alertas de consolas, alarmas de red, alarmas de los controles de acceso
	Protección de la información de los registros	**Las instalaciones de información de registro deben ser protegidas contra acciones forzosas y accesos no autorizados.** Controlar la capacidad de almacenamiento del medio del archivo de registro de los eventos ocurridos, archivar los registros de auditoria o evidencias importantes
	Registros de administradores y operadores	**Las actividades del administrador y de los operadores del sistema deben ser registradas**. Los registros deben incluir el tiempo en el que ocurrió el evento, información acerca del evento, que cuenta y que administrador u operador fue implicado, que procesos fueron implicados
	Registro de fallos (averías)	**Los fallos deben ser registrados, analizados y se deben tomar acciones apropiadas. Las fallas o averías reportadas por usuarios o por programas del sistema deben ser registrados con el fin de resolverlas satisfactoriamente**, revisar medidas correctivas para asegurar que los controles no han sido comprometidos
	Sincronización del reloj	**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**

Tabla 9: Dominio (7): Control de Accesos

DOMINIO (7): CONTROL DE ACCESOS		
OBJETIVOS DE CONTROL	**CONTROLES**	**EXTRACTO DEL CONTROL**
Requisitos de negocio para el control de accesos Controlar los accesos a la información. Tener en cuenta para ello las políticas de distribución de la información y de autorizaciones	**Política de control de acceso.**	**Una política de control de acceso debe ser establecida, documentada y revisada y debe estar basada en los requerimientos de seguridad y del negocio.** Establecer reglas y derechos de los usuarios o grupos de usuarios, controles de acceso lógicos y físicos, perfiles de usuarios, segregación de roles de control de acceso. Estas deben ser apoyadas por responsabilidades y procedimientos formales claramente definidos
Gestión de acceso de usuarios Asegurar el acceso autorizado de usuarios y prevenir accesos no autorizados a los sistemas de información. Establecer procedimientos formales para controlar la asignación de los derechos de acceso a los sistemas y servicios cubriendo todas las etapas del ciclo de vida de acceso de los usuarios, desde el registro inicial de los nuevos hasta la baja de los usuarios que ya no requieran accesos a los sistemas y servicios. Tener controles especiales a los usuarios privilegiados pues pueden evitar los controles del sistema	**Registro de usuarios**	**Se debe formalizar un procedimiento de registro de altas y bajas de usuarios para garantizar el acceso a los sistemas y servicios de información multiusuario. Los registros de acceso en sistemas multiusuario deben tener un identificador único para cada usuario, identificadores del grupo, comprobación de autorizaciones por el propietario del servicio para utilizar el sistema, documento escrito de sus derechos de acceso,** eliminación inmediata de autorizaciones de acceso a usuarios que dejan la organización, eliminación de cuentas redundantes
	Gestión de privilegios	**Se debe restringir y controlar el uso y asignación de privilegios. Tener un proceso formal para controlar la asignación de privilegios considerando: identificar los privilegios asociados a cada elemento del sistema como el sistema operativo, el gestor de base de datos y sus aplicaciones, las categorías de empleados que necesitan de ellos,** asignar privilegios según principios de necesidad de uso, registros de asignación de privilegios, asignar privilegios a un identificador de usuario distinto al asignado para uso normal
	Gestión de contraseñas de usuario	**Se debe controlar la asignación de contraseñas por medio de un proceso de gestión formal. Requisitos como el de requerir firmas de compromiso de los usuarios para mantener en secreto sus contraseñas personales y las compartidas por un grupo, proporcionar claves temporales que forzosamente deben cambiar después**, verificación de identidad del usuario antes de proveer una contraseña, establecer envíos seguros para hacer llegar las contraseñas temporales, **las contraseñas temporales deben ser únicas para cada individuo y no deben ser obvias**
	Revisión de los derechos de acceso de los usuarios	**La gerencia debe establecer un proceso formal de revisión periódica de los derechos de acceso de los usuarios**. Revisar los derechos de acceso con privilegios especiales, los derechos que son reasignados cuando se trasladan de un empleo a otro dentro de la organización
Responsabilidades de los usuarios Una protección eficaz necesita la cooperación de los usuarios autorizados. Los usuarios deben ser conscientes de sus responsabilidades en el mantenimiento de la eficacia de las medidas de control de acceso, uso de contraseñas, de la seguridad del material puesto a su disposición, escritorios limpios, pantallas claras, acceso de usuarios no autorizados, hurto de la información.	**Uso de contraseñas**	**Los usuarios deben seguir prácticas de seguridad para la selección y uso de sus contraseñas.** Capacitar a usuarios para que mantengan la confidencialidad de sus contraseñas, evitar guardar registros de papel de contraseñas, cambio de contraseñas en intervalos de tiempo regulares o si existe indicio de vulnerabilidad, uso de contraseñas complejas o de buena calidad, no compartir contraseñas, no usar mismas contraseñas para propósitos personales o de negocio, no almacenar permanentemente la contraseña en procedimientos automáticos. La gestión que trata con los sistemas de ayuda que tratan con problemas de perdida y olvido de claves necesitan un cuidado especial
	Equipo informático de usuario desatendido	**Los usuarios deben asegurar que los equipos informáticos desatendidos estén debidamente protegidos. Los usuarios tienen responsabilidades de cancelar todas las sesiones activas antes de marcharse de la organización**, uso de protectores de pantalla con claves, apagado de los equipos críticos correctamente
	Política de pantalla limpia y escritorio limpio	**Se debe adoptar una política de escritorio limpio de papeles y medios removibles de almacenamiento así como una política de pantalla limpia para instalaciones de procesamiento de información. Tomar en cuenta la clasificación de la información, requerimientos legales y contractuales, los riesgos correspondientes y aspectos culturales de la organización.** Hacer uso de cajas fuertes o gavetas seguras, los computadores y terminales deben tener protección de acceso mediante uso de claves, debe ser controlado el uso de fotocopiadoras y escáner, tener cuidado con la información que se imprime
Control de acceso a la red Prevenir el acceso no autorizado de los servicios de la red. Se debe controlar el acceso a los servicios de las redes internas y externas asegurándose que el acceso de los usuarios no comprometan la seguridad informática implementando interfaces de comunicación adecuadas, autenticación para usuarios y equipos, control de acceso de los usuarios	**Política de uso de los servicios de la red**	**Los usuarios sólo deberían tener acceso directo a los servicios para los que estén autorizados de una forma específica**. Formular políticas, controles y procedimientos que abarquen las redes y servicios de red a los que se puede acceder, procedimientos de autorización, medios usados para el acceso
	Autenticación de usuario para conexiones externas	**Utilizar métodos apropiados de autenticación para controlar el acceso de usuarios remotos.** Se podría usar técnicas de criptografía, protocolos de desafío-respuesta, redes privadas virtuales, líneas dedicadas, dial-back, cuidados especiales en los controles para redes inalámbricas
	Identificación de los equipos en las redes	La identificación de equipos puede ser utilizada si es importante que las comunicaciones puedan ser iniciadas, **un indicador dentro del equipo puede ser utilizado para indicar si el equipo esta autorizado para conectarse a la red**
	Diagnostico remoto y configuración de protección de puertos	**Se debe controlar el acceso físico y logístico para diagnosticar y configurar puertos**. Los puertos, servicios y equipos que no son requeridos para la funcionalidad del negocio deben ser inhabilitados o removidos
	Segregación de las redes	**Los grupos de servicios de información, usuarios y sistemas de información deben ser segregados en las redes. Para controlar la seguridad de grandes redes, se las puede dividir en dominios lógicos**, protegidos cada uno por perímetros definidos de seguridad usando gateways, firewalls, redes virtuales privadas, capacidad de enrutamiento
	Control de conexión a la red	**Los requisitos de la política de control de accesos para redes compartidas o redes fuera de la organización, se deben basar en los requisitos de las aplicaciones del negocio.** Identificar la capacidad de conexión de los usuarios para restringir el tráfico en correo electrónico, transferencias de archivos, accesos a las aplicaciones, accesos en ciertos períodos de tiempo
	Control de enrutamiento en la red	**Se debe 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, usar controles de verificación de direcciones de origen y destino**

Tabla 10: Dominio (7): Control de Accesos

DOMINIO (7): CONTROL DE ACCESOS		
OBJETIVOS DE CONTROL	**CONTROLES**	**EXTRACTO DEL CONTROL**
Control de acceso al sistema operativo Evitar accesos no autorizados a los computadores. Implementar controles de seguridad a nivel de sistema operativo para identificar y verificar la identidad de cada usuario, registrar los accesos satisfactorios y fallidos al sistema, alarmas, mecanismos de autenticación, restringir tiempos de conexión	**Procedimientos de conexión de terminales (inicio de sesión)**	**El acceso a los servicios de información debe estar disponible mediante un proceso de conexión segura.** Un buen procedimiento debe: no mostrar mucha información sobre el sistema para no facilitar ayuda innecesaria a usuarios no autorizados, mostrar mensajes de restricción de acceso, validar la información de conexión, **limitar el número de intentos fallidos de conexión, no mostrar la contraseñas**
	Identificación y autenticación de usuario	**Todos los usuarios deben disponer de un identificador único para su uso personal y debería ser escogida una técnica de autenticación adecuada para verificar la identidad de estos**
	Sistema de gestión de contraseñas	**Los sistemas de gestión de contraseñas deben proporcionar un medio eficaz e interactivo para asegurar la calidad de las mismas.** Una buena gestión de contraseñas debe almacenar las contraseñas en forma cifrada con algoritmos unidireccionales, imponer el uso de contraseñas de calidad, imponer cambio de contraseñas iniciales, permitir que los usuarios puedan cambiar sus contraseñas, mantener registros de todas las contraseñas utilizadas anteriormente, usar contraseñas individuales bajo responsabilidades individuales
	Utilización de las facilidades del sistema	**Si las instalaciones informáticas disponen de programas capaces de eludir las medidas de control del sistema, es fundamental que su uso se restrinja y se mantenga fuertemente controlado**
	Desconexión automática de sesión	**Las sesiones se deberían desactivar tras un periodo definido de inactividad, especialmente las aplicaciones y sesiones de conexión a la red**
	Limitación del tiempo de conexión	**Las restricciones en los tiempos de conexión ofrecen seguridad adicional para aplicaciones de alto riesgo, especialmente para terminales instalados en áreas de alto riesgo**
Control de acceso a las aplicaciones y a la información Prevenir el acceso no autorizado a la información contenida en los sistemas. Las aplicaciones deben controlar el acceso de los usuarios a la información y a las funciones del sistema, protegerse de software que eluda los controles de seguridad, no comprometer la seguridad de otros sistemas donde exista información compartida	**Restricción del acceso a la información.**	**Se debe dar acceso a la información y a las funciones del sistema de aplicaciones sólo a los usuarios de éste, incluido el personal de apoyo, de acuerdo con una política de control de accesos definidos.** Se debe establecer menús para controlar los accesos a las funciones, controlar los derechos de acceso de lectura-escritura-borrado-ejecución
	Aislamiento de sistemas sensibles	**Los sistemas sensibles pueden necesitar entornos informáticos dedicados o aislados y pueden necesitar un tratamiento especial**
Informática móvil (portátiles) y teletrabajo Garantizar la seguridad de la información cuando se usan portátiles y teletrabajo. La protección requerida debe ser proporcional a los riesgos que causan estas formas específicas de trabajo	**Informática móvil (portátiles) y comunicaciones móviles**	**Se debe adoptar una política formal y medidas de seguridad apropiadas con el fin de protegernos contra los riesgos cuando se usan medios móviles como portátiles, agendas, teléfonos.** Considerar la protección física, controles de acceso, técnicas criptográficas, respaldos de información de las portátiles, antivirus, controles en los protocolos de seguridad inalámbrica
	Teletrabajo	**Se debe desarrollar e implementar una política, planes operacionales y procedimientos para las actividades de teletrabajo**. La gerencia es la única que permitirá que se realicen trabajos fuera de la institución y debe exigir que se cumplan con las mismas seguridades que se tiene en la institución

Tabla 11: Dominio (8): Adquisición, Desarrollo y Mantenimiento de Sistemas

DOMINIO (8): ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS		
OBJETIVOS DE CONTROL	**CONTROLES**	**EXTRACTO DEL CONTROL**
Requisitos de seguridad de los sistemas Asegurar que la seguridad esté embebida dentro de los sistemas de información. Esto incluye la infraestructura, aplicaciones de negocio y desarrolladas por usuarios, el diseño, la implementación, el análisis y la justificación para desarrollar un sistema	**Análisis y especificación de los requisitos de seguridad**	**Los enunciados de los requisitos de negocio para sistemas nuevos o mejoras a sistemas existentes deben especificar los requisitos de control**. Las especificaciones deben considerar los controles automatizados a ser incorporados en el sistema, deben reflejar el valor de los activos de información implicados, pruebas formales en los procesos de adquisición
Seguridad de las aplicaciones del sistema Evitar pérdidas, modificaciones o mal uso de los datos de usuario en las aplicaciones. Se debe implementar dentro de las aplicaciones medidas de control para validar los datos de entrada, el tratamiento interno y los datos de salida	**Validación de los datos de entrada**	**Se deben validar los datos de entrada a las aplicaciones del sistema para garantizar que son correctas y apropiadas. Se debe verificar los datos de referencia, tablas de parámetros, entradas duplicadas, valores fuera de rango, caracteres inválidos, datos que faltan o están incompletos**, inspección del contenido de los campos clave y documentos físicos de entrada para ver si hay cambios no autorizados, definición de responsabilidades de los implicados en el proceso de entrada de datos
	Control del proceso interno	**Se debe incorporar en los sistemas comprobaciones de validación para detectar cualquier tipo de corrupción de información a través de errores del proceso o por actos deliberados. Se debe tener restricciones que minimicen el riesgo de los fallos del proceso con pérdidas de integridad** al añadir o borrar datos, considerar el uso de programas correctos de recuperación después de fallas, tener controles de sesión o de lotes
	Integridad de los mensajes	**Se debe identificar los requerimientos para asegurar la autenticación y protección de la integridad de los mensajes en aplicaciones usando controles apropiados como técnicas criptográficas**
	Validación de los datos de salida	**Se debe validar los datos de salida de un sistema de aplicación para garantizar que el proceso de información ha sido correcto y apropiado a las circunstancias. Validación de verosimilitud, conciliación**
Controles criptográficos Proteger la confidencialidad, autenticidad o integridad de la información. Se debe usar criptografía cuando otros controles no proporcionen la protección adecuada a la información	**Política de uso de los controles criptográficos**	**La organización debe desarrollar e implementar una política de uso de las medidas criptográficas para proteger la información.** Considerando la información que se maneja utilizar el algoritmo de cifrado requerido, incluir métodos para tratar de recuperar la información cifrada en caso de pérdida de claves, tener en cuenta las consideraciones de regulación nacional
	Gestión de claves	**La gestión de claves debe apoyar el uso de las técnicas criptográficas en la organización.** Se debe tener protección física para el equipo usado en la generación, almacenamiento y archivo de claves
Seguridad de los archivos del sistema Asegurar la seguridad de los archivos del sistema. El acceso a los archivos del sistema deben ser controlados y evitar la exposición de datos sensibles en ambientes de prueba	**Control del software en producción**	**Debe existir procedimientos para controlar la instalación del software en sistemas operacionales,** considerar que la actualización de librerías de programas operativos solo la realiza un administrador capacitado, los sistemas deben tener solo código ejecutable y compiladores, controlar y documentar la configuración del sistema, tener estrategias de restauración no actualizada antes de que se implementen cambios, retener versiones anteriores de software como medida de contingencia, controlar la aplicación de parches en el software
	Protección de los datos de prueba del sistema	**Los datos de prueba deben ser seleccionados cuidadosamente, protegidos y controlados**
	Control de acceso al código fuente de los programas	**El acceso al código fuente de los programas debe ser restringido.**
Seguridad en los procesos de desarrollo y soporte Mantener la seguridad del software de aplicación y la información. Los responsables de los sistemas deben controlar todo cambio propuesto al sistema, el soporte al mismo y comprobar que no se debilite la seguridad del sistema o del sistema operativo	**Procedimientos de control de cambios**	**La implementación de cambios debe ser controlada usando procedimientos formales de cambio.** Un proceso formal adecuado es aquel que se documenta, se especifica el alcance, se analiza el riesgo y el impacto, se prueba, se realiza control de calidad, se tiene una aprobación o acuerdo con la gerencia y se implementa
	Revisión técnica de los cambios en el sistema operativo	**Se debe revisar y probar las aplicaciones del sistema cuando se efectúen cambios, para asegurar que no impactan adversamente en el funcionamiento o en la seguridad.**
	Restricciones a los cambios en los paquetes de software	**No se recomiendan modificaciones a los paquetes de software. Se debe limitar a cambios necesarios y todos estos deben ser estrictamente controlados.**
	Fugas de información	**Las oportunidades de fuga de información deben ser prevenidas.**
	Desarrollo externo del software	**El desarrollo externo del software debe ser supervisado y monitoreado por la organización.** Considerar acuerdos bajo licencia, propiedad del código, acuerdos de calidad, funcionalidad y soporte, pruebas antes de la implantación
Gestión de la vulnerabilidad técnica Reducir los riesgos resultantes de la explotación de vulnerabilidades técnicas publicadas de una manera efectiva, sistemática y respetable con medidas tomadas para confirmar su efectividad	**Control de las vulnerabilidades técnicas**	**Se debe obtener a tiempo la información sobre las vulnerabilidades técnicas de los sistemas utilizados y evaluar la exposición de la organización a tales vulnerabilidades.** Para esto se requiere definir roles y responsabilidades de los que monitorean las vulnerabilidades, parchar correctamente los sistemas

Tabla 12: Dominio (9): Gestión de Incidentes en la Seguridad de la Información

DOMINIO (9): GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN		
OBJETIVOS DE CONTROL	**CONTROLES**	**EXTRACTO DEL CONTROL**
Notificación de eventos y debilidades de la seguridad de la información Asegurar que los eventos y debilidades en la seguridad de la información sean comunicados de una manera que permita realizar una acción correctiva a tiempo	**Notificación de los eventos de seguridad de la información**	**Los eventos en la seguridad de información deben ser reportados lo más rápido posible a través de una gestión de canales apropiados. Se debe establecer respuestas a incidencias y procedimientos de escalada, puntos de contacto para el reporte de eventos**, entrega de respuestas adecuadas y a tiempo por parte del punto de contacto
	Notificación de puntos débiles en la seguridad de información	**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.**
Gestión de incidentes y mejoras en la seguridad de la información Asegurar un alcance consistente y efectivo aplicado a la gestión de incidentes en la seguridad de la información. Procesos de mejora continua deben ser aplicados en respuesta al monitoreo, evaluación y gestión de los incidentes	**Responsabilidades y procedimientos**	**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 la información**
	Aprendiendo de los incidentes en la seguridad de la información	**Debe existir un mecanismo que permita que los tipos, volúmenes y costos de los incidentes en la seguridad de la información sean cuantificados y monitoreados**
	Recopilación de evidencias	**Cuando una acción de seguimiento contra una persona u organización, después de un incidente en la seguridad de la información implique acción legal o civil, la evidencia debe ser recolectada, retenida y presentada para estar conforme con las reglas para colocación de evidencia en la jurisdicción relevante**

Tabla 13: Dominio (10): Gestión de la Continuidad del Negocio

DOMINIO (10): GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO		
OBJETIVOS DE CONTROL	CONTROLES	EXTRACTO DEL CONTROL
Aspectos de la gestión de la continuidad del negocio Reaccionar a la interrupción de actividades del negocio y proteger sus procesos críticos frente a grandes fallos de los sistemas de información o desastres naturales o fallas de equipos. Los procesos de gestión de continuidad deben tener controles preventivos y de recuperación, identificando procesos críticos del negocio, generando planes de contingencias para asegurar que los procesos del negocio se puedan restaurar en plazos requeridos por la organización.	**Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio**	**Se debe instalar en toda la organización un proceso de gestión para el desarrollo y el mantenimiento de la continuidad del negocio que trate los requerimientos en la seguridad de información necesarios para la continuidad del negocio. Se debe concientizar y comprender los riesgos que la organización corre desde el punto de vista de su vulnerabilidad e impacto que tendrían la interrupciones en el negocio, se debe identificar todos los activos implicados en los procesos críticos del negocio**, identificar controles adicionales de prevención, probar y actualizar regularmente los planes y procesos instalados
	Continuidad del negocio y evaluación de riesgos	**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 la información.** La evaluación debe identificar, cuantificar y priorizar los riesgos, definir el impacto de las interrupciones, tiempos permisibles de interrupción y prioridades de recuperación
	Desarrollo e implantación de planes de continuidad que incluyen la seguridad de la información	**Se debe 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 falla de sus procesos críticos. Se debe identificar los procesos de emergencia y acuerdos de todas las responsabilidades**, la identificación de las pérdidas aceptables de información y servicios. Los planes de gestión de crisis deben ser diferentes de la gestión de continuidad del negocio.
	Marco de planificación para la continuidad del negocio	**Se debe mantener un esquema único de planes de continuidad del negocio para asegurar que dichos planes sean consistentes para tratar los requisitos de seguridad y para identificar prioridades de prueba y mantenimiento. Se deben aclarar alcances para la continuidad, condiciones para su activación y responsables de ejecutar cada etapa del plan**, se debe tener un calendario de mantenimiento y un calendario de cómo y cuándo se harán las pruebas del plan
	Pruebas, mantenimiento y revaluación de planes de continuidad	Los planes de continuidad del negocio se deben probar **regularmente para asegurarse de su actualización y eficacia**. Asegurarse de que todos los miembros del equipo de recuperación y personal relevante estén prevenidos de los planes y de sus responsabilidades para la continuidad del negocio

Tabla 14: Dominio (11): Cumplimiento

DOMINIO (11): CUMPLIMIENTO		
OBJETIVOS DE CONTROL	CONTROLES	EXTRACTO DEL CONTROL
Cumplimiento de los requisitos legales Evitar los incumplimientos de cualquier ley civil o penal, requisito reglamentario, regulación u obligación contractual y de todo requisito de seguridad por parte del personal de la organización	**Identificación de la legislación aplicable**	**Se debe definir, documentar y mantener actualizado de forma explícita todos los requisitos legales, regulatorios y contractuales que sean importantes para cada sistema de información**
	Derechos de propiedad intelectual (DPI)	**Se debe implantar los procedimientos apropiados para asegurar el cumplimiento de las restricciones legales, reguladores y contractuales sobre el uso del material protegido por derechos de propiedad intelectual y sobre el uso de productos de software propietario**
	Salvaguarda (Protección) de los registros y documentos de la organización	**Se debe proteger los registros importantes de la organización (contables, bases de datos, transacciones, auditoría, operativos) frente a su pérdida, destrucción y falsificación en concordancia con los requisitos regulatorios, contractuales y de negocio**
	Protección de los datos y privacidad de la información de carácter personal	**La protección de datos y privacidad de la información personal debe ser asegurada como se requiere en la legislación y en las regulaciones, implementando una política organizacional que debe ser comunicada a todo el personal de la organización**
	Prevención en el mal uso de los recursos de tratamiento de la información	**El personal debe ser disuadido de utilizar los recursos de tratamiento de la información para propósitos no autorizados o que estén fuera de los fines del negocio, se deben implementar acciones disciplinarias y/o legales apropiadas, los usuarios deben conocer el alcance del acceso qeu se les permite y del monitoreo que se lleva acabo para detectar un uso no autorizado**
	Regulación de los controles criptográficos	**Los controles criptográficos deben ser utilizados en conformidad con todos los acuerdos, leyes y regulaciones**
Cumplimiento de la políticas y normas de seguridad y cumplimiento técnico Asegurar la conformidad de los sistemas con las políticas y normas de seguridad mediante revisiones regulares	**Cumplimiento de las políticas y estándares de seguridad**	**Los gerentes deben asegurarse que se cumplan correctamente todos los procedimientos de seguridad dentro de su área de responsabilidad cumpliendo las políticas y estándares de seguridad, si se encuentran no conformidades se debe determinar las causas de no conformidad**, evaluar las acciones para asegurar que la no conformidad no vuelva a ocurrir, implementar acciones correctivas y revisar la acción correctiva que se realizó
	Comprobación del cumplimiento técnico	**Se debe comprobar regularmente el cumplimiento de las normas de implantación de la seguridad en los sistemas de información.** Esta debe ser realizada manualmente por un ingeniero competente y experimentado o automáticamente por un paquete informático que genere reporte técnicos para ser intepretados posteriormente por el experto
Consideraciones sobre la auditoria de sistemas Maximizar la efectividad y minimizar las interferencias en el proceso de autidoria de sistemas	**Controles de auditoria de sistemas**	**Se debe planificar y acordarse los requisitos y actividades de auditoria que impliquen comprobaciones en los sistemas operativos, para minimizar el riesgo de interrupción de los procesos de negocio**
	Protección de las herramientas de auditoria de los sistemas de información	**Se debe proteger los accesos a las herramientas de auditoria de sistemas con el fin de prever cualquier posible mal uso o daño**. Estas herramientas deben estar separadas de los sistemas de producción y desarrollo y no se mantendrán en librerías de cintas o en áreas de los usuarios

2.12. Limitaciones de la ISO/IEC 27002

Las posibles causas o limitaciones que se tiene cuando se desea implementar un estándar o norma internacional es: creer que el responsable de la seguridad informática solamente es un nombre en un papel y no de cada usuario que tiene acceso a la tecnología, esta es sin lugar a duda el elemento clave dentro de la disciplina laboral y de convivencia con las normas internacionales.

Sin embargo, se consideran otras causas por las cuales las organizaciones no pueden implementar la norma de seguridad, es de suma importancia tomar en consideración que estos causales no son menos importantes que la descrita anteriormente:

- El temor al cambio, que no es más que la resistencia de las personas para mejorar sus procedimientos de procesar información.
- El tiempo excesivo que toma la implantación de la norma, obligando a la desmotivación del personal y al alejamiento de los objetivos iniciales.
- Las discrepancias que existen en los puestos de Dirección.
- La delegación de toda la responsabilidad a los departamentos técnicos.
- El pensar que la seguridad de la información es innato a los procesos del negocio.
- El no poder cumplir un calendario de revisiones técnicas con todos los involucrados.
- Un incongruente análisis de riesgo de la institución frente a la seguridad informática.
- Definición poco clara del alcance a implementar la norma.

2.13. Empresas certificadas ISO/IEC 27001 en Ecuador

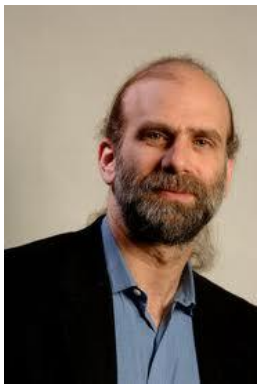
De acuerdo a la revista de tecnología PCWORLD, la operadora de tecnología celular, Telefónica Movistar Ecuador, recibió de la AENOR10 , la certificación del “Sistema de gestión de Seguridad de la Información bajo la norma ISO 27001”, la cual tiene relación con la provisión y soporte del servicio de datos fijos e internet dedicado, para el segmento de grande empresas.

Según la revista, a la operadora de telefonía celular, Movistar, le tomo aproximadamente un año el proceso de implementación de los requisitos para lograr esta certificación. El proceso concluyó en febrero de este año (2012), con la validación de la auditoría externa realizada por parte de AENOR. (PCWorld, 2012)

Otra de las empresas reconocidas como líder en el mercado tecnológico es TELCONET, la misma que se ha convertido en el primer proveedor de servicios, en Ecuador, con una Certificación ISO 27001 de Seguridad de la Información; alcanzada en el año 2008. (Telconet, 2012)

[10] Asociación Española de Normalización y Certificación

“Si piensas que la tecnología puede solucionar tus problemas de seguridad, está claro que ni entiendes los problemas, ni entiendes la tecnología.” Bruce Schneier



3. CAPÍTULO III – SITUACIÓN ACTUAL DE SEGURIDAD DE LA INFORMACIÓN EN LA ESPE

3.1. Definición de la ESPE

La ESPE es una institución de educación superior, con domicilio en la ciudad de Quito y sede principal en la ciudad de Sangolquí; se rige por la Constitución Política de la República del Ecuador. La Escuela Politécnica del Ejército está reconocida por el Sistema Nacional de Educación Superior como una Universidad clase “A”.

La ESPE dirige sus esfuerzos al mejoramiento de las condiciones de vida del país y a impulsar su desarrollo. El hecho de ser una institución educativa pluralista y abierta al pensamiento, sin discrimen de ninguna naturaleza, le ha permitido ganarse el favor de la juventud ecuatoriana sedienta de educación. Desde su creación en 1922, ha propiciado una permanente diversificación en su oferta educativa, dando oportunidad a que cada vez mayores sectores de la población ecuatoriana eleven su condición personal mediante el estudio y aporten al progreso de su comunidad. (ESPE)

3.1.1. Misión

Formar profesionales e investigadores de excelencia, creativos, humanistas, con capacidad de liderazgo, pensamiento crítico y alta conciencia ciudadana; generar, aplicar y difundir el conocimiento y proporcionar e implantar alternativas de solución a los problemas de la colectividad, para promover el desarrollo integral del Ecuador.

3.1.2. Visión

La Visión al 2012 es: Líder en la gestión del conocimiento y de la tecnología en el Sistema Nacional de Educación Superior, con reconocimiento en América Latina y referente de práctica de valores éticos, cívicos y de servicio a la sociedad.

3.1.3. Principios filosóficos

La Escuela Politécnica del Ejército conduce y desarrolla sus eventos y procesos mediante los siguientes principios:

- ✓ La Institución se debe fundamentalmente a la nación ecuatoriana; a ella orienta todo su esfuerzo contribuyendo a la solución de sus problemas mediante la formación profesional y técnica de los miembros de su población.
- ✓ Es una Institución abierta a todas las corrientes del pensamiento universal, sin proselitismo político ni religioso.
- ✓ La búsqueda permanente de la excelencia a través de la práctica de la cultura de la calidad en todos sus actos.
- ✓ La formación consciente, participativa y crítica con libertad académica y rigor científico, que comprenda y respete los derechos fundamentales del ser humano y de la comunidad.
- ✓ El cultivo de valores morales, éticos y cívicos, respetando los derechos humanos con profunda conciencia ciudadana; coadyuva a la búsqueda de la verdad y forma hombres de honor, libres y disciplinados.
- ✓ El mantenimiento de las bases históricas de la identidad nacional para incrementar el orgullo de lo que somos y así proyectamos al futuro.
- ✓ La conservación, defensa y cuidado del medio ambiente y el racional aprovechamiento de los recursos naturales; y,

- ✓ La práctica de los valores tradicionales de orden, disciplina, lealtad, justicia, gratitud y respeto, en el contexto de la responsabilidad, la honestidad, el autocontrol, la creatividad, el espíritu democrático, la solidaridad y la solución de los problemas mediante el diálogo y la razón.

3.1.4. Estructura organizacional

La ESPE mantiene una estructura orgánica, en la cual militares de la Fuerza Terrestre y de Aviación mantienen las diversas direcciones, en la siguiente figura se muestra la estructura orgánica vigente en la ESPE. (SGC)

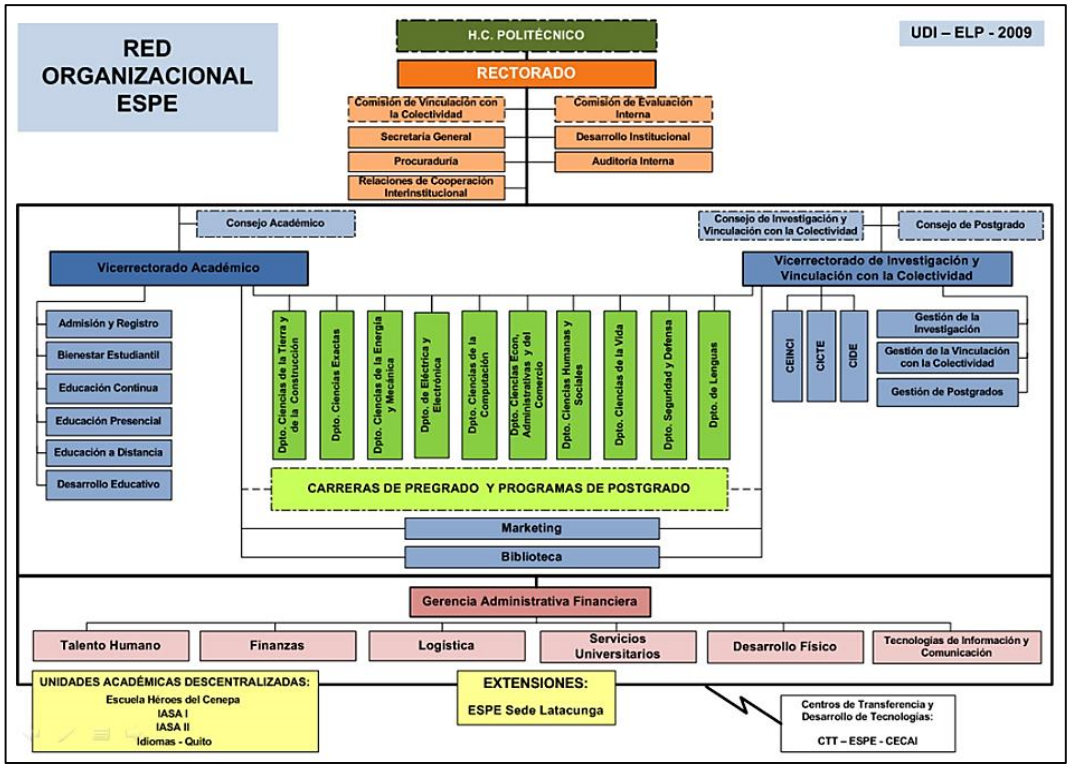


Figura 10: Red Organizacional ESPE

3.1.5. Política general

La ESPE mantiene una política general para su desarrollo. Orientar el esfuerzo institucional en forma sinérgica y participativa, hacia la modernización integral, que permita alcanzar la excelencia académica y organizacional.

3.1.6. Sedes académicas

El considerables crecimiento de la ESPE, gracias a la acogida que ha tenido en la población ecuatoriana por mucho tiempo ha provocado el crecimiento de la infraestructura materializando su experiencia en cinco nuevas filiales, las cuales son las de Latacunga, Escuela de Ciencias Agropecuarias en Sangolqui y en la ciudad de Santo Domingo de los Tsáchilas, Héroes del Cenepa en Quito e Instituto de Idiomas, también en la capital.

Estas filiales o centros de estudios descentralizados se respaldan en los mismos patrones de organización académica y administrativa de la sede matriz, las cinco dependencias forman profesionalmente redondeando aproximadamente veinte mil jóvenes ecuatorianos en las más diversas áreas del saber y la técnica, contribuyendo de esta manera al desarrollo del país a través de un recurso humano solventemente preparado. A continuación se enuncian las cinco filiales descentralizadas de la ESPE:

ESPE Latacunga: La ESPE Extensión Latacunga se encuentra ubicada en la provincia de Cotopaxi, cantón Latacunga, en la zona central del país. Es un establecimiento de educación superior, líder en la zona central del país, creado en junio de 1984, ofrece a la juventud carreras profesionales de excelente futuro laboral y económico.

Departamento de Lenguas (Quito): El 26 de Febrero de 1960 en la Comandancia General del Ejército, se constituye el Departamento de Inglés. Es una extensión académica enrumbada al servicio de la comunidad ecuatoriana en el quehacer del conocimiento de idiomas extranjeros, consolidando el manejo de básico de comunicación; comunicación, comprensión y expresión tanto oral como escrita desde una perspectiva esencialmente practica y aplicando en la medida de los posible el marco de las relaciones interpersonales y profesionales en sus dos modalidades presencial y a distancia, formando profesionales en el campo de la lingüística, la enseñanza y áreas afines al idioma Inglés.

Escuela de Tecnologías Héroes del Cenepa (Quito): Esta extensión fue creada para satisfacer la demanda de carreras cortas, a nivel de tecnologías, en áreas no explotadas profesionalmente, formando profesionales competitivos y comprometidos con el desarrollo de su comunidad.

Instituto de Ciencias Agropecuarias – IASA I (Sangolquí): Inicio sus actividades desde el 4 Febrero de 1992, fue creada bajo la iniciativa del General de División Carlomagno Andrade Paredes, quien diseñó el proyecto como un centro alternativo integral de formación superior agropecuario, que combine la seriedad, credibilidad y otros valores de las Fuerzas Armadas, con las experiencias educativas nacionales e internacionales, y forme profesionales competentes e integrales que contribuyan a la solución de los problemas del agro, generando progreso social y crecimiento económico para el país.

Instituto de Ciencias Agropecuarias – IASA II (Santo Domingo de los Tsáchilas): La Carrera de Ingeniería en Ciencias Agropecuarias Santo Domingo (IASA II), es una Carrera creada mediante convenios firmados entre el CONSEP – NAG, en al año de 1999. Extensión nueva de la ESPE que se encuentra ubicada en la provincia de Santo Domingo de los Tsáchilas. Es una institución entregada a

la formación del recurso humano que el campo necesita para su desarrollo y para generar trabajo y riqueza en beneficio de la comunidad.

En el Anexo 1 se muestra la cantidad de estudiantes que pertenecen a cada una de las carreras que ofrece la ESPE a la sociedad. Los datos obtenidos son de los dos últimos períodos académicos Septiembre 2011 – Febrero 2012 y Marzo 2012 – Agosto 2012.

Anexo 1: Numérico de Estudiantes por Carrera y Extensión.

3.1.7. Estrategia general

La ESPE se basa en la siguiente estrategia: Innovar y mejorar continuamente los procesos institucionales, trabajando proactivamente y en equipo. Esta estrategia ha permitido a la institución ser vista como un sistema, el cual se lo representa en la siguiente figura.

Figura 11: Sistema Valor de la ESPE

3.1.8. Carreras que oferta la ESPE

3.1.9. Pregrado

- ✓ Ingeniería Mecánica
- ✓ Ingeniería Electrónica en Telecomunicaciones
- ✓ Ingeniería Electrónica en Redes y Comunicación de Datos
- ✓ Ingeniería Electrónica en Automatización y Control
- ✓ Ingeniería Mecatrónica
- ✓ Ingeniería de Sistemas de Computación e Informática
- ✓ Ingeniería en Biotecnología
- ✓ Ingeniería Civil
- ✓ Ingeniería Geográfica y del Medio Ambiente
- ✓ Ingeniería en Comercio Exterior y Negociación Internacional

- ✓ Ciencias de la Educación
- ✓ Ciencias Económicas Administrativas y de Comercio
- ✓ Ciencias Agropecuarias IASA
- ✓ Ciencia Militares
- ✓ Licenciatura en Ciencias de la Actividad Física Deportes y Recreación
- ✓ Ingeniería en Seguridad

3.1.10. Postgrado

- ✓ Maestría en Ciencias Electrónicas
- ✓ Maestría en Sistemas de Gestión Ambiental
- ✓ Maestría en Ingeniería de Software
- ✓ Maestría Internacional en Administración de Empresas
- ✓ Maestría en Redes de Información y Conectividad
- ✓ Maestría en Gerencia de Sistemas
- ✓ Maestría en Docencia Universitaria
- ✓ Maestría en Gestión de la Calidad y Productividad
- ✓ Maestría en Gerencia de la Seguridad y Riesgos
- ✓ Maestría en Gerencia de Redes y Telecomunicaciones
- ✓ Maestría en Administración Gerencial Hospitalaria
- ✓ Maestría en Planificación y Dirección Estratégica
- ✓ Maestría en Gestión de Empresas
- ✓ Maestría en Agricultura Sostenible
- ✓ Maestría en Entrenamiento Deportivo
- ✓ Maestría en Evaluación y Auditoría de Sistemas Tecnológicos
- ✓ Diplomado en Gestión Directiva
- ✓ Diplomado Superior en Gestión de Proyectos
- ✓ Diplomado en Gestión para el Aprendizaje
- ✓ Diplomado en Prospectiva Estratégica

- ✓ Diplomado en Metodología de la Investigación Científica

3.2. Definición de la UTIC

La Unidad de Tecnologías de la Información y Comunicaciones administra los recursos tecnológicos requeridos por la Institución para el manejo de la información y mantener una adecuada comunicación, para lo cual ejecuta los procesos de gestión estratégica de la tecnología informática; de soporte técnico; de administración de redes y comunicaciones; de desarrollo, implantación y mantenimiento de aplicativos; y, de administración de software.

La Unidad de Tecnologías de la Información es responsable de:

- ✓ Realizar la gestión estratégica de la tecnología informática;
- ✓ Dar soporte técnico en el ámbito de aplicación que corresponde;
- ✓ Administrar las redes y las comunicaciones;
- ✓ Desarrollar, implantar y mantener los aplicativos;
- ✓ Administrar los aplicativos y bases de datos;
- ✓ Proporcionar seguridad a la información de servidores; y,
- ✓ Cumplir la normatividad institucional y las resoluciones emitidas por los órganos competentes.

3.2.1. Objetivo de la UTIC

Asegurar la disponibilidad, actualización tecnológica, innovación y operación de los recursos y servicios TIC´s, para alcanzar un alto novel de Tecnología con estándares de calidad acorde con las exigencias Institucionales.

3.2.2. Estructura organizacional

Actualmente la UTIC mantiene la estructura organizacional que se muestra en la siguiente figura:

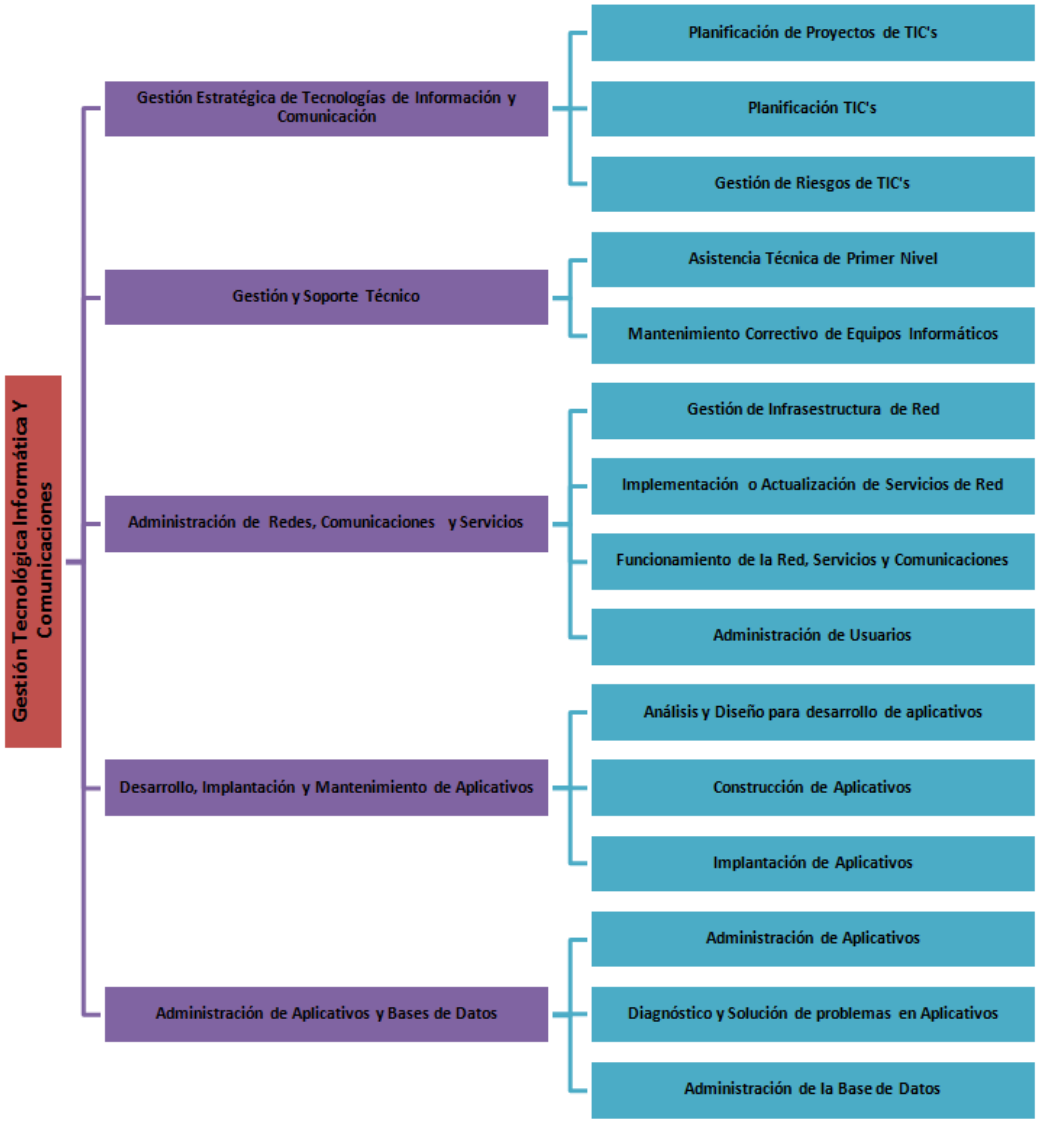


Figura 12: Estructura Organizacional de la UTIC

3.2.3. Catálogo de servicios de la UTIC

En la siguiente tabla se muestra el catálogo de servicios con los que la UTIC cuenta actualmente, los ítems pintados con color azul son los servicios correspondientes a las áreas de Administración de Aplicativos y Base de Datos y, Administración de Servicios de Redes y Comunicaciones, objeto de esta investigación.

Tabla 15: Catálogo de Servicios de la UTIC

CATÁLOGO DE SERVICIOS DE LA UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN		
ORD	DESCRIPCIÓN	ÁREA RESPONSABLE
1	Sistema de Gestión Académica de Pregrados	ADMINISTRACIÓN DE APLICATIVOS Y BASES DE DATOS
2	Sistema de Gestión Académica de Postgrados	ADMINISTRACIÓN DE APLICATIVOS Y BASES DE DATOS
3	Sistema de Gestión Administrativa Financiero	ADMINISTRACIÓN DE APLICATIVOS Y BASES DE DATOS
4	Sistema de Gestión Investigaciones	ADMINISTRACIÓN DE APLICATIVOS Y BASES DE DATOS
5	Asistencia/Asesoría Técnica en Desarrollo de Redes y Comunicación	ADMINISTRACIÓN DE SERVICIOS DE REDES Y COMUNICACIONES
6	Red LAN	ADMINISTRACIÓN DE SERVICIOS DE REDES Y COMUNICACIONES
7	Red WAN	ADMINISTRACIÓN DE SERVICIOS DE REDES Y COMUNICACIONES
8	Red Inalámbrica	ADMINISTRACIÓN DE SERVICIOS DE REDES Y COMUNICACIONES
9	Acceso Internet	ADMINISTRACIÓN DE SERVICIOS DE REDES Y COMUNICACIONES
10	Acceso Internet Avanzado (CEDIA)	ADMINISTRACIÓN DE SERVICIOS DE REDES Y COMUNICACIONES
11	Correo Electrónico	ADMINISTRACIÓN DE SERVICIOS DE REDES Y COMUNICACIONES
12	Administración de Usuarios	ADMINISTRACIÓN DE SERVICIOS DE REDES Y COMUNICACIONES
13	Comunicaciones de voz (VoIP / Mode)	ADMINISTRACIÓN DE SERVICIOS DE REDES Y COMUNICACIONES
14	Repositorio de Archivos (FTP)	ADMINISTRACIÓN DE SERVICIOS DE REDES Y COMUNICACIONES
15	Videoconferencias	ADMINISTRACIÓN DE SERVICIOS DE REDES Y COMUNICACIONES
16	Housing	ADMINISTRACIÓN DE SERVICIOS DE REDES Y COMUNICACIONES
17	Asistencia/Asesoría Técnica en Desarrollo de Sistemas de Información	DESARROLLO, IMPLANTACIÓN Y MANTENIMIENTO DE APLICATIVOS
18	Portal de Servicios Institucionales (MIESPE)	DESARROLLO, IMPLANTACIÓN Y MANTENIMIENTO DE APLICATIVOS
19	Portal Web Institucional / Micrositios	DESARROLLO, IMPLANTACIÓN Y MANTENIMIENTO DE APLICATIVOS
20	Desarrollo de Sistemas y Aplicaciones Institucionales	DESARROLLO, IMPLANTACIÓN Y MANTENIMIENTO DE APLICATIVOS
21	Asistencia/Asesoría Técnica Primer Nivel / Gestión de incidencias	GESTIÓN DE SOPORTE TÉCNICO
22	Mantenimiento Preventivo de equipos informáticos de la ESPE	GESTIÓN DE SOPORTE TÉCNICO
23	Mantenimiento Correctivo de equipos informáticos de la ESPE	GESTIÓN DE SOPORTE TÉCNICO
24	Asesoría Técnica en Adquisiciones de equipos TIC´s	GESTIÓN ESTRATÉGICA DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

3.2.4. Matriz BCG de los servicios de la UTIC

En la siguiente tabla se presenta un análisis de la Matriz BCG del catálogo de servicios de las áreas Administración de Aplicativos y Base de Datos y, Administración de Servicios de Redes y Comunicaciones, con la finalidad de evaluar de forma gráfica los servicios que tienen mayor crecimiento y mayor demanda de uso por parte de la comunidad politécnica. Ésta matriz permite a la UTIC; identificar estrategias y planes de mejoramiento sobre el catálogo de

servicios a fin de satisfacer las necesidades que tienen los miembros de la comunidad politécnica.

Tabla 16: Matriz BCG de la UTIC

ALTO USO DEL SERVICIO		
DEBIL CRECIMIENTO DEL SERVICIO	CUADRANTE II	CUADRANTE I
	Red WAN	Red Inalámbrica
	Repositorio de Archivos (FTP)	Acceso Internet
	Videoconferencias	Correo Electrónico
	Mantenimiento de los Sistemas de Información de la ESPE	Creación y Administración de micrositios departamentales
	Portal Web Institucional / Micrositios	Comunicaciones de voz (VoIP / Mode)
	Mantenimiento de Portal Web Institucional	Sistema de Gestión Académica de Pregrados
	Desarrollo de Sistemas y Aplicaciones Institucionales	Sistema de Gestión Administrativa Financiero
	Soporte Técnico Primer Nivel (Sitio - teléfono - remoto - mail)	
	Administración de Antivirus Institucional	
	Mantenimiento Preventivo de equipos informáticos de la ESPE	
	Mantenimiento Correctivo de equipos informáticos de la ESPE	
	CUADRANTE IV	CUADRANTE III
	Red LAN	Sistema de Gestión Académica de Postgrados
	Administración de usuarios	Sistema de Gestión Investigaciones
		Sistemas de Gestión Investigaciones
		Asistencia/Asesoría Técnica en Desarrollo de Redes y Comunicación
		Acceso Internet Avanzado (CEDIA)
		Housing
		Asistencia/Asesoría Técnica en Desarrollo de Sistemas de Información
		Asesoría Técnica en Adquisiciones de equipos TIC´s
		Compras centralizadas de Recursos TIC's (PAC)
BAJO USO DEL SERVICIO		FUERTE CRECIMIENTO DEL SERVICIO

3.2.5. Cadena de valor de la UTIC

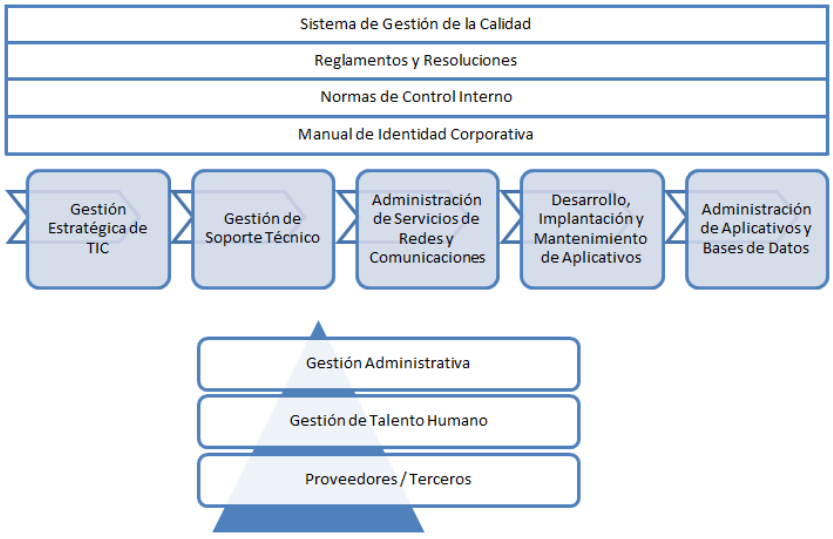


Figura 13: Cadena de Valor de la UTIC

Para el desarrollo de la presente investigación, no se tomado en consideración un análisis FODA de las políticas vigentes en la UTIC, debido a que se evalúa el contexto y su cumplimiento. Una vez terminada la tesis, se procederá a entregar a la Unidad de Tecnologías de la Información con la finalidad de analizar la factibilidad de implementación las políticas propuestas en esta investigación.

3.2.6. Unidad de desarrollo institucional de la ESPE

Es de suma relevancia considerar que la Unidad de Desarrollo Institucional es la encargada de ejecutar los procesos de planificación, evaluación y asesoramiento institucional para el cumplimiento de la misión y el logro de los objetivos estratégicos institucionales; y, coordinar la ejecución de actividades para el desarrollo de la ESPE. (Comisión de Elaboración ESPE, 2008)

3.2.6.1. Responsabilidades de la UDI

- ✓ Elaborar y actualizar el Plan Estratégico Institucional.
- ✓ Realizar el despliegue del Plan Estratégico Institucional.
- ✓ Coordinar y consolidar los planes Operativos Anuales vinculados al presupuesto.
- ✓ Evaluar el cumplimiento del Plan Estratégico y Planes Operativos.
- ✓ Coordinar el mejoramiento e innovación institucional.
- ✓ Asesorar en lo relacionado con la gestión institucional.
- ✓ Realizar la planificación presupuestaria anual, así como preparar las propuestas de modificaciones presupuestarias.
- ✓ Consolidar las necesidades de capacitación y perfeccionamiento del personal docente y administrativo y someterlas a aprobación del H. Consejo Politécnico.

- ✓ Cumplir con lo que se establezca en otras normas, reglamentos y resoluciones emitidas por los órganos competentes.

3.3. Análisis de las políticas de seguridad de la información vigente en la UTIC

El análisis de las políticas de seguridad de la información vigente en la UTIC se las desarrollo acorde a las buenas prácticas y sugerencias de OCTAVE. Para la visión gerencial de la UTIC, es imperioso contar con un Sistema de Gestión de Seguridad de la Información, en el cual se describan una serie de políticas, normas de carácter institucional y de cumplimiento obligatorio, para otorgar a la comunidad politécnica servicios de mejor calidad, y sobre todo que garanticen integridad, disponibilidad y confiabilidad en sus datos.

Actualmente, tanto la visión operativa como la de apoyo de la UTIC, coinciden en manifestar que la ESPE no posee una Sistema de Gestión de Seguridad de la Información, el cual vele por el activo más importante de la institución, los datos. Bajo este contexto, la UTIC no posee un plan maestro de seguridad de la información, en el cual se establezcan políticas estándares o procedimientos que establezcan las mejores prácticas para preservar y garantizar la integridad de la información.

Dado el análisis y la recopilación de la información, la UTIC posee dos documentos relacionados con estándares y políticas que rigen el área, estos son:

Anexo 2: Manual de Gestión de TI y Comunicaciones

Anexo 3: Plan de Contingencia de TI y Comunicaciones.

Estos documentos no se encuentran legalizados por la UDI[11], unidad encargada de la revisión, aprobación e inclusión de los documentos al proceso de gestión de la ESPE.

3.3.1. Manual de gestión de tecnologías de información y comunicaciones

Este documento describe una serie de políticas, normas de carácter institucional y de cumplimiento obligatorio, con la finalidad de otorgar la viabilidad adecuada en la administración de tecnología y alcanzar una mayor agilidad y eficiencia en el desarrollo de sistemas de tecnología y la automatización de procesos operativos.

De acuerdo al manual, la responsabilidad del cumplimiento recae directamente sobre todo el personal institucional; así como de terceros, que interactúen o accedan a información sensible, recursos tecnológicos y de comunicaciones de manera constante o eventual, para la ejecución de las actividades cotidianas.

Dado el objetivo de investigación de la presente tesis, es relevante mencionar que el manual de gestión de tecnologías de información y comunicaciones, se desarrolló con lineamientos a estándares internacionales como lo son:

- ✓ Buenas prácticas para la seguridad de la información ISO/IEC 27000
- ✓ Information Systems and Audit Control Association - ISACA, a través de su pronunciamiento en COBIT AUDIT GUIDELINES - COBIT: Control Objectives for Information and Related Technology.

[11] Unidad de Desarrollo Institucional

- ✓ Manual sobre Normas de Control Interno para el Área de Sistemas de Información Computarizados (Contraloría General del Estado).

El manual de gestión de tecnologías de información y comunicaciones, para facilidad de estudio fue divido en dos partes:

- ✓ Políticas de gestión de tecnologías de información y comunicaciones
- ✓ Políticas de uso de los servicios de tecnologías de información y comunicaciones

3.3.2. Políticas de gestión de tecnologías de información y comunicaciones

El objetivo es establecer las políticas que mayor relevancia tiene sobre el desarrollo de tecnologías de información y comunicaciones, así como para la optimización en la prestación de servicios TIC´s.

La responsabilidad del cumplimiento de estas políticas recae sobre todo el personal de servidores públicos y docente, que tengan relación con TI.

Entre las generalidades más sobresalientes de las políticas de gestión de tecnologías de información y comunicaciones se encuentran las siguientes:

- ✓ Las funciones del área de UTIC están separadas, la parte operativa y la gestión se alinea a la planificación estratégica institucional.
- ✓ La UTIC es responsable del diseño, transición, operación y control de los servicios de tecnología de información y comunicaciones.
- ✓ La adquisición de los sistemas de tecnologías de información, para todas las áreas administrativas, académicas, extensiones descentralizadas, centros de apoyo entre otros, es gestionado a través

de la UTIC, por lo tanto; la unidad solicitante deberá remitir un informe que justifique la necesidad.

- ✓ Los estudios preliminares de factibilidad, investigaciones y recomendaciones técnicas, es la base para la toma de decisiones sobre tecnologías de información y comunicaciones.
- ✓ Todo proyecto de TIC´s, debe ser aprobado por la autoridad correspondiente.
- ✓ La UTIC es la unidad encargada de la definición de tecnología, administración de la red de voz/datos y las aplicaciones institucionales existentes que están bajo su responsabilidad. Adicionalmente, participará en el proceso de adquisición de recursos de tecnología de información y comunicaciones (hardware, software, aplicaciones, infraestructura, servicios de TIC´s).

Con respecto al desarrollo e implementación de nuevas tecnologías de información, se manifiesta que la prioridad en el desarrollo de las aplicaciones institucionales responderá al impacto en el servicio que se otorga a los usuarios internos y externos, a las políticas y estrategias institucionales y la relación coste/beneficio.

Una nueva implementación o desarrollo será sujeto a verificación del análisis, diseño, estudio preliminar y de factibilidad correspondiente, según las normas que se encuentren establecidas por la Contraloría General del Estado y los respectivos estándares internacionales imputados. El proceso de desarrollo de sistemas de información se basa en la metodología que al menos comprenda las actividades descritas en el Manual sobre Normas Técnicas de Control Interno relativas a los Sistemas de Información, emitido por la Contraloría General del Estado.

Los mantenimientos y las actualizaciones de los sistemas de tecnología de información de la ESPE; se los realiza únicamente con técnicas probadas y actuales. La UTIC cuenta con mecanismos documentados de los cambios y ajustes efectuados. Sin embargo, no se ha verificado las evidencias que avalen un control de cambios sobre los sistemas de TI.

El punto 3.4 SEGURIDAD DE LA GESTIÓN del documento, indica sobre la responsabilidad de la UTIC en la elaboración, actualización, aprobación y divulgación del Plan de Contingencia de Tecnologías de la Información y Comunicación en cada uno de los niveles organizativos de TI.

Adicionalmente, se manifiesta que: las áreas que operen o administren las aplicaciones institucionales, deben mantener respaldos actualizados, así como software base y sus respectivos componentes. Para la mejora del desempeño de los funcionarios, la UTIC deberá formular un plan anual de capacitación de TI.

Finalmente, la UTIC es la unidad responsable del mantenimiento, actualización y renovación de todo equipo informático, por lo que se le faculta la autoridad para tomar decisiones sobre su estado.

3.3.3. Correo electrónico y de internet

Como un punto de suma importancia, dado el objeto de investigación de la presente tesis, se realizó un análisis minucioso sobre el uso de correo electrónico y acceso a las diferentes aplicaciones de internet, tomando como referencia el Manual de Gestión de Tecnologías de la Información y Comunicación.

Las políticas de uso de correo electrónico y de acceso a internet se aplican a todas y a cada una de las personas que forman parte de la comunidad politécnica y que tienen acceso a las diferentes aplicaciones institucionales.

3.3.4. Generalidades

Las medidas de seguridad son aplicables para todo el servicio de correo electrónico de usuarios internos y externos, tanto para su envío como para su recepción.

Las políticas de uso de correo electrónico y de acceso a internet se aplican a todas y a cada una de las personas que forman parte de la comunidad politécnica y que tienen acceso a las diferentes aplicaciones institucionales

Actualmente, las cuentas de correos electrónico de directivos, docentes, servidores públicos, estudiantes, entre otros; se encuentran creadas sobre la plataforma gratuita de Google; es decir, la institución hace uso de recursos tecnológicos disponibles en internet para brindar este servicio a la comunidad politécnica. Sin embargo, el correcto uso del correo electrónico se ajusta exclusivamente a las funciones que le competen a cada usuario; en virtud que el contenido de cada mensaje puede ser sujeto a monitoreo y conservación permanente por parte de la ESPE.

En el documento se hace referencia a que Auditoria Interna y el Administrador de Seguridad, previa autorización, accederán al contenido de un determinado correo electrónico ya sea de salida como de entrada. No obstante, la información no puede ser accedida ya que el servidor donde se almacenan los mensajes se encuentran físicamente en Google. Adicionalmente, de acuerdo a las reuniones mantenidas con las visiones de las áreas operativas, se evidenció que las actividades del técnico que administra la seguridad de la información son básicamente la obtención de respaldos de aplicaciones críticas de la institución, en tal virtud esta persona no posee las competencias necesarias para analizar el contenido de los mensajes de correo electrónico.

Al mantener el servidor de correo electrónico bajo la plataforma de Google, la implementación de una herramienta que permita la administración de mails “basura” o virus que circulan por la red no es factible, este control se lo realiza actualmente, de forma limitada a través de aplicaciones informáticas que son instaladas en los computadores personales de los usuarios.

3.3.5. Consideraciones para el acceso a información de internet

La principal consideración que deben poseer los miembros de la comunidad politécnica, es que el servicio de Internet es de uso exclusivo para las actividades y funciones que se desarrollan en la institución, por lo que es terminantemente prohibido utilizarse para uso personal o para algún otro fin.

La UTIC, con la finalidad de cumplir con esta mención, implementó sobre la red de datos servidores proxis, sobre los cuales se configuraron políticas de navegación, restringiendo a todos los usuarios el acceso a sitios y aplicaciones que se encuentren disponibles en el internet, sin embargo esta solución no dio los resultados esperados, ya que los usuarios encontraron técnicas para evitar esta políticas.

En el 2011, durante el proceso de análisis y recopilación de necesidades para la implementación de una nueva infraestructura de red y de seguridad, se consideró que la ESPE al ser una institución de educación superior y por ende de investigación, no era correcto la restricción de sitios, por tal motivo, se tomo la medida de habilitar el acceso a todo sitio, a excepción de páginas pornográficas, violencia, armas, drogadicción, entre otros. Actualmente, la UTIC controla este acceso a través de un equipo administrador de ancho de banda, el cual no restringe el acceso, limita la velocidad a un determinado sitio.

El personal de Redes y Comunicaciones, entre sus funciones, tiene la obligación de monitorear los accesos que realizan los usuarios a las diversas aplicaciones y sitios de internet a los que acceden los usuarios de la comunidad politécnica, esto a fin de asegurar el cumplimiento de las medidas de seguridad.

Dado lo descrito anteriormente, la restricción de privilegios a usuario se eliminó, en virtud de que todos los usuarios tienen el mismo perfil de navegación. Para finales del presente año, se estima realizar la diferenciación de funciones que tienen los usuarios dentro de la ESPE, es decir, se establecerán 5 perfiles: Directivos, Administrativos, Docentes, Estudiantes e Invitados, esto con el objetivo de segmentar el ancho de banda para acceder a una aplicación, tomando en consideración el perfil.

3.3.6. Licencia legales de software

Todo software, está protegido por el IEPI[12], en tal virtud se encuentra prohibida su reproducción o distribución total o parcial sin la autorización expresa de su fabricante. La UTIC, todo software que adquiera para su utilización en los equipos de tecnología de la información y comunicaciones, lo deberá realizar a nombre de la ESPE y debe contar obligatoriamente con una licencia legal.

A fin de precautelar esta norma y la seguridad de la información, la UTIC es el único ente responsable y autorizado para la instalación o eliminación de cualquier tipo de software en los equipos de la escuela, servidores y en cualquiera de los conectados a la red. Lastimosamente, este escrito no se cumple en su en su totalidad, debido a que existen departamentos académicos o unidades organizativas que este proceso lo realizan independientemente, sin previa autorización o coordinación con la UTIC. Todos los desarrollos que se realicen dentro de la ESPE; automáticamente su autoría pertenecen a la institución. Como

[12] Instituto Ecuatoriano de Propiedad Intelectual

complemento a lo mencionado es responsabilidad de la UTIC mantener el inventario de las licencias existentes, así como el responsable de su uso.

3.3.7. Generalidades de las políticas de uso de los recursos de tecnologías de la información y comunicaciones

Esta política tiene como fin, difundir a los miembros de la comunidad politécnica mejores prácticas para el uso eficiente de los recursos de tecnología de información y comunicaciones.

3.3.7.1. Uso del computador personal

Básicamente, lo que se recomienda en este enunciado, es precautelar el buen estado de los equipos informáticos a través de recomendaciones orientadas a las buenas prácticas en el manejo de equipos informáticos.

Entre las consideraciones más relevantes se encuentran: la introducción de unidades de almacenamiento en el computador personas, actualización periódica de los sistemas de prevención de virus, creación de claves con una complejidad difícil de descifrar, evitar la instalación de software sin autorización de la UTIC, entre otras.

Todas estas recomendaciones, permiten a los usuarios preservar su computador personal en condiciones normales y óptimas para la elaboración de sus actividades cotidianas, sin embargo, la información otorgada por personal técnico de HelpDesk de la UTIC, indica que todas estas recomendaciones no son acatadas por la gran mayoría de la comunidad politécnica debido a diferentes factores. Esta afirmación es evidenciable con el alto número de soportes en sitio o por el elevado número de computadores personales infectados de virus o daños de hardware que entran a Mantenimiento Técnico.

3.3.7.2. Usuarios del portal web

El objetivo de este punto, esta orientado a los estudiantes de la UED a fin de promover lineamientos adecuados para el envío de guías académicas, entre las principales consideraciones están el tamaño máximo así como su formato de compresión.

3.3.7.3. Uso de las cuentas de correo electrónico

Las políticas se encuentras diferenciadas en dos grupos, para estudiantes y para el personal directivo, docente y administrativo. Para objeto de estudio, se estableció un análisis general; ya que el correcto uso de este servicio es responsabilidad de todos los usuarios que forman parte de la comunidad politécnica. Adicionalmente, como se mencionó, la cuentas de correo electrónico se encuentran montadas sobre la plataforma Google, por lo que la diferenciación de estos grupos no es aplicable a la realidad actual.

Toda persona que ingresa a formar parte de la institución, tiene derecho a la obtención de su cuenta de correo electrónico para uso oficial y principalmente para la ejecución de las actividades netamente relacionadas con la institución.

Es responsabilidad de cada usuario el buen uso y de la información que se envíe o se reciba de cada cuenta de correo electrónico, por tal motivo, esta cuenta es personal e intransferible. La vigencia de las cuentas asignadas será definida por la Unidad de Tecnologías de la Información, con respecto al tamaño de almacenamiento, este es sujeto a la disponibilidad del recurso que Google entregue.

3.3.7.4. Uso del servicio de internet

La red de Datos de la ESPE tiene el objetivo de brindar de los mejores servicios a la comunidad politécnica con fines académicos y administrativos. El Internet, hoy en día es una herramienta tecnológica muy valiosa que debe ser usada con racionalidad y responsabilidad.

A fin de precautelar los recursos de Internet, la UTIC ha implementado un sistema de administración de ancho, en el que mediante políticas de calidad y descubrimiento de aplicaciones se asigna el recurso necesario para su acceso. Como política general, se tiene restringido el consumo de ancho de banda para buscadores de descargas de música, videos o archivos comerciales, acceso a páginas pornográficas, armas, violencia, drogas, entre otras.

Las actuales políticas descritas en este documento, no son aplicables, ya que fueron desarrolladas para el sistema antiguo de bloqueo de contenidos. Como se mencionó anteriormente, la ESPE utilizó hasta el 2011 servidores proxis, mediante los cuales se realizaba este filtrado, este cambio se realizó debido a la implementación de una infraestructura de mayor robustez que fue adquirida por la institución.

3.3.7.5. Uso de las licencias de software

Preservar la legitimidad del software es el fin del análisis de este punto, el proceso de nuevas herramientas se lo gestionará a través de la UTIC, no se entregarán a los usuarios el software original a los usuarios directamente.

3.3.7.6. Usos de otras aplicaciones de red (central telefónica y video conferencia)

La UTIC en su catálogo de servicios ofrece a la comunidad politécnica el sistema telefónico y el sistema de video conferencia, este último instalado a inicios del presente año.

Al igual que el servicio de correo electrónico, todo usuario que pertenezca a la institución tiene el derecho de recibir una clave para uso de llamadas telefónicas, la misma que es personal e intransferible; en virtud de que el consumo excesivo de este servicio será cobrado al responsable de la clave.

Los rubros de cobros son considerados de acuerdo al tipo de llamada (Local, Internacional o Celular), adicionalmente se contempla gastos administrativos como: proporcional de tiempo laboral, proporcional del mantenimiento de la central telefónica, entre otros.

Todo tipo de llamadas se encuentran temporizadas, la central telefónica bloqueará automáticamente las claves de los usuarios que excedan los tiempos establecidos previamente por la UTIC. Para que una clave telefónica sea nuevamente habilitada, los usuarios deberán cancelar los rubros, mencionados anteriormente.

La ESPE dispone de un Manual de Uso del Servicio Telefónico, en el cual se visualiza claramente las recomendaciones que deben seguir los usuarios para el correcto uso de este servicio de comunicaciones. Es importante destacar que estas políticas se encuentran en proceso de legalización.

Respecto al sistema de video conferencia, la ESPE, durante al año 2011 realizó la adquisición de un Sistema Integral de Video Conferencia, la misma que

ha permitido una mayor interactividad de las actividades técnicas, administrativas, de investigación y vinculación. La video conferencia es uno de los recursos de mayor potencialidad comunicativa, ya que se basa en la comunicación multimedia, misma que tiene una enorme similitud con contextos de comunicación presencial.

El sistema integral de videoconferencia, actualmente ofrece tecnología que fortalece la enseñanza virtual mediante la implementación de aulas, en donde se pueda asistir a clases en forma virtual, con contenidos en tiempo real o pregrabado, mediante sistema de grabación y streaming, con agendamiento y publicación en la WEB.

Paralelamente, la ESPE ha fortalecido mediante el sistema de video conferencia los canales de comunicación multimedia de sus autoridades, de tal forma que se pueda alternar entre la interacción presencial y virtual, a fin de coordinar las actividades gerenciales, técnicas y administrativas entre: Sedes, Extensiones, Unidades Descentralizadas y Campus ESPE.

En el mes de mayo del presente año, la UTIC elaboró el Manual de Uso del Sistema de Video Conferencia (Anexo 4), el cual ya ha sido legalizado por la máxima autoridad de la institución y ha sido difundido a través del correo electrónico para conocimiento y cumplimiento general de la comunidad politécnica.

Anexo 4: Manual de Uso del Sistema de Video Conferencia

3.3.8. Plan de contingencia de tecnologías de información y comunicaciones

El Plan de contingencia de Tecnologías de Información y Comunicaciones de la UTIC realizada en el año 2011 presenta un análisis de los posibles riesgos y desastres que podría sufrir el Data Center de la ESPE, asociando cada riesgo con

un nivel de criticidad, probabilidad de ocurrencia y el impacto que tendría; también muestra las acciones de las estrategias de emergencia y recuperación que deberán realizarse por parte del personal responsable para la continuidad del negocio.

Este plan se encuentra orientado directamente a evitar interrupciones que podría sufrir el Data Center y por consecuencia los servicios de red de la ESPE. Adicionalmente, busca minimizar los tiempos de restauración de los sistemas en caso de que algún problema o percance técnico se presente, esto con la finalidad de que la operatividad de los sistemas y los procesos de la Institución se encuentren en un 99% disponible y con un grado de seguridad razonable. Sin embargo, este documento muestra políticas o procedimientos referentes a la seguridad integral de los sistemas de información de manera general, en virtud de que se centran en el objetivo principal el cual es salvaguardar la integridad física de los activos del Data Center, eludiendo los principios de confidencialidad e integridad de la información.

La metodología usada en el plan de contingencias de la UTIC esta basada en la norma IRAM/ISO 17550 y esta constituido esencialmente de las siguientes partes:

- ✓ La identificación de los recursos que hay que proteger.
- ✓ La clasificación de los riesgos que podrían sufrir los recursos ligado al análisis de impacto y probabilidad de ocurrencia.
- ✓ Las fichas técnicas de contingencia.

3.3.8.1. Identificación de los recursos que hay que proteger

En el desarrollo de este punto se realizó un inventario de todos los actores y activos existentes que intervienen en el centro de datos institucional y se da una

prioridad según el grado de seguridad que requiere dicho elemento. Este inventario esta actualizado hasta el primer semestre del año 2011, por lo tanto a la fecha existen varios activos que no están mencionados. En la siguiente tabla se muestra un resumen de los puntos más importantes en cuanto a este inventario de recursos según el plan de contingencias vigente:

Tabla 17: Recursos existentes en la UTIC - Manual de Contingencias 2011

RECURSOS	ACTORES	IDENTIFICACIÓN	PRIORIDAD
Humano	Empleados Permanentes	Todo el personal que labora permanentemente en la UTIC (29 personas)	Alta
Dispositivos Informáticos	Hardware	30 Computadores personales	Media
		10 Laptops	Media
		20 Teléfonos IP	Baja
		4 Routers	Alta
		20 Servidores	Alta
		10 Swtichs	Alta
	Aplicativos	Sistema Académico en Power Builder	Baja
		Sistema Financiero Olympo en Visual Basic	Media
		Sistema Recursos Humanos en Power Builder	Baja
		Portal Web en Java	Alta
		Sistema de Educación Virtual plataforma Educativa	Alta
		Sistema ESPE MEDIC en Power Buider	Baja
		Sistema de Pedidos en Power Builder	Baja
		Sistema BANNER-ESPE en Oracle	Alta
	Base de Datos	SYBASE	Alta

		ORACLE	Alta
Servicios	Redes y Comunicaciones	Red WAN proveedor CNT	Alta
		Internet proveedor Global Crossing	Alta
		FTP proveedor ESPE	Baja
		Correo Electrónico Microsoft Exchange	Alta
		Telefónica proveedor CNT-ESPE	Alta
		Active Directory proveedor Microsoft	Alta
		DNS proveedor ESPE	Alta
		DHCP proveedor Microsoft	Alta
		Red Interna proveedor ESPE	Alta

3.3.8.2. Clasificación de los riesgos

La identificación y clasificación de los riesgos permitirán a la UTIC decidir cual puede ser la inversión razonable en seguridad frente a todos los posibles desastres que podrían afectar los recursos o activos existentes en el DataCenter de la ESPE. Esta clasificación fue desarrolla en función de la experiencia de los técnicos de la UTIC, mas no se realizo un estudio sistemático fundamentado en inspecciones técnicas especializadas en desastres, que valoren no solo los activos tangibles si no también los intangibles, tal es así que se enumeran riesgos improbables que no tengan validez o que no ocurran en un tiempo determinado.

Los tipos de riesgos identificados en el plan de contingencias con una probabilidad MEDIA de ocurrencia y de impacto son:

- ✓ Incendio, Erupción volcánica, terremoto.
- ✓ Robo físico de equipos, explosión.
- ✓ Ataques de Virus informáticos.
- ✓ Suspensión de la central telefónica.

- ✓ Suspensión del servicio de red.
- ✓ Daños físicos o lógicos de dispositivos de red.
- ✓ Daño del cableado estructurado.

Los tipos de riesgos identificados en el plan de contingencias con una probabilidad ALTA de ocurrencia y de impacto son:

- ✓ Falla del UPS del DataCenter.
- ✓ Falla del aire acondicionado.
- ✓ Daño físico de componentes o activos del DataCenter.

3.3.8.3. Fichas de contingencias

En esta última parte del plan de contingencia, se detallan las fichas técnicas a seguir en caso de ocurrencia de un desastre, es decir, son memorias técnicas de procedimientos a realizar en caso de que un evento de riesgo este ocurriendo. En estas fichas se encuentran especificados los síntomas que posiblemente presentan los servicios o los activos cuando aparece un desastre o riesgo, las acciones para volver operable el servicio, las posibles estrategias de prevención con el fin de que el desastre no ocurra nuevamente y las estrategias de emergencia y recuperación como una segunda posibilidad de recuperar el servicio lo más pronto posible.

Dado que en el Data Center de la ESPE existen varios servidores y equipos de comunicaciones en los cuales alojan diferentes tipos de servicios con diferentes administradores u operarios, en este punto del plan, también se enumeran varios manuales de apagado y encendido de los servidores, dispositivos de redes/comunicaciones y servicios críticos con el fin de que la persona que ejecuto la ficha de contingencia pueda apagar, inicializar o volver a

operar nuevamente el servicio interrumpido. Los manuales expuestos para levantar y bajar los servicios son:

- ✓ Proyecto ESPE Digital
- ✓ Portal Luminis
- ✓ Base de datos Sybase, Oracle, Tomcat
- ✓ Central telefónica
- ✓ Switch Core, Firewall, IPS, Administrador de ancho de banda, AAA
- ✓ Active Directory

Una vez realizado el análisis y levantamiento de información referenciados o disponibles en la UTIC, se debe mencionar que las políticas vigentes no cumplen con una normatividad formal que regulen el uso de los sistemas críticos y de las bases de datos institucionales, por lo que las visiones operativas y de apoyo que administran este servicio únicamente se basan en experiencia vividas para solventar o solucionar incidentes, afectando directamente con la disponibilidad, integridad y confiabilidad de los datos, principios básicos de la seguridad de la información.

3.3.9. Cuestionario de políticas de S-I[13]

Con la finalidad de recopilar información de acuerdo a la metodología planteada en la presente investigación, se elaboró un cuestionario el cual hace referencia a cada uno de los controles que recomienda la ISO/IEC 27002. El cuestionario fue enviado a través de correo electrónico a todo el personal de técnicos de la UTIC (29 personas). (Anexo 5)

Anexo 5: Cuestionario y Respuestas de Políticas de S-I de la UTIC

[13] S-I: Seguridad de la Información

3.3.10. Resultados del cuestionario de políticas de S-I

El cuestionario se encuentra enfocado a visualizar el nivel de cumplimiento que tiene la UTIC respecto a las mejores prácticas que recomienda la norma ISO/IEC 27002. La estructura de su elaboración contiene 11 Dominios y 37 Objetivos de Control.

No se ha considerado los objetivos de control de Teletrabajo y Comercio en Línea, en virtud de que no aplican actualmente a la ESPE. La tabulación de la información obtenida mantendrá la misma estructura, es decir; en función de 11 Dominios. El cuestionario fue contestado por el 45% de los profesionales que laboran en la UTIC.

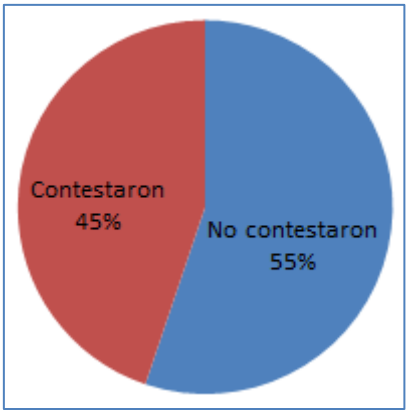


Ilustración 1: Nro. De Cuestionarios Contestados

DOMINIO 1: Política de seguridad

La **pregunta 1** afirma que el 85% de las profesionales mantiene un desconocimiento de una Política de Seguridad de la Información que haya sido aprobada, publicada y comunicada. El 15% hace referencia al Manual de Políticas

de UTIC y Plan de Seguridad de la Informática del 2005, sin embargo no se da a conocer la ubicación física y tampoco la frecuencia de su actualización.

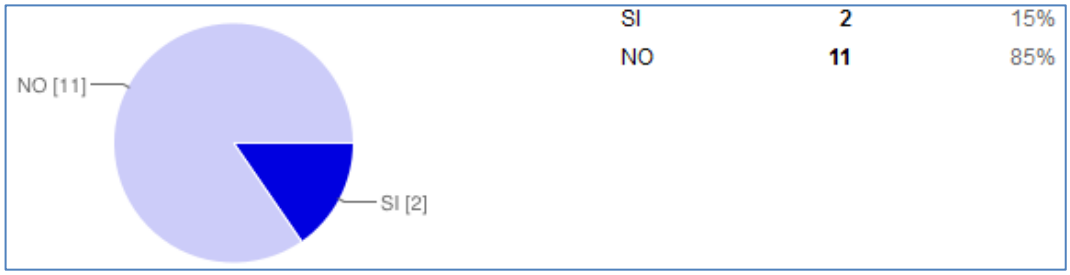


Ilustración 2: OC - Política de Seguridad de la Información

DOMINIO 2: Aspectos organizativos de la seguridad de la información

Los resultados de la **pregunta 2**, manifiestan lo siguiente:

- ✓ El 77% de las respuestas afirma que la asignación y reconocimiento de responsabilidades por parte de la funcionarios es el control que se aplica dentro de la UTIC en cuanto a S-I[14]
- ✓ El 2% dice que existen procesos adecuados de autorización cuando se incorporan nuevos recursos tecnológicos, el 5% referencia acuerdos de confidencialidad para proteger la información de la institución y finalmente el 6% afirma que existe un compromiso de la dirección para establecer controles de seguridad de la información.
- ✓ El 8% de las respuestas asegura que el control que se mantiene es el contacto con grupos especialistas en seguridad de la Información.

[14] S-I: Seguridad de la Información

Desconozco del tema	0	0%
Asignación y reconocimiento de responsabilidades por parte de los funcionarios	10	77%
Acuerdos de confidencialidad para proteger la información de la institución	5	38%
Contactos con grupos especialistas en Seguridad de la Información	1	8%
Procesos adecuados de autorización cuando se incorporan nuevos recursos tecnológicos	2	15%
Compromiso de la dirección	6	46%

Los usuarios pueden seleccionar más de una casilla de verificación, por lo que los porcentajes pueden superar el 100%.

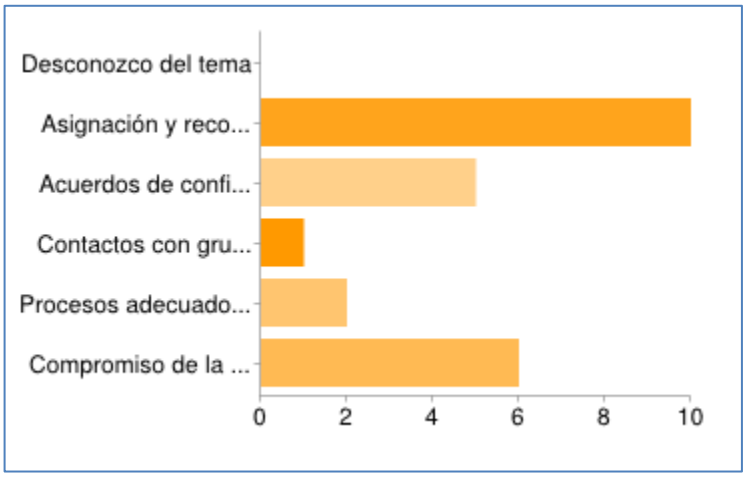


Ilustración 3: OC - Organización Interna

La **pregunta 3** muestra una similitud de criterios entre las personas que perciben un control Medio y Bajo para el acceso a todos los dispositivos de tratamiento de la información que tienen los proveedores o terceros cuando ingresan a la institución. Únicamente el 8% asegura que este control tiene un nivel alto.

Ilustración 4: OC - Seguridad en los accesos a Terceros

DOMINIO 3: Gestión de activos

La **pregunta 4** permite determinar la importancia que se le entrega a la gestión de los activos informáticos de la UTIC.

- Las respuestas obtenidas en el literal “a” de la pregunta 4, indica que el 62% de los consultados considera que la identificación clara de los activos mantiene un nivel de control medio. El 31% supone que el nivel de cumplimiento de este control es bajo y nuevamente el 8% afirma que se tiene identificados claramente los activos de la información.

Ilustración 5: OC - Responsabilidad sobre los activos (a)

- Las respuestas obtenidas en el literal “b” determinan que el 77% de los consultados son responsables del servicio y del correcto funcionamiento del activo. El 23% alega manifestando que el responsable del servicio únicamente se enfoca en garantizar el servicio más no del funcionamiento del activo.

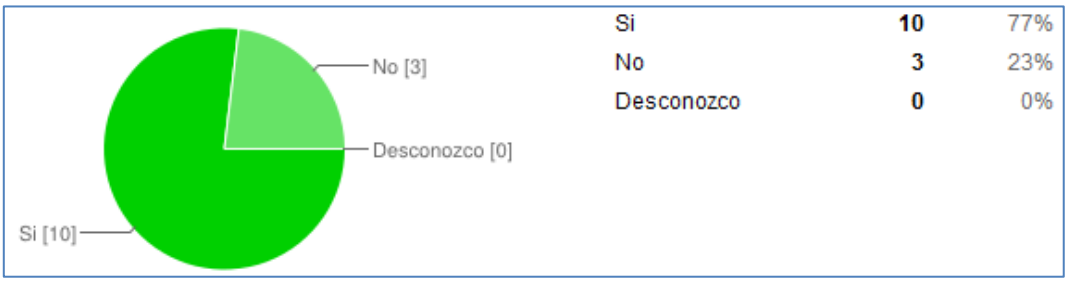


Ilustración 6: OC - Responsabilidad sobre los activos (b)

- El 100% de las respuestas obtenidas en el literal “c”, determinan la carencia de reglas y políticas para el uso adecuado de la información y de los activos asociados

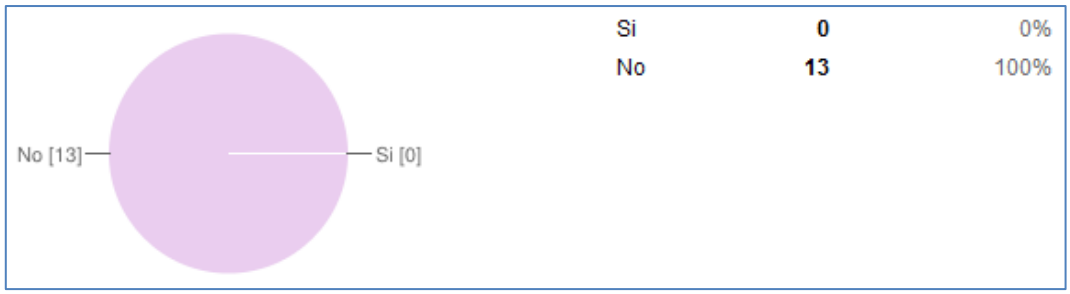


Ilustración 7: OC - Responsabilidad sobre los activos (c)

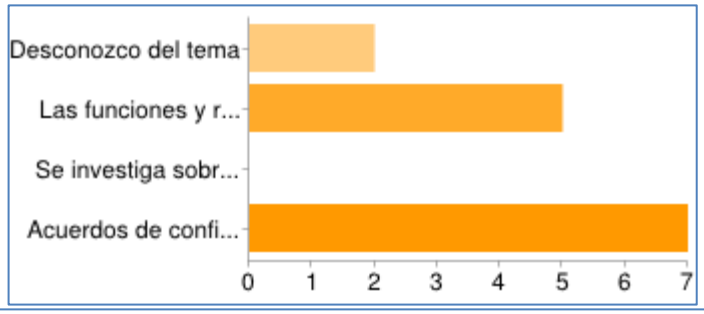
La **pregunta 5** muestra una paridad (46%) entre el grado de control bajo y medio concerniente a la clasificación adecuada de la información en función de su valor, requisitos legales, sensibilidad, criticidad, o procedimientos adecuados para manipular, almacenar, etiquetar, transmitir y destruir la información.

Ilustración 8: OC - Clasificación de la Información

DOMINIO 4: Seguridad ligada a los recursos humanos

Los resultados de la **pregunta 6**; respecto al hurto, fraude o mal uso de la información y de los activos informáticos de la institución se mitiga, en función al 54%, con acuerdos de confidencialidad en donde se indica la obligación contractual del empleado y la institución. Ninguno de los encuestados manifestó

que en la UTIC se investigan sobre los antecedentes legales y éticos de los proveedores, personal temporal o de planta.

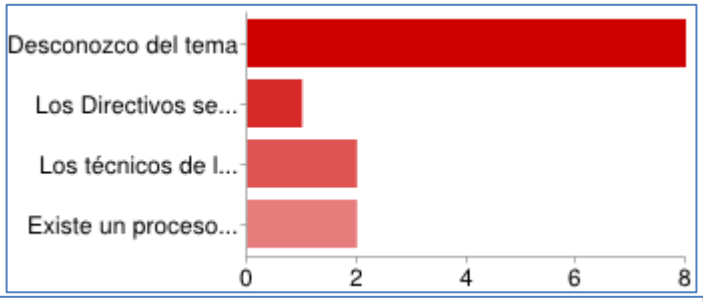


Desconozco del tema	2	15%
Las funciones y responsabilidades de los empleados y proveedores están definidas y documentadas	5	38%
Se investiga sobre los antecedentes legales y éticos de los candidatos que desean ingresar a la UTIC, de los proveedores y del personal temporal	0	0%
Acuerdos de confidencialidad en donde se indica la obligación contractual del empleado y la obligación de la Institución	7	54%

Los usuarios pueden seleccionar más de una casilla de verificación, por lo que los porcentajes pueden superar el 100%.

Ilustración 9: OC - Seguridad antes del Empleo

El 62% de las respuestas de la **pregunta 7** muestran una superioridad del desconocimiento del control que permite identificar las amenazas y riesgos que puede tener la seguridad de la información. Se evidencia una paridad del 15% entre los criterios que afirman que los técnicos de la UTIC reciben un entrenamiento apropiado en políticas y procedimientos organizacionales para la función de su trabajo y que existe un proceso formal disciplinario para empleados que han cometido una apertura en la seguridad o han violado alguna política de seguridad.

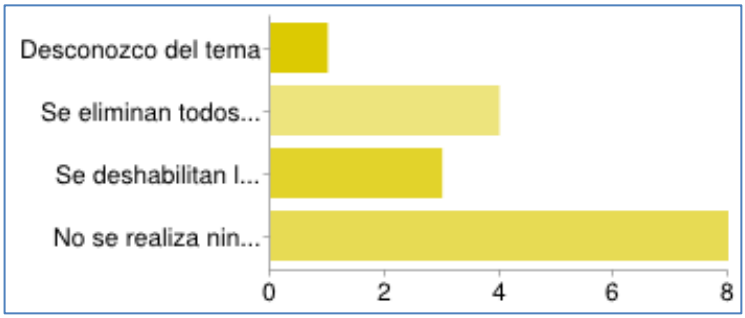


Desconozco del tema	8	62%
Los Directivos se preocupan por que sus técnicos tengan en claro sus responsabilidades, roles, estén motivados y capacitados en Seguridad de la Información.	1	8%
Los técnicos de la UTIC reciben un entrenamiento apropiado en políticas y procedimientos organizacionales para la función de su trabajo	2	15%
Existe un proceso formal disciplinario para empleados que han cometido una apertura en la seguridad o han violado alguna política de seguridad	2	15%

Los usuarios pueden seleccionar más de una casilla de verificación, por lo que los porcentajes pueden superar el 100%.

Ilustración 10: OC - Durante el Empleo

El 62% de los encuestados que respondieron a la **pregunta 8**, determina que cuando una persona o proveedor ha finalizado su contrato, ha cambiado sus funciones o ha cambiado sus responsabilidades no se realiza ninguna acción sobre los accesos y/o privilegios asignados por un tiempo indefinido



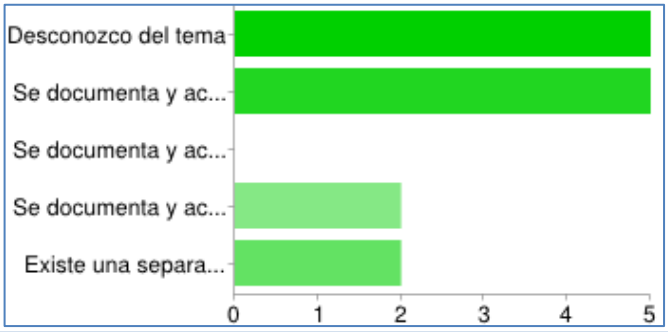
Desconozco del tema	1	8%
Se eliminan todos los privilegios y accesos asignados	4	31%
Se deshabilitan las cuentas de usuario	3	23%
No se realiza ninguna acción por un tiempo indefinido	8	62%

Los usuarios pueden seleccionar más de una casilla de verificación, por lo que los porcentajes pueden superar el 100%.

Ilustración 11: OC - Finalización del empleo o cambio de puesto de trabajo

DOMINIO 5: SEGURIDAD FÍSICA Y DEL ENTORNO

La **pregunta 9** evidencia una paridad del 38% entre el desconocimiento del tema y que se documenta y actualiza procedimientos de operación y se los pone a disposición de todos los usuarios que lo requieran. El 15% de los encuestados indica que se documenta y actualiza los servicios, reportes, reuniones, incidentes de los proveedores. El otro 15% manifiesta una separación de los recursos para las áreas de desarrollo, prueba y producción con el fin de reducir los riesgos de un acceso no autorizado o de cambios al sistema operacional.



Desconozco del tema	5	38%
Se documenta y actualiza procedimientos de operación (prendido-apagado de equipos, backups, mantenimiento y manipulación de los equipos críticos, etc.) y se los pone a disposición de todos los usuarios que lo requieran	5	38%
Se documenta y actualiza estrictamente los cambios en los sistemas informáticos, esto es: identificación, registro, evaluación del impacto, comunicación a involucrados, responsabilidad de abortar y recuperarse de los cambios sin éxito	0	0%
Se documenta y actualiza los servicios, reportes, reuniones, incidentes de los proveedores	2	15%
Existe una separación de los recursos para las áreas de desarrollo, prueba y producción con el fin de reducir los riesgos de un acceso no autorizado o de cambios al sistema operacional	2	15%

Los usuarios pueden seleccionar más de una casilla de verificación, por lo que los porcentajes pueden superar el 100%.

Ilustración 12: OC - Áreas Seguras

Pregunta 10, se identifica que los encuestados tienen diferentes percepciones sobre la seguridad de los equipos informáticos, los cuales deben estar protegidos de amenazas y se debería considerar una instalación alterna fuera de la ESPE en caso de emergencia. Sin embargo, 69% concuerda en que el DataCenter posee equipos de protección como generadores eléctricos, UPS, suministros de agua, aire acondicionado de precisión, los cuales son inspeccionados regularmente y probados apropiadamente para asegurar su funcionamiento.

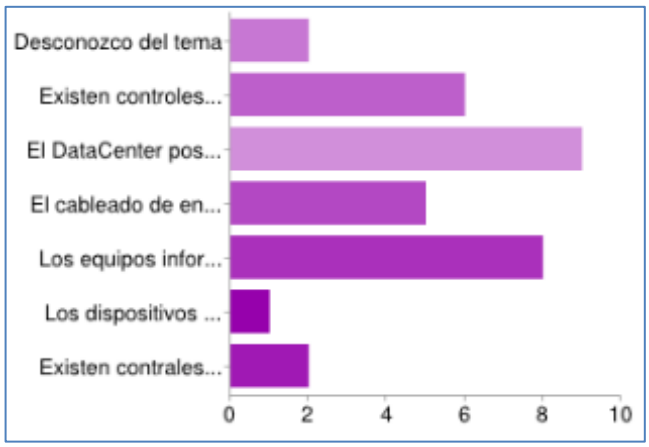
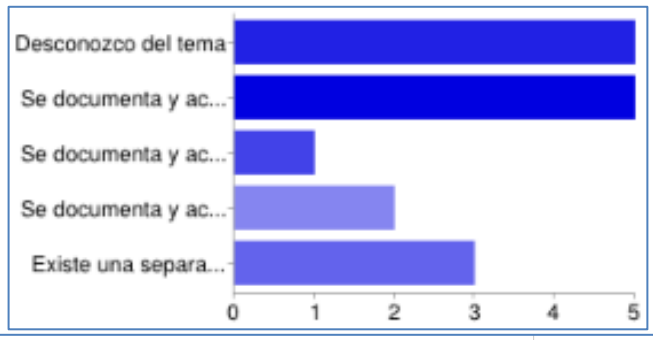


Ilustración 13: OC - Seguridad de los Equipos

DOMINIO 6: Gestión de comunicaciones y operaciones

Pregunta 11, el 38% de los encuestados afirma no conocer un control para garantizar la operación correcta y segura de los recursos de tratamiento de la información, otro 38% indica que se documenta y actualiza procedimientos de operación (prendido-apagado de equipos, backups, mantenimiento y manipulación de los equipos críticos, etc.) y se los pone a disposición de todos los usuarios que lo requieran. El 23% afirma que existe una separación de los recursos para las áreas de desarrollo, prueba y producción con el fin de reducir los riesgos de un acceso no autorizado o de cambios al sistema operacional.

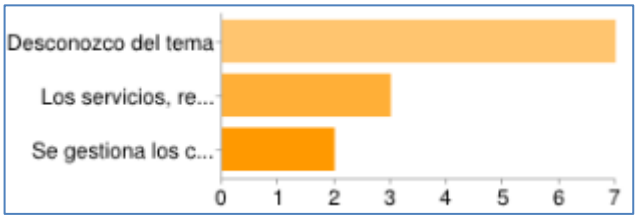


Desconozco del tema	5	38%
Se documenta y actualiza procedimientos de operación (prendido-apagado de equipos, backups, mantenimiento y manipulación de los equipos crìticos, etc.) y se los pone a disposición de todos los usuarios que lo requieran	5	38%
Se documenta y actualiza estrictamente los cambios en los sistemas informáticos, esto es: identificación, registro, evaluación del impacto, comunicación a involucrados, responsabilidad de abortar y recuperarse de los cambios sin éxito	1	8%
Se documenta y actualiza los servicios, reportes, reuniones, incidentes de los proveedores	2	15%
Existe una separación de los recursos para las áreas de desarrollo, prueba y producción con el fin de reducir los riesgos de un acceso no autorizado o de cambios al sistema operacional	3	23%

Los usuarios pueden seleccionar más de una casilla de verificación, por lo que los porcentajes pueden superar el 100%.

Ilustración 14: OC - Procedimientos y responsabilidad de operación

Pregunta 12, el 64% de los encuestados afirma desconocer que la UTIC tenga implementado un nivel apropiado de seguridad, entrega de servicios y acuerdos contratados por proveedores. El 27% indica que los servicios, reuniones, incidentes, reportes y registros provistos por proveedores son monitoreados, auditados y revisados regularmente y finalmente el 18% se gestiona los cambios en la provisión del servicio (incluye: mantenimiento, mejoras en las políticas de seguridad de información, controles nuevos para resolver incidentes, uso de nuevas tecnologías, nuevas versiones lanzadas).



Desconozco del tema	7	64%
Los servicios, reuniones, incidentes, reportes y registros provistos por proveedores son monitoreados, auditados y revisados regularmente	3	27%
Se gestiona los cambios en la provisión del servicio (incluye: mantenimiento, mejoras en las políticas de seguridad de información, controles nuevos para resolver incidentes, uso de nuevas tecnologías, nuevas versiones lanzadas)	2	18%

Los usuarios pueden seleccionar más de una casilla de verificación, por lo que los porcentajes pueden superar el 100%.

Ilustración 15: OC - Gestión de servicios externos

Pregunta 13, de acuerdo a los resultados obtenidos para minimizar el riesgo de fallos y sobrecargas de los sistemas:

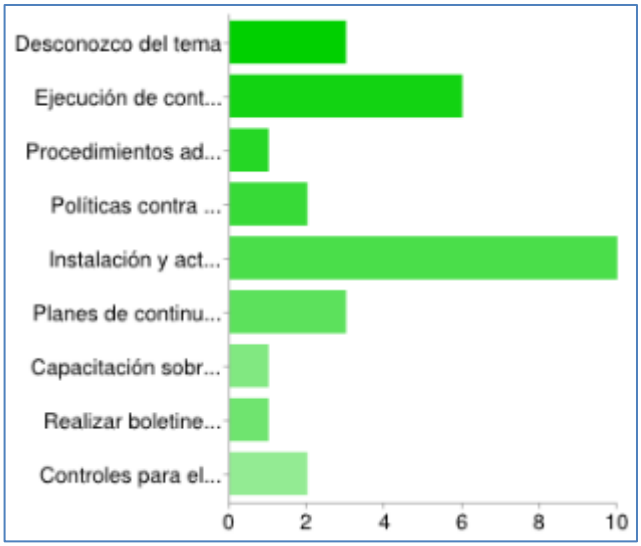
- El 54% considera; que se monitorea el uso de recursos y las proyecciones hechas de requisitos de capacidades adecuadas futuras para asegurar el sistema de funcionamiento requerido.

Ilustración 16: OC - Planificación y aceptación del sistema (a)

- El 54% considera; que se establecen criterios de aceptación para nuevos sistemas de información o versiones nuevas mejoradas desarrollando con ellos pruebas adecuadas antes de su aceptación.

Ilustración 17: OC - Planificación y aceptación del sistema (b)

Pregunta 14, el 77% de las respuestas permiten determinar que la institución con el fin de proteger, prevenir, detectar y evitar la introducción de software malicioso o virus mantiene instalado y actualizado un sistema de antivirus corporativo. Adicionalmente, únicamente el 8% afirma tener capacitación sobre nuevos virus creados y otro 8% indica que se realizan boletines de información de alertas de ataques.



Desconozco del tema	3	23%
Ejecución de controles y políticas de seguridad definidas para detectar y prevenir software malicioso	6	46%
Procedimientos adecuados para concientizar a los usuarios	1	8%
Políticas contra el software no licenciado o no autorizado	2	15%
Instalación y actualización de un antivirus corporativo	10	77%
Planes de continuidad del negocio para recuperarse de los ataques de virus	3	23%
Capacitación sobre nuevos virus creados	1	8%
Realizar boletines de información de alerta de ataques	1	8%
Controles para el uso o ejecución del código descargable (creación de ambientes lógicos aislados)	2	15%

Los usuarios pueden seleccionar más de una casilla de verificación, por lo que los porcentajes pueden superar el 100%.

Ilustración 18: OC - Protección contra software malicioso

Pregunta 15, con el fin de mantener la integridad de y la disponibilidad de los servicios de información, se obtuvo los siguientes resultados de acuerdo a cada ítem:

- El 92% de los encuestados afirmo que se realizan regularmente copias de seguridad de toda la información esencial del negocio. La copia de seguridad se encuentra en un sistema de almacenamiento de Discos (Data Center) y posteriormente pasa a un medio de Cintas Magnéticas (Secretaria General de ESPE Idiomas).

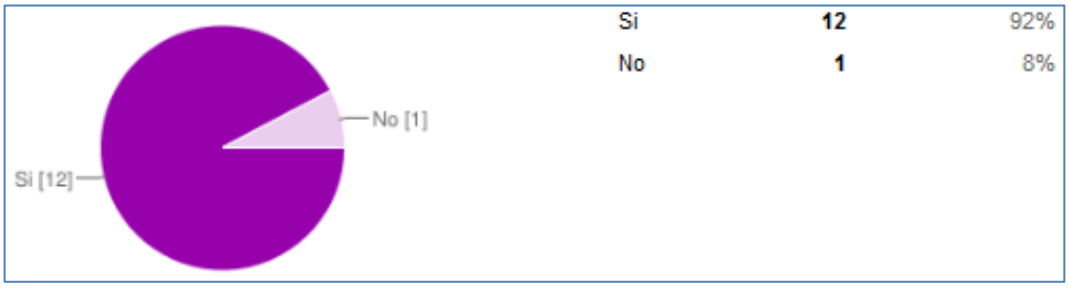


Ilustración 19: OC - Gestión de respaldo y recuperación (a)

- El ítem “b” indica que el 54% de las respuestas afirma que establecen procedimientos rutinarios haciendo copias de seguridad, sin embargo; no se realiza un ensayo oportuno de recuperación de la información. El 46% no acepta que en la UTIC se realice o ejecute este control.

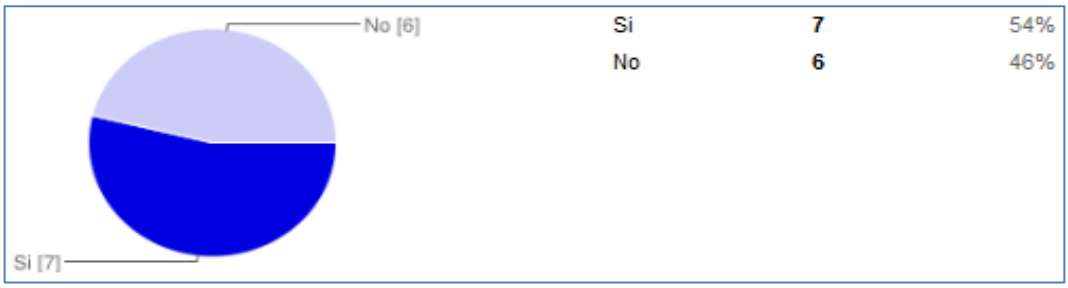


Ilustración 20: OC - Gestión de respaldo y recuperación (b)

Pregunta 16, el 46% de respuestas permite determinar que la UTIC dispone de controles y medidas adicionales para proteger los datos sensibles que circulan por las redes públicas a fin de mantener la integridad, confidencialidad y la disponibilidad de los servicios de información. Sin embargo, el 31% de encuestados no conoce del tema, esto debido a falta de comunicación para difundir este control.

Desconozco del tema	4	31%
Las redes son manejadas y controladas adecuadamente para protegerse de amenazas	6	46%
Se mantiene la seguridad de los sistemas incluyendo la información en transito	4	31%
Se asigna responsabilidades para la gestión de equipos remotos	4	31%
Se salvaguardar la confidencialidad e integridad de los datos en redes públicas	4	31%
Se tiene un registro y monitoreo de acciones de seguridad	2	15%
En la entrega del servicio de red, las características de seguridad son monitoreadas y auditadas	3	23%

Los usuarios pueden seleccionar más de una casilla de verificación, por lo que los porcentajes pueden superar el 100%.

Ilustración 21: OC - Gestión de la seguridad de redes

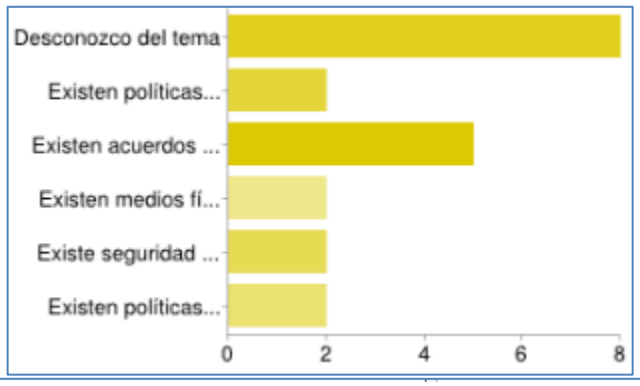
Pregunta 17, con el fin de prevenir accesos no autorizados, modificaciones o robos a los medios de información (documentos, discos, cintas, CDs/DVDs, correo, entre otros), el 38% de los encuestados afirma que el acceso a la información es autorizada y controlada por el propietario de la aplicación, el 31% indica que en la institución existe una adecuada seguridad para almacenar la información crítica. Sin embargo, el 46% evidencia el desconocimiento de los profesionales sobre controles que permitan mitigar el acceso no autorizado a los recursos informáticos de la ESPE.

Desconozco del tema	6	46%
Se eliminan los medios extraíbles de una forma segura cuando no se necesiten mas	0	0%
Se guarda registros de eliminación de información con el fin de guardar pistas de auditoria	2	15%
Se tiene un control de la vida útil de los medios de información	2	15%
Existen procedimientos para la manipulación y almacenamiento de la información con el fin de protegerla de divulgaciones o usos no autorizados	2	15%
Existe una adecuada seguridad para almacenar la información crítica	4	31%
El acceso a la información es autorizada y controlada por el propietario de la aplicación	5	38%
La lista de accesos a la información crítica de la Institución es limitada al máximo	2	15%

Los usuarios pueden seleccionar más de una casilla de verificación, por lo que los porcentajes pueden superar el 100%.

Ilustración 22: OC - Utilización de los medios de información

Pregunta 18, el 62% de las respuestas indican que los profesionales no conocen de un intercambio de información entre organizaciones. Como un dato representativo, se tiene que el 38% afirma que existen acuerdos establecidos para el intercambio de información entre la organización y los proveedores.

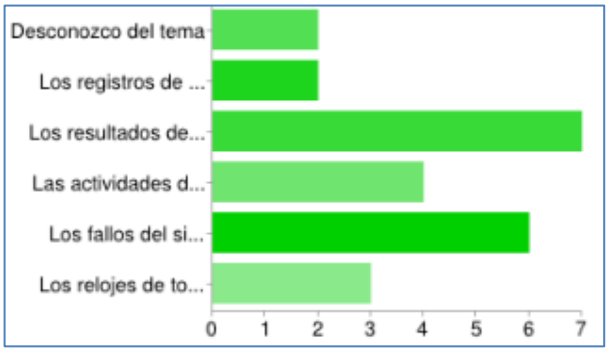


Desconozco del tema	8	62%
Existen políticas o procedimientos formales para proteger la información a través de cualquier medio de comunicación	2	15%
Existen acuerdos establecidos para el intercambio de información entre la organización y proveedores	5	38%
Existen medios físicos seguros de transporte y comunicación con los proveedores	2	15%
Existe seguridad en la mensajería electrónica	2	15%
Existen políticas para proteger la información asociada con la interconexión de sistemas de información de otras instituciones públicas y/o privadas negocios	2	15%

Los usuarios pueden seleccionar más de una casilla de verificación, por lo que los porcentajes pueden superar el 100%.

Ilustración 23: OC - Intercambio de información

Pregunta 19, el 54% de los encuestados manifiesta que se mantiene un monitoreo adecuado del sistema y que estos son revisados regularmente, además un 46% afirma que los fallos del sistema o averías son registrados, analizados y se toman acciones apropiadas con el fin de resolverlas satisfactoriamente.



Desconozco del tema	2	15%
Los registros de auditoría son producidos y guardados para un periodo acordado con el fin de que asistan en investigaciones futuras	2	15%
Los resultados de las actividades de monitoreo son revisadas regularmente	7	54%
Las actividades del administrador y de los operadores del sistema son registrados	4	31%
Los fallos del sistema o averías son registrados, analizados y se toman acciones apropiadas con el fin de resolverlas satisfactoriamente	6	46%
Los relojes de todos los sistemas de procesamiento de información dentro de la institución son sincronizados con una fuente acordada y exacta de tiempo	3	23%

Ilustración 24: OC - Monitoreo

DOMINIO 7: Control de accesos

Pregunta 20, de acuerdo a los resultados obtenidos; es visible que la ESPE no mantiene un control de acceso alto a la información a través de dispositivos lógicos y físicos, basando en políticas y procedimientos formales claramente establecidos. Los profesionales de acuerdo a sus respuestas establecieron un nivel medio con el 54% y con el 46% un nivel bajo.

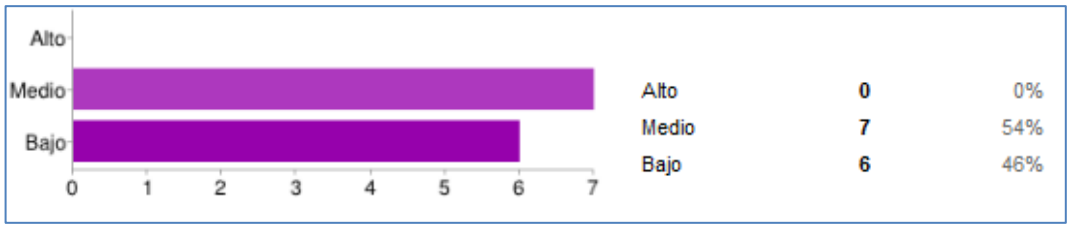
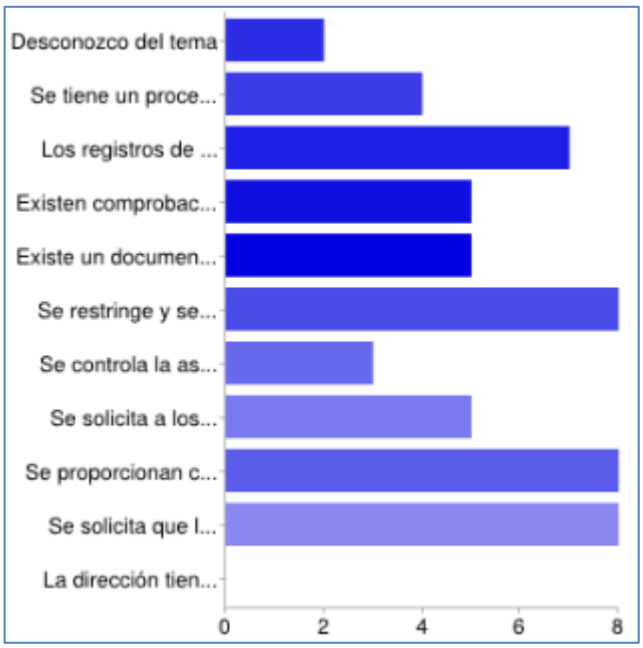


Ilustración 25: OC - Requisitos de negocio para el control de accesos

Pregunta 21, para los profesionales de la UTIC; la ESPE cuento con un control para el acceso autorizado de usuarios y la prevención de accesos no autorizados a los sistemas de información. El porcentaje de nivel de cumplimiento de este control es muy parejo de acuerdo a lo que recomienda la ISO/IEC 27002, con un 62% se encuentran:

- Se restringe y se controla el uso y asignación de privilegios
- Se proporcionan claves temporales que forzosamente el usuario debe cambiar en un tiempo definido
- Se solicita que las contraseñas deben ser únicas para cada individuo y no deben ser obvias

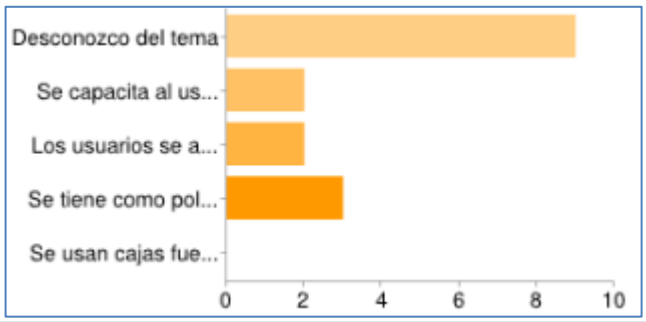


Desconozco del tema	2	15%
Se tiene un procedimiento de registro de altas y bajas de usuarios	4	31%
Los registros de acceso en sistemas multiusuario tienen un identificador único para cada usuario	7	54%
Existen comprobaciones de autorizaciones por el propietario del servicio para utilizar el sistema	5	38%
Existe un documento escrito de los derechos de acceso que tiene el usuario	5	38%
Se restringe y se controla el uso y asignación de privilegios	8	62%
Se controla la asignación de contraseñas por medio de un proceso de gestión formal	3	23%
Se solicita a los usuarios firmas de compromiso para mantener en secreto sus contraseñas personales y las compartidas por un grupo	5	38%
Se proporcionan claves temporales que forzosamente el usuario debe cambiar en un tiempo definido	8	62%
Se solicita que las contraseñas deben ser únicas para cada individuo y no deben ser obvias	8	62%
La dirección tiene un proceso formal de revisión periódica de los derechos de acceso de los usuarios	0	0%

Los usuarios pueden seleccionar más de una casilla de verificación, por lo que los porcentajes pueden superar el 100%.

Ilustración 26: OC - Gestión de acceso de usuarios

Pregunta 22, el 69% de los resultados indican que no se conoce un control establecido en la ESPE para mantener una protección eficaz, sin embargo la implementación de políticas permitirá la cooperación de los usuarios autorizados, de acuerdo al 23%, mantener un escritorio limpio de papeles.



Desconozco del tema	9	69%
Se capacita al usuario en buenas prácticas de seguridad para la selección, uso y cambio de sus contraseñas	2	15%
Los usuarios se aseguran que los equipos informáticos desatendidos están debidamente protegidos o cancelan todas las sesiones activas antes de marcharse de la Institución	2	15%
Se tiene como política el tener un escritorio limpio de papeles.	3	23%
Se usan cajas fuertes o gavetas seguras para guardar información crítica impresa	0	0%

Los usuarios pueden seleccionar más de una casilla de verificación, por lo que los porcentajes pueden superar el 100%.

Ilustración 27: OC - Responsabilidades de los usuarios

Pregunta 23, el 62% de los consultados da a conocer que el acceso a los servicios de las redes internas y externas, asegurándose que el acceso de los usuarios no comprometa la seguridad informática de la Institución se lo controla a través des habilitación de los puertos, servicios y equipos que no son requeridos para la funcionalidad del negocio.

Adicionalmente, se asegura con el 46% que se mantiene otro control a través de la división de la red de la ESPE en redes privadas virtuales. Existen otros criterios de control que han sido considerados por los profesionales. Es importante resaltar que un porcentaje considerable (23%) no conoce de métodos de conexiones seguras establecidas en la institución.

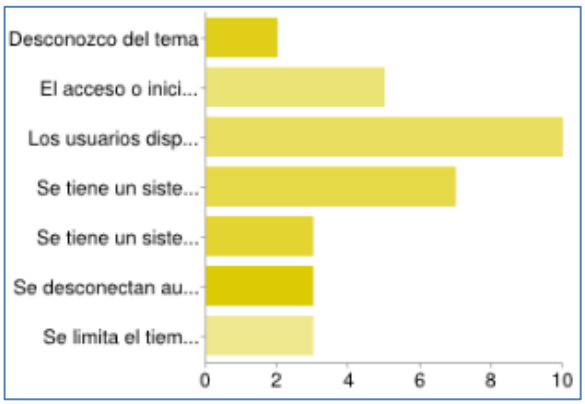
Desconozco del tema	3	23%
Políticas y procedimientos para que los usuarios sólo deban acceder a los servicios para los que están autorizados	3	23%
Utilización de métodos apropiados de autenticación para controlar el acceso de usuarios remotos (criptografía, protocolos de desafío-respuesta, redes privadas virtuales, cuidados especiales en los controles para redes inalámbricas)	5	38%
Manejo de indicadores dentro de los equipos informáticos para revelar si el equipo esta autorizado o no para conectarse a la red de la Institución	1	8%
Se controla y se inhabilitan los puertos, servicios y equipos que no son requeridos para la funcionalidad del negocio	8	62%
Se divide la gran red de la Institución en dominios lógicos separados, protegidos por perímetros definidos de seguridad usando gateways, firewalls, redes virtuales privadas, capacidad de enrutamiento, entre otros	6	46%
Se tienen controles de enrutamiento adecuados que verifiquen direcciones de origen y destino	4	31%

Los usuarios pueden seleccionar más de una casilla de verificación, por lo que los porcentajes pueden superar el 100%.

Ilustración 28: OC - Control de acceso a la red

Pregunta 24, con la finalidad de minimizar los riesgos de accesos no autorizados a los computadores de los usuarios el 77% de los profesionales que respondieron el cuestionario afirman que:

- Los usuarios disponen de un identificador único para uso personal
- El 54%, manifestó que se tiene un sistema de autenticación adecuado para verificar la identidad de los usuarios

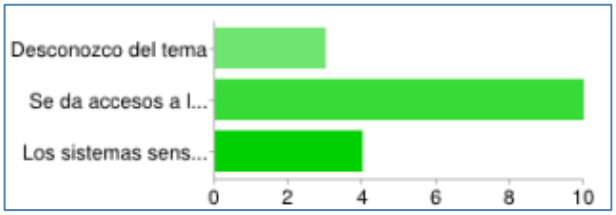


Desconozco del tema	2	15%
El acceso o inicio de sesión a los equipos informáticos se lo realiza mediante un proceso de conexión segura	5	38%
Los usuarios disponen de un identificador único para su uso persona	10	77%
Se tiene un sistema de autenticación adecuada para verificar la identidad de los usuarios	7	54%
Se tiene un sistema adecuado de gestión de contraseñas para proporcionar un medio eficaz e interactivo para asegurar la calidad de las mismas	3	23%
Se desconectan automáticamente las sesiones tras un periodo definido de inactividad	3	23%
Se limita el tiempo de conexión para aplicaciones de alto riesgo	3	23%

Los usuarios pueden seleccionar más de una casilla de verificación, por lo que los porcentajes pueden superar el 100%.

Ilustración 29: OC - Control de acceso al sistema operativo

Pregunta 25, con la finalidad de prevenir el acceso no autorizado a la información contenida en los sistemas, el 77% de los encuestados afirma que se da acceso a la información y a las funciones del sistema de aplicaciones sólo a los usuarios de mismo. El 31% indica que los sistemas sensibles usan entornos informáticos dedicados o aislados y el 23% manifiesta no conocer del tema.



Desconozco del tema	3	23%
Se da accesos a la información y a las funciones del sistema de aplicaciones sólo a los usuarios de mismo	10	77%
Los sistemas sensibles usan entornos informáticos dedicados o aislados	4	31%

Los usuarios pueden seleccionar más de una casilla de verificación, por lo que los porcentajes pueden superar el 100%.

Ilustración 30: OC - Control de acceso a las aplicaciones

Pregunta 26, de acuerdo a los resultados obtenidos; es visible que la ESPE no mantiene un control la seguridad de la información cuando se usan equipos portátiles (notebooks, netbooks) y equipos móviles (celulares, tabletas). Los profesionales de acuerdo a sus respuestas establecieron un nivel medio con el 54% y con el 46% un nivel bajo.

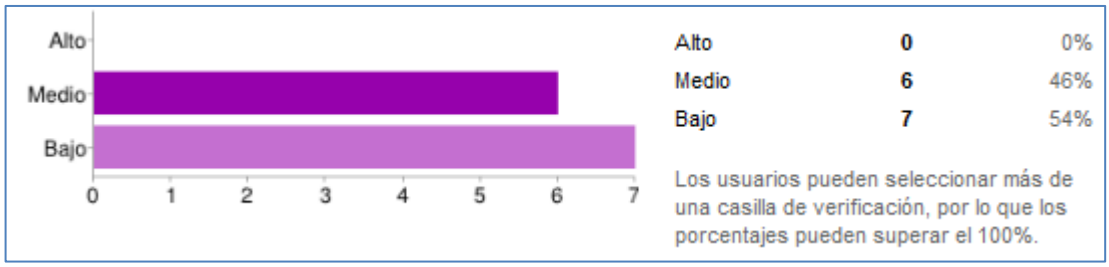


Ilustración 31: OC - Ordenadores portátiles y teletrabajo

DOMINIO 8: Adquisición, desarrollo y mantenimiento de sistemas

Pregunta 27, el 62% de los encuestados manifiestan que el nivel de controles que existen en la UTIC para evitar que la seguridad esté embebida dentro de los sistemas de información se encuentra en nivel medio. El 28% de los profesionales indicó que este control se mantiene en un nivel bajo y ninguno considera que es una seguridad alta.

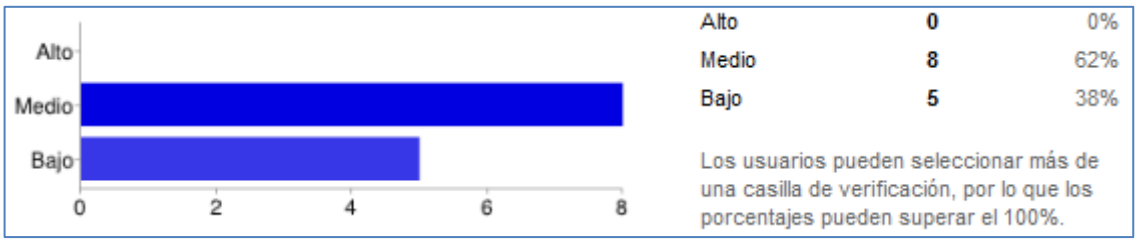
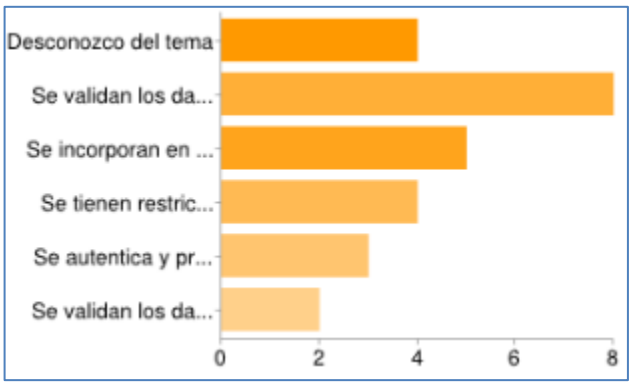


Ilustración 32: OC - Requisitos de seguridad de los sistemas

Pregunta 28, se videncia una notable superioridad (62%) en lo indicado por los profesionales en manifestar que para evitar pérdidas, modificaciones o mal uso de los datos de usuario en las aplicaciones de la Institución, el control implementado en la validación de los datos de entrada en las aplicaciones del sistema para garantizar que estas sean correctas y apropiadas, es decir, se verifican los datos de referencia, tablas de parámetros, entradas duplicadas, valores fuera de rango, caracteres inválidos, definición de responsabilidades de los implicados en el proceso de ingreso de datos.

El 38% indica que se incorporan en los sistemas comprobaciones de validación para detectar cualquier tipo de corrupción de información a través de errores del proceso o por actos deliberados.

El 31% desconoce el tema y el mismo porcentaje afirma que se tienen restricciones que minimicen el riesgo de los fallos del proceso con pérdidas de integridad al añadir o borrar datos, considerando el uso de programas correctos de recuperación después de fallas.



Desconozco del tema	4	31%
Se validan los datos de entrada a las aplicaciones del sistema para garantizar que son correctas y apropiadas	8	62%
Se incorporan en los sistemas comprobaciones de validación para detectar cualquier tipo de corrupción de información a través de errores del proceso o por actos deliberados.	5	38%
Se tienen restricciones que minimicen el riesgo de los fallos del proceso con pérdidas de integridad al añadir o borrar datos, considerando el uso de programas correctos de recuperación después de fallas	4	31%
Se autentica y protege la integridad de los mensajes en aplicaciones usando controles apropiados como técnicas criptográficas	3	23%
Se validan los datos de salida de un sistema de aplicación para garantizar que el proceso de información ha sido correcto y apropiado a las circunstancias(verosimilitud, conciliación)	2	15%

Los usuarios pueden seleccionar más de una casilla de verificación, por lo que los porcentajes pueden superar el 100%.

Ilustración 33: OC - Seguridad de las aplicaciones del sistema

Pregunta 29, permite determinar que:

- Ítem “a”, muestra que el 62% de las respuestas de los profesionales consideran que el control es bajo respecto a la protección de la confidencialidad, disponibilidad o integridad de la información utilizando métodos o medidas criptográficas.

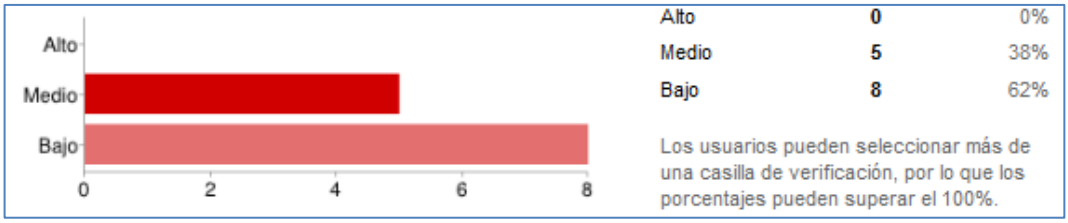


Ilustración 34: OC - Controles criptográficos (a)

- Ítem “b”, El 8% de los encuestados consideran que la protección física para garantizar la confidencialidad, disponibilidad o integridad de la información utilizando métodos o medidas criptográficas es alta,

mientras que el 62% la considera baja y el 30% dice que este control se lo mantiene en un nivel medio.

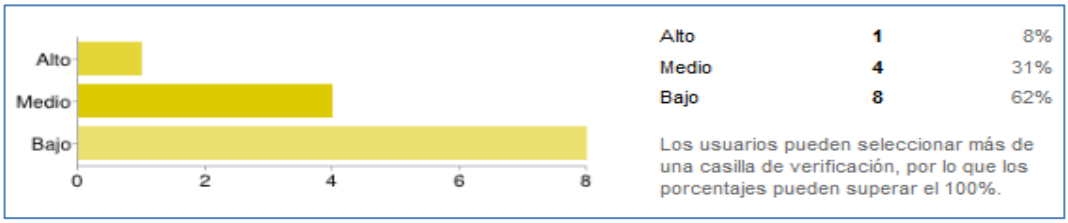
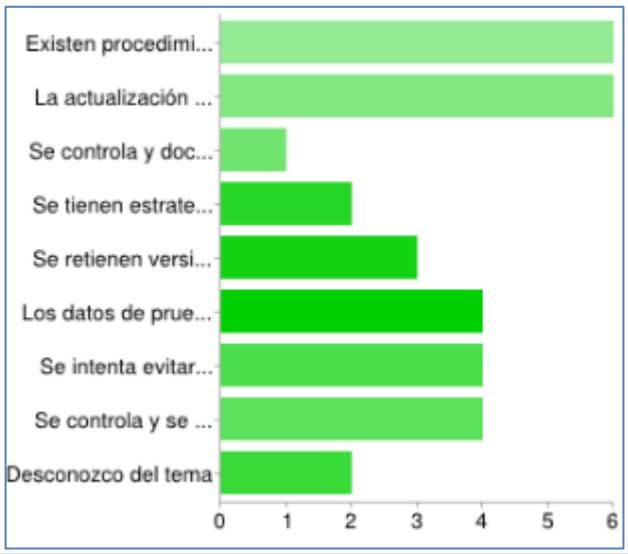


Ilustración 35: OC - Controles criptográficos (b)

Pregunta 30, los encuestados indican que en la institución se evidencian diferentes controles para garantizar la seguridad de los archivos del sistema, sin embargo con el 46% consideran que existen procedimientos para controlar la instalación del software en sistemas operacionales, y con el mismo porcentaje, la actualización de librerías de programas operativos y aplicación de parches en el software son realizadas solo por un administrador capacitado.



Existen procedimientos para controlar la instalación del software en sistemas operacionales	6	46%
La actualización de librerías de programas operativos y aplicación de parches en el software solo la realiza un administrador capacitado	6	46%
Se controla y documenta la configuración del sistema	1	8%
Se tienen estrategias de restauración no actualizada antes de que se implementen cambios	2	15%
Se retienen versiones anteriores de software como medida de contingencia	3	23%
Los datos de prueba deben son seleccionados cuidadosamente, protegidos y controlados	4	31%
Se intenta evitar la exposición de datos sensibles en ambientes de prueba	4	31%
Se controla y se restringe el acceso al código fuente de los programas	4	31%
Desconozco del tema	2	15%

Los usuarios pueden seleccionar más de una casilla de verificación, por lo que los porcentajes pueden superar el 100%.

Ilustración 36: OC - Seguridad de los archivos del sistema

Pregunta 31, el 38% afirma que la prevención de fuga información mantiene la seguridad del software de aplicación y la información, los responsables de los sistemas controlan todo cambio propuesto en el sistema, el soporte al mismo y comprueban que no se debilite la seguridad del mismo bajo ninguna circunstancia. El mismo porcentaje es considerado para las profesionales que por algún motivo no conoce de este control.

La implementación de cambios en el sistema es controlada usando procedimientos formales de cambio	1	8%
Se revisan y se prueban las aplicaciones del sistema cuando se efectúan cambios para asegurar que no impacten adversamente en el funcionamiento o en la seguridad	4	31%
Se previene toda oportunidad de fuga de información	5	38%
Cuando se desarrolla externamente el software, este es supervisado y monitoreado por la UTIC	2	15%
Desconozco del tema	5	38%

Los usuarios pueden seleccionar más de una casilla de verificación, por lo que los porcentajes pueden superar el 100%.

Ilustración 37: OC - Seguridad en los procesos de desarrollo y soporte

Pregunta 32, el 69% de los encuestados han indicado que la ESPE cuenta con un nivel de control medio sobre las vulnerabilidades técnicas detectadas en los sistemas utilizados, mientras que el 31% consideran que este control es bajo.

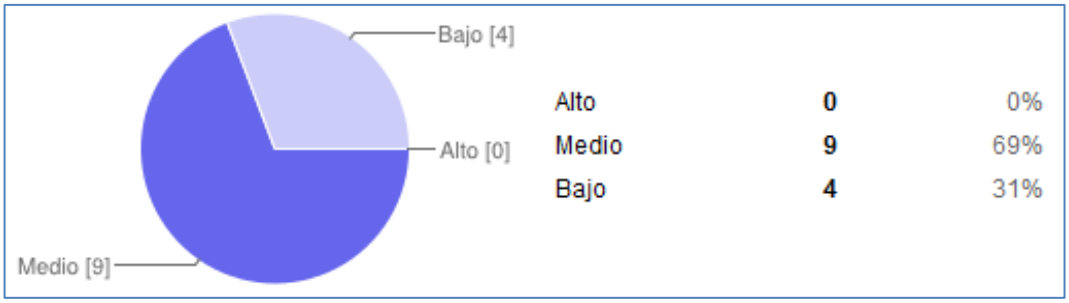
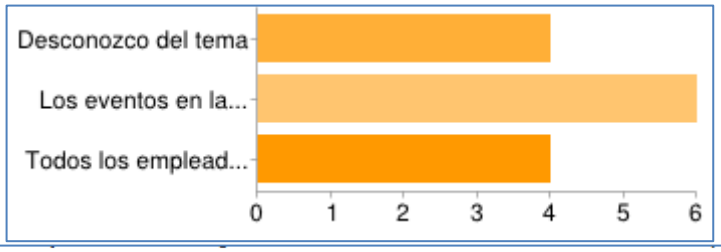


Ilustración 38: OC - Gestión de la vulnerabilidad técnica

DOMINIO 9: Gestión de incidentes en la seguridad de la información

Pregunta 33, de acuerdo a las respuestas obtenidas el 46% de los eventos en la seguridad de información son reportados en el menor tiempo, mientras que para el 31% de los profesionales indican que todos los empleados, contratistas y

proveedores que son usuarios de los sistemas reportan oportunamente cualquier debilidad observada. El resto de respuestas (31%) manifiestan que no conocen el tema.



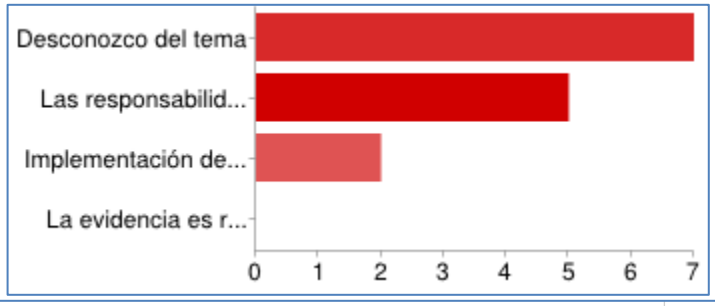
Desconozco del tema	4	31%
Los eventos en la seguridad de información son reportados lo más rápido posible	6	46%
Todos los empleados, contratistas y proveedores que son usuarios de los sistemas reportan oportunamente cualquier debilidad observada	4	31%

Los usuarios pueden seleccionar más de una casilla de verificación, por lo que los porcentajes pueden superar el 100%.

Ilustración 39: OC - Notificación de eventos y debilidades de la S-I

Pregunta 34, con el fin de asegurar una gestión efectiva de incidentes (monitoreo y evaluación) en la seguridad de la información, los encuestados, con un 38%, indican que el control que se evidencia en la institución son las responsabilidades y procedimientos que se encuentran establecidos para asegurar una rápida, efectiva y ordenada respuesta a los incidentes. Sin embargo, el 54% indica no conocer del tema.

La implementación de un mecanismo que permita que los tipos y costos de los incidentes en la seguridad de la información sean cuantificados y monitoreados, es otro control existente en la ESPE, en referencia al 15% de respuestas.



Desconozco del tema	7	54%
Las responsabilidades y procedimientos están establecidas para asegurar una rápida, efectiva y ordenada respuesta a los incidentes en la seguridad de la información	5	38%
Implementación de un mecanismo que permita que los tipos y costos de los incidentes en la seguridad de la información sean cuantificados y monitoreados	2	15%
La evidencia es recolectada, retenida y presentada a la jurisdicción adecuada, cuando existe una acción de seguimiento contra una persona o empresa	0	0%

Los usuarios pueden seleccionar más de una casilla de verificación, por lo que los porcentajes pueden superar el 100%.

Ilustración 40: OC - Gestión de incidentes y mejoras en la S-I

DOMINIO 10: Gestión de la continuidad del negocio

Pregunta 35, a fin de poder reaccionar adecuadamente en caso de interrupción de actividades de la ESPE y proteger los procesos críticos frente a grandes fallos de los sistemas de información o desastres naturales o fallas de equipos, con el 23% los profesionales de la UTIC han indicado que se evidencia los siguientes controles:

- Se tiene identificados todos los activos implicados en los procesos críticos del negocio.
- Se identifican los eventos que pueden causar interrupciones a los procesos de negocio junto con la probabilidad e impacto de dichas interrupciones y sus consecuencias.
- Se tiene un plan de recuperación del negocio para asegurar la disponibilidad de información al nivel y en las escalas de tiempo requeridas tras la interrupción.

Frente a esta pregunta, el 46% de las respuestas indican que los técnicos de la UTIC no conocen de un documento formal en el que se explique los

procedimientos adecuados a fin de contrarrestar la paralización de los servicios causados por desastres naturales o fallas de equipos.

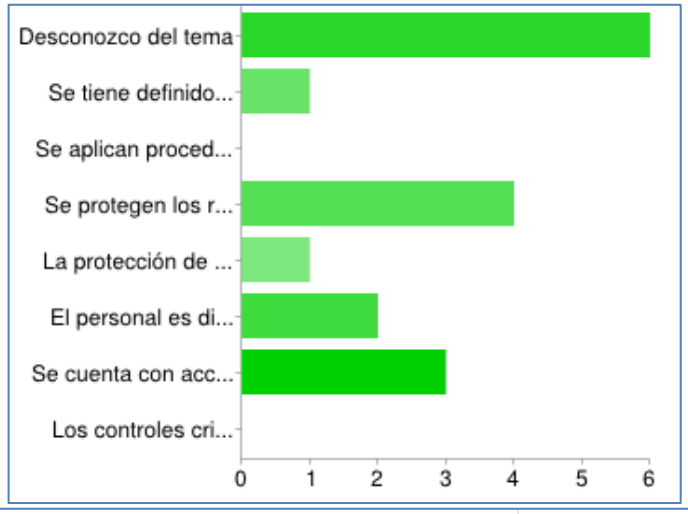
Desconozco del tema	6	46%
Se tiene un proceso adecuado de gestión para el desarrollo y el mantenimiento de la continuidad del negocio	0	0%
Se concientiza sobre los riesgos que la Institución corre desde el punto de vista de su vulnerabilidad e impacto que tendrían las interrupciones en el negocio	2	15%
Se tiene identificados todos los activos implicados en los procesos críticos del negocio	3	23%
Se prueba y se actualiza regularmente los planes y procesos instalados de continuidad del negocio	1	8%
Se identifican los eventos que pueden causar interrupciones a los procesos de negocio junto con la probabilidad e impacto de dichas interrupciones y sus consecuencias	3	23%
Se tiene un plan de recuperación del negocio para asegurar la disponibilidad de información al nivel y en las escalas de tiempo requeridas tras la interrupción	3	23%
Se identifican los procesos de emergencia y acuerdos de todas las responsabilidades	2	15%
Se identifican las pérdidas aceptables de información y servicios	1	8%
Se tiene un plan de gestión de crisis diferente al de gestión de continuidad del negocio	1	8%
Se tiene un plan de continuidad del negocio consistentes	0	0%
Se prueban regularmente los planes de continuidad del negocio para asegurarse de su actualización y eficacia	0	0%

Los usuarios pueden seleccionar más de una casilla de verificación, por lo que los porcentajes pueden superar el 100%.

Ilustración 41: OC - Aspectos de la gestión de la continuidad del negocio

DOMINIO 11: Cumplimiento

Pregunta 36, el 46% de las respuestas evidencian el desconocimiento de los profesionales sobre el incumplimiento de cualquier ley civil o penal, requisito reglamentario, regulación u obligación contractual por parte del personal de la Institución. El 31% de los encuestados indican que actualmente se protegen los registros importantes de la organización (contables, bases de datos, transacciones, auditoría, operativos) frente a su pérdida, destrucción y falsificación en concordancia con los requisitos regulatorios, contractuales y de negocio



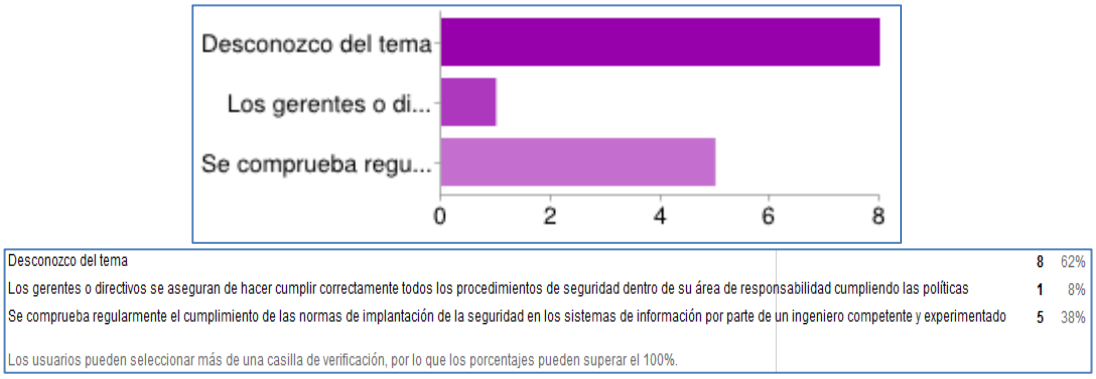
Desconozco del tema	6	46%
Se tiene definido, documentado y actualizado de forma explícita todos los requisitos legales, regulatorios y contractuales que sean importantes para cada sistema de información	1	8%
Se aplican procedimientos apropiados para asegurar el cumplimiento de las restricciones legales, reguladores y contractuales sobre el uso del material protegido por derechos de propiedad intelectual	0	0%
Se protegen los registros importantes de la organización frente a su pérdida, destrucción y falsificación en concordancia con los requisitos regulatorios	4	31%
La protección de datos y privacidad de la información personal debe ser asegurada como se requiere en la legislación y en las regulaciones	1	8%
El personal es disuadido de utilizar los recursos de tratamiento de la información para propósitos no autorizados o que estén fuera de los fines del negocio	2	15%
Se cuenta con acciones disciplinarias y/o legales apropiadas	3	23%
Los controles criptográficos deben ser utilizados en conformidad con todos los acuerdos, leyes y regulaciones	0	0%

Los usuarios pueden seleccionar más de una casilla de verificación, por lo que los porcentajes pueden superar el 100%.

Ilustración 42: OC - Cumplimiento de los requisitos legales

Pregunta 37, de acuerdo al 38% de respuestas, actualmente; se comprueba regularmente el cumplimiento de las normas de implantación de la seguridad en los sistemas de información por parte de un ingeniero competente y experimentado, con la finalidad de asegurar el cumplimiento de las políticas y

normas de seguridad implementadas en la Institución. El 62% manifiesta no conocer políticas o estándares implementados en los procesos de TI de la ESPE.

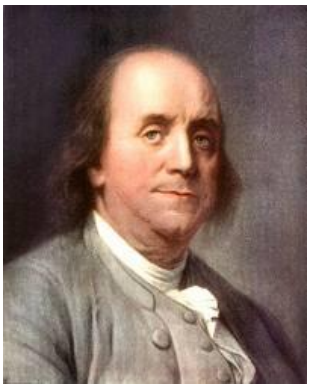


Desconozco del tema	8	62%
Los gerentes o directivos se aseguran de hacer cumplir correctamente todos los procedimientos de seguridad dentro de su área de responsabilidad cumpliendo las políticas	1	8%
Se comprueba regularmente el cumplimiento de las normas de implantación de la seguridad en los sistemas de información por parte de un ingeniero competente y experimentado	5	38%

Los usuarios pueden seleccionar más de una casilla de verificación, por lo que los porcentajes pueden superar el 100%.

Ilustración 43: OC - Cumplimiento de políticas, normas de seguridad y técnico

“Aquellos que cederían la libertad esencial para adquirir una pequeña seguridad temporal, no merecen ni libertad ni seguridad” ***Benjamín Franklin***



4. CAPÍTULO IV – POLÍTICAS DE SEGURIDAD DE INFORMACIÓN

4.1. Historia

Tabla 18: Políticas de Seguridad de Información

VER.	FECHA	AUTORES	MODIFICACIONES
1.0	30-07-2012	Ing. Mauricio Baldeón Ing. Christian Coronel	Versión Inicial
ÁREA DE INFLUENCIA		Escuela Politécnica del Ejército, sedes, extensiones, centros de apoyo	
		Unidad de Tecnologías de la Información y Comunicación	
PROGRAMA DE POSTGRADOS			**PROMOCIÓN**
Maestría de Gerencia de Sistemas			XII

Autores: El desarrollo de la Políticas de Seguridad de la Información para la UTIC de la ESPE con lineamientos de la Norma ISO/IEC 27002 fue llevando a cabo por un equipo de profesionales conformado por las siguientes personas:

Ing. Mauricio Baldeón, profesional que ha cursado con los siguientes estudios académicos:

i. Título de Ingeniero en Sistemas e Informática, Escuela Politécnica del Ejército
ii. Curso Internacional de Seguridad de la Información, avalado por el Instituto Tecnológico Monterrey, Sede Quito.
iii. Egresado de la Maestría de Gerencia de Sistemas, Escuela Politécnica del Ejército.

Como una breve descripción de su experiencia laboral se destaca 2 años en el desarrollo de sistemas de información en la CREATEC S.A. Sin embargo, ha sido su alma mater, la “ESPE”, en donde ha venido desarrollado su conocimiento

de TI. Actualmente, el profesional se encuentra trabajando en la Unidad de Tecnologías de la Información, proporcionando a la comunidad politécnica los servicios integrados de red, internet, intranet y comunicaciones de acuerdo a los avances tecnológicos, realizando un seguimiento y registro de las actividades de red, detección de eventos y ejecutando las acciones necesarias para garantizar los servicios de comunicación requeridos por la comunidad politécnica.

Ing. Christian Coronel, profesional que se destaca por cumplir con lo siguientes títulos académicos:

i. Título de Ingeniero en Sistemas e Informática, Escuela Politécnica del Ejército
ii. Diploma Superior en Gestión para el Aprendizaje Universitario, Escuela Politécnica del Ejército
iii. Egresado de la Maestría de Gerencia de Sistemas, Escuela Politécnica del Ejército.

Christian, mantiene una relación laboral con la ESPE desde hace 10 años, tiempo en el cual ha desarrollado sus aptitudes en la Unidad de Tecnologías de la Información y Comunicación en el área de Soporte y Mantenimiento de Equipos Informáticos, brindando a la institución los servicios de: soporte en sitio, mantenimiento preventivo y mantenimiento correctivo de equipos computacionales.

4.2. Resumen ejecutivo

Como para todas las organizaciones, la información es un activo esencial para la ESPE. Es de suma relevancia que la información que sea considerada como sensible se catalogue como confidencial, precisa y se encuentre disponible a fin de solventar los requerimientos de la comunidad politécnica.

La información recopilada para el desarrollo del presente documento será responsabilidad de los integrantes del equipo de trabajo, con la finalidad de preservarla y manejarla adecuadamente durante la ejecución de las tareas planificadas.

Es responsabilidad de todos y cada uno de los miembros de la comunidad politécnica; asegurar la información y por tal motivo deberá actuar positivamente en función de su preservación.

Las presentes políticas deberán ser cumplidas por los directivos, docentes, servidores públicos, personal militar, alumnos que forman parte de la ESPE. Los terceros involucrados (proveedores) serán incluidos en estas políticas en un proceso contractual que tenga como objeto la adquisición de un bien/servicio.

Cada una de las direcciones, UA[15] y departamentos académicos deberán ser responsables de la seguridad de su información; por tal motivo se alinearán a las medidas descritas en estas políticas y estarán basadas en el valor de la información y en el riesgo del negocio. Los objetivos de estas medidas se deberán alinear a la confidencialidad, integridad y confidencialidad, fundamentos básicos de la seguridad de la información.

La presente política, referenciará un marco de trabajo para todos los procesos definidos y sus mecanismos de seguridad. Los requerimientos que la ISO/IEC 27002 recomienda, se describen a continuación:

- ✓ Objetivos de seguridad
- ✓ Clasificación de la información
- ✓ Asignación de responsabilidades

[15] UA: Unidad Administrativa

- ✓ Principios enfocados a los objetivos de la ESPE
- ✓ Tiempo de revisión de la presente política

Esta política determina los requerimientos mínimos recomendados por los 11 Dominios en la ISO/IEC 27002, y estará disponible para todo el personal de la comunidad politécnica y terceros involucrados.

Como se mencionó anteriormente, se definió una metodología de análisis de riesgos denominada OCTAVE, y se fundamenta las políticas de seguridad de la información alineándose a la ISO/IEC 27002 ((11) Dominios – (39) Objetivos de control – (133) Controles).

4.3. Objetivo y alcance

4.3.1. Alcance

Esta política se aplicará a toda la información que es creada, recibida, almacenada, procesada, transmitida, entregada y descartada usando cualquier sistema o medio de almacenamiento. Adicionalmente, será aplicable a todas las UAs de la ESPE, miembros de la Comunidad Politécnica (Directivos, oficiales, personal administrativo, docentes, alumnos) y a terceros (proveedores).

Cumpliendo el alcance de elaboración de la investigación, se desarrollan las políticas de los siguientes dominios:

a. Dominio (1): Política de Seguridad
b. Dominio (6): Gestión de Comunicaciones y Operaciones
c. Dominio (8): Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.
d. Dominio (10): Gestión de la Continuidad del Negocio

4.4. Ética

El código de ética de la institución, deberá regular las actividades y las decisiones a tomar sobre los recursos de tratamiento y de los activos de la información. Adicionalmente, deberá promover el involucramiento de los miembros de la comunidad politécnica y terceros a las actividades de fortalecimiento de la ética informática, entre las que se mencionan las siguientes: monitoreo de actividades de los usuarios, pruebas de penetración, accesos no autorizados a información clasificada como sensible, entre otras.

El código de ética debe especificar claramente el alcance y las responsabilidades que corresponde a cada usuario de los sistemas de información y recursos tecnológicos, rigiéndose a las leyes, reglamentos y normas vigentes y de control interno de la ESPE.

4.5. Normas y disposiciones generales

- ✓ La ESPE es y será responsable de la protección y custodia de toda la información recibida o producida por los directivos, servidores públicos, docentes, alumnos y terceros.

- ✓ La Información que haya ingresado a la institución por parte de terceros, pasará a estar bajo la custodia de la ESPE y de la misma forma se sujetará a las normas y procedimientos de control interno.

- ✓ El acceso a la información institucional; de personal externo que preste servicios a la ESPE, estará regulada por los respectivos contratos y acuerdos de confidencialidad que suscriban para el efecto.

4.6. Cumplimiento y violaciones

Será de estricto cumplimiento para toda la Comunidad Politécnica y toda persona considerada en el alcance de esta política, en tal virtud tendrá que aceptar sus términos. El uso de los recursos informáticos o de información con fines ilegales o consideradas inapropiadas que atenten contra un ambiente de trabajo bien controlado, es considerado como PROHIBIDO.

Las violaciones a esta Política por parte de cualquier usuario de la Comunidad Politécnica, motivará la ejecución de medidas disciplinarias y/o legales, ya que serán consideradas como faltas graves.

4.7. Gerenciamiento de la seguridad de la información de la ESPE

Para cumplir con los requisitos de S-I es necesario que:

- ✓ Toda persona que forme parte de la Comunidad Politécnica y terceros, sea responsable del correcto uso de la información.
- ✓ Se evidencie registros, logs y eventos sobre cambios u operaciones transaccionales a la que se someta la información.
- ✓ Se enfatice en medidas preventivas y no correctivas. Las medidas de seguridad que se pongan en práctica deben ser en lo posible reforzadas con soluciones técnicas que no dependan de procesos humanos.
- ✓ La implementación de mecanismos específicos de seguridad, se justifiquen en relación al valor asociado con la información que este siendo protegida.
- ✓ Se realice una evaluación independiente y periódica de la administración y uso de la información.

4.8. Análisis de riesgo y clasificación de la información

El análisis y clasificación de riesgos, es el soporte para determinar el éxito de una correcta implementación de una Política de la Seguridad. Los mecanismos de seguridad de la información deben ser definidos en función al alcance de los niveles requeridos y que se encuentren documentados de manera clara, sencilla y actualizada, caso contrario en esta Política de Seguridad, serán puestos a consideración de la Unidad de Tecnologías de la Información, esto en virtud de que actualmente la ESPE no cuenta con un área específica de Seguridad de la Información.

4.9. Clasificación de la información

Se definen los niveles estándares y los criterios de sensibilidad de la información institucional, tomando en consideración para ellos los aspectos estratégicos y operativos que influyan en su gestión y control.

- ✓ NIVEL 0: Información de acceso público

  - Se catalogará en este nivel, toda aquella Información que puede encontrarse disponible y ser utilizada sin previa autorización por cualquier persona, pertenezca o no a la Comunidad Politécnica. Es información que se considera de dominio público (Página WEB institucional, Portal de Servicios MI ESPE).

- ✓ NIVEL 1: Información de acceso privado e interno de la institución

  - Es la información que sin ser publicada, puede ser conocida y utilizada por miembros de la Comunidad Politécnica y de terceros, previa autorización. La divulgación parcial o total de esta

información que no haya sido autorizada, podría ocasionar pérdidas leves por la ESPE.

- Documentos que contengan metodologías o mejores prácticas probadas para la ejecución de actividades puntuales internas.
- Documentos que contengan un conjunto de procedimientos secuenciales necesarios para generar un producto o servicio esperado.
- Memorandos e informes internos que contengan información concerniente a las actividades propias de la ESPE.
- Expedientes de estudio y proyectos no expedidos o no publicados, excepto para los órganos competentes.
- Estrategias, normas, políticas, manuales, procedimientos internos y documentos relacionados, no publicados en la página web de la ESPE.
- Resoluciones y reglamentos internos.
- Actividades descritas en el Workflow.
- Documentos de diseño, manuales técnicos y de usuario de las aplicaciones informáticas institucionales.
- Bases de datos institucionales y las que fueren entregadas a la institución, que contengan información de estudiantes, responsables o terceros; o que tengan relación con planes y programas de control académico, así como la información transaccional derivada de los procesos propios de la Educación Superior.

✓ <u>NIVEL 2: Información considerada como confidencial</u>

- Es la información que sólo puede ser conocida y utilizada por un grupo de funcionarios, que la necesiten para cumplir con sus funciones y colaborares externos autorizados y que hayan firmado el compromiso de confidencialidad, su divulgación o uso no autorizado

podría ocasionar pérdidas significativas materiales o de imagen. Este tipo de información es considerada como sensible.

- Información utilizada en procesos precontractuales antes de su divulgación, y que no hayan sido detalladas en el literal anterior.
- Servicios WEB (Confidenciales, Notas académicas)
- Documentos que contengan información de postulantes a pruebas psicométricas, técnicas y entrevistas para concursos de merecimiento y oposición.

✓ NIVEL 3: Información considerada como estrictamente confidencial

- Es la información que sólo puede ser conocida y utilizada por las Autoridades de la Institución, se encuentra relacionada directamente con las decisiones estratégicas de la Institución; o en su defecto es conocida únicamente por su propietario, su uso no autorizado puede ocasionar pérdidas materiales o de imagen a la ESPE.
- Documentos de configuración de todos los equipos y servicios pertenecientes a la plataforma tecnológica.
- Mensajes de correo electrónico unipersonales
- Servicios WEB (Confidenciales, Notas académicas)

4.10. Roles y responsabilidades

Se definen los siguientes roles y responsabilidades propuestos en esta investigación.

4.10.1. Estructura organizacional propuesta

La estructura organizacional propuesta, se muestra en la siguiente figura:

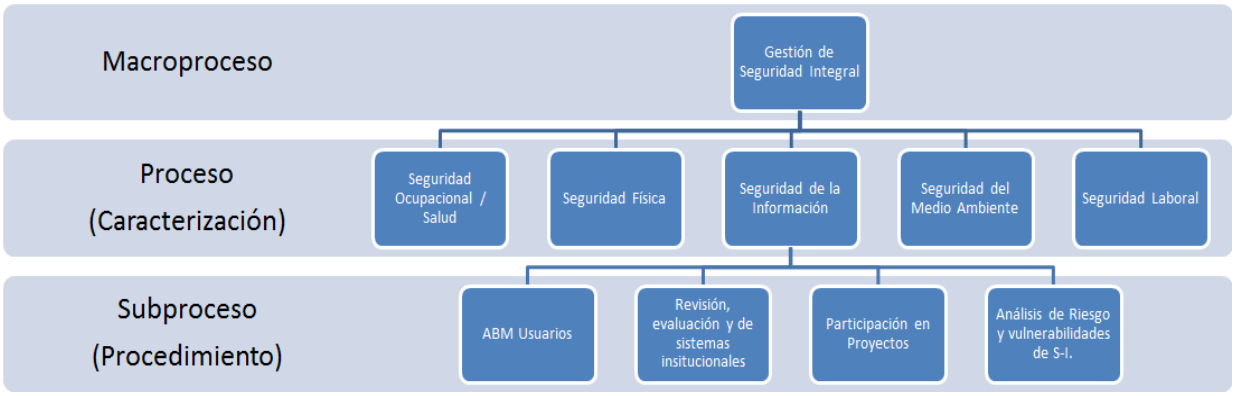


Figura 14: Estructura Organizacional SI Propuesto

4.10.1.1. Funciones del área de Seguridad de la Información

1. Establecer y mantener actualizado un sistema de seguridad de la información, para todas las unidades operativas de la ESPE.
2. Desarrollar, mantener, concientizar, promover una cultura de seguridad de la información en los procesos académicos, administrativos, financieros y de terceros.
3. Informar a la coordinación de la Gestión de Seguridad Integral, para su aprobación, el Plan de Evaluación Anual a la Seguridad de la Información, y monitorear su ejecución.
4. Evaluar e informar los resultados del cumplimiento de controles, políticas y normas de seguridad de la información.
5. Desarrollar, mantener y ejecutar un marco de trabajo, norma o estándar de seguridad de la información en la institución
6. Difundir entre la comunidad politécnica las políticas y normas de seguridad, así como de su estricto cumplimiento.
7. Promover la aplicación de metodologías de trabajo en las fases de planificación, ejecución, evaluación y actualización de las acciones de preservación y protección de los activos claves de la organización

4.10.1.2. Funciones del ABM Usuarios

1. Diseñar, implementar y mantener un sistema de administración de roles y perfiles de accesos y privilegios, para el uso de los activos y aplicaciones informáticas de la institución.
2. Mantener los usuarios, passwords y accesos a los sistemas de información.
3. Establecer acuerdos de confidencialidad con los usuarios.
4. Preparar los informes de evaluación y control, que contengan observaciones, conclusiones y recomendaciones

4.10.1.3. Funciones de la revisión, evaluación y mantenimiento

1. Monitorear constantemente la implementación y el uso de los mecanismos de seguridad de la información.
2. Recibir, Revisar, Investigar y responder a informes y actividad sobre incidentes de seguridad. (CSIRT)
3. Revisar logs de auditoría y los sistemas de detección de intrusos.
4. Analizar y especificar los requisitos de seguridad para su adquisición, desarrollo y mantenimiento de sistemas de información.
5. Preparar los informes de evaluación y control, que contengan observaciones, conclusiones y recomendaciones.

4.10.1.4. Funciones de la participación en proyectos

1. Participar en los proyectos relacionados con TI, agregando todas las consideraciones de seguridad de la información.
2. Establecer criterios, modelos y marcos de referencia de seguridad de la información en todas las fases del proyecto.

3. Preparar los informes de evaluación y control, que contengan observaciones, conclusiones y recomendaciones.

4.10.1.5. Funciones del análisis de riesgo y vulnerabilidades del S-I

1. Definir la planificación para la continuidad del negocio
2. Promover el desarrollo de una cultura de prevención y mitigación oportuna de riegos
3. Monitorear las actividades de riesgo en la gestión institucional, planificadas anualmente
4. Preparar los informes de evaluación y control, que contengan observaciones, conclusiones y recomendaciones.

En cada una de las unidades operativas de la Comunidad Politécnica, se designará una persona que será Responsable de Seguridad de la Información y de la implementación de la política. El director de la UO, brindará todo el apoyo necesario para el correcto cumplimiento de las funciones del Responsable de Seguridad de la Información en la UO.

4.10.2. Separación de roles y responsabilidades

A fin de minimizar el riesgo de abuso de privilegios y maximizar la habilidad de las personas que controlan las tareas de otros, estas deben ser separadas enfocándose al principio de segregación de funciones, algunos roles serán ejercidos por diferentes individuos o grupos, como por ejemplo: Administración de acceso, uso normal de los sistemas y aplicaciones, auditoria y administración de la seguridad.

4.10.3. Propietario de la información

Todo miembro de la Comunidad Politécnica será propietario de una determinada información, este debe ser responsable de su clasificación y garantizar el cumplimiento de la integridad, disponibilidad y confidencialidad de la misma.

4.10.4. Usuarios

Los usuarios son los custodios de la información que crean, almacenan, modifican, eliminan por tal motivo deberán cumplir con la Política que respecta a uso y administración. Los directivos, docentes, servidores públicos, alumnos entre otros serán informados regularmente sobre las políticas y estándares existentes, y de ser el caso; recibirán la capacitación respectiva.

4.10.5. Terceros involucrados

Los terceros involucrados (Proveedores) deberán cumplir con los lineamientos descritos en la Política de Seguridad de la Información.

4.10.6. Responsables de seguridad se la información de la ESPE

El RSI[16] es el líder de todas las actividades relacionadas con la seguridad de la información. Entre las actividades principales están:

- ✓ Coordinar las actividades relacionadas a la seguridad
- ✓ Reportar las novedades directamente al Director del Departamento de Seguridad Corporativa
- ✓ Iniciar nuevos procesos de seguridad, y su estado

[16] RSI: Responsable de la Seguridad de la Información

- ✓ Resolverá posibles conflictos entre la Política de Seguridad y los requerimientos locales de cada área.

Las responsabilidades principales son:

- ✓ Supervisar la implementación del programa de Seguridad de la Información
- ✓ Actualizar la Política y normas de Seguridad de la información
- ✓ Promover la concientización de la Seguridad de la información,
- ✓ Definir un marco de referencia, para los responsables de seguridad dependientes.

4.10.7. Responsable de seguridad de la información en cada área

Será responsable de la implementación de la Política de Seguridad de la Información y de los procesos y mecanismos resultantes en su área. Se deberá comunicar directa y regularmente con el Responsable de Seguridad de la Información de la ESPE, por tal motivo sus responsabilidades son similares:

- ✓ Contactar al Responsable de Seguridad de la Información del Grupo
- ✓ Asegurar que los aspectos relacionados con la seguridad sean considerados durante los procesos de contratación
- ✓ Mantener monitoreado la implementación y uso de los mecanismos de seguridad de la información

4.10.8. Auditoria interna

La principal responsabilidad será evaluar si la consistencia de los mecanismos de seguridad implementados se ajusta con los requerimientos y los lineamientos del plan estratégico de la ESPE.

4.10.9. Administrador de los sistemas

El Administrador de Sistemas deberá garantizar las prestaciones del servicio, de acuerdo a los lineamientos y a las normas establecidas en la ESPE.

4.10.10. Personal

Los nuevos funcionarios que se incorporen a la institución, deberán ser capacitados respecto de la sensibilidad de los Sistemas de Información y la información que este bajo su control. Como valor agregado se deberá establecer periódicamente jornadas de concientización de la necesidad de la Seguridad de la Información en toda la Comunidad Politécnica.

4.11. Políticas de aspectos organizativos de la seguridad de la información

La gerencia de seguridad de la información, debe apoyar activamente en el cumplimiento de la política de seguridad, así como en las recomendaciones de las mejores prácticas para el uso de sistemas y recursos informáticos. Las disposiciones claras y explícitas deben demostrar compromiso y reconocimiento a fin de alcanzar los objetivos planteados en la presente política.

4.11.1. Objetivo

Establecer una estructura de gestión para iniciar y controlar la implantación de la seguridad de la información a fin de gestionarla dentro de la ESPE.

4.11.2. Normas generales de operación

4.11.2.1. Base legal

Los documentos legales y aprobados por la institución, se encuentran en el portal institucional **MIESPE** (https://miespe.espe.edu.ec), en la opción **ENLACES DE INTERÉS.**

- Política de Seguridad de la Información.
- Código de Ética
- Normas de control interno
- Reglamentos y resoluciones

4.11.2.2. Normas Generales

- Los nuevos recursos tecnológicos deberán obtener la aprobación de un profesional que sea el responsable del mantenimiento del entorno de seguridad del sistema de información, certificando que cumple con las políticas y requisitos de seguridad de la información establecidos.
- Se debe comprobar que el nuevo hardware o software sea compatible con los demás dispositivos del sistema instalados en la ESPE.
- Los equipos personales (laptops, tabletas, celulares, entre otros) deben ser sujetos de una evaluación, control y autorización previa a su uso, ya que estos pueden ser un foco de nuevas vulnerabilidades.

4.12. Política de seguridad

4.12.1. Política de seguridad de la información

La gerencia de la ESPE debe establecer un marco de trabajo para la Comunidad Politécnica, el cual se enfoque al cumplimiento de políticas, apoyo y

compromiso a las actividades relacionadas en mantener un control de protección de la seguridad de la información.

4.12.1.1. Objetivo

- Establecer la dirección y apoyo gerencial a fin de establecer lineamientos de seguridad de la información para la ESPE.

4.12.1.2. Documento de política de seguridad de la información

La UTIC, debe gestionar la aprobación y publicación de las políticas de seguridad como de la comunicación entre el personal de la Comunidad Politécnica y terceros. La UDI, como ente de control de la ESPE deberá manifestar su compromiso y establecer el enfoque de la ESPE con respecto a la gestión de la seguridad de la información. Se debe considerar:

a) La información es un activo que representa un valor muy importante para la institución, como consecuencia debe ser protegido. La seguridad de la información se encuentra enfocada a proteger los datos contra amenazas, con la finalidad de garantizar la continuidad de las actividades académicas, administrativas, investigativas y de vinculación con la comunidad de la ESPE. La información, se puede presentar en diferentes formas; impresa o escrita, digital, transmitida utilizando servicios electrónicos, en imágenes o expuestas oralmente.
b) Es responsabilidad de todos los miembros de la Comunidad Politécnica; el fiel cumplimiento de las políticas, así como del respectivo apoyo de la UDI; a los objetivos y principios fundamentales de la seguridad de la información.
c) El desarrollo de las políticas de seguridad se encuentran alineadas a las mejores prácticas que sugiere la norma ISO/IEC 27002. A fin de cumplir

con el alcance de la investigación propuesta, se desarrollaron las políticas en relación a los siguientes dominios:

a. Dominio (1): Política de Seguridad.
b. Dominio (6): Gestión de Comunicaciones y Operaciones.
c. Dominio (8): Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.
d. Dominio (10): Gestión de la Continuidad del Negocio.

d) Esta política, debe ser difundida a todos los usuarios de la ESPE de manera pertinente, accesible y comprensible.

4.12.1.3. Revisión de la Política de Seguridad de la Información

La institución, debe definir la unidad responsable del SGSI el cual sea responsable del mantenimiento y revisión de la política de seguridad de la información. El SGSI debe garantizar que se lleve a acabo una revisión periódica en respuesta a cualquier cambio que pueda afectar la base original de evaluación de riesgos como los incidentes de seguridad, vulnerabilidades detectadas en la red, cambios sobre la infraestructura técnica de la ESPE, acciones a tomar sobre el personal que salga de la institución, entre otros.

a) Se debe registrar datos estadísticos de incidentes de seguridad detectados, accesos no autorizados a las aplicaciones de la ESPE, logs y pistas de auditoría, entre otros, que verifiquen los controles realizados por el SGSI.
b) Se debe establecer costos y ventajas de la implementación de los controles en las actividades administrativas, académicas, de investigación y vinculación que realiza la ESPE.
c) Se debe establecer efectos provocados por la implementación de los controles sobre los Recursos de TI de la institución.

4.13. Políticas de Comunicaciones y Operaciones

4.13.1. Procedimientos y responsabilidades operativas

Se debe considerar la asignación de las responsabilidades y procedimientos para la gestión y operación de las instalaciones de procesamiento de información, esto referencia el desarrollo de instrucciones operativas y procedimientos apropiados para la respuesta de incidentes.

Adicionalmente, se debe implementar la separación de funciones; a fin de reducir el riesgo por el uso inadecuado o deliberado de los recursos de TI de la ESPE.

4.13.1.1. Objetivo

- Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información.

4.13.1.2. Documentación de los procedimientos operativos

La UTIC se encuentra en la obligación de documentar y mantener actualizados los procedimientos operativos identificados por su política de seguridad, estos deben ser considerados documentos formales y sus cambios deberán ser autorizados por la unidad de control pertinente, la UDI.

Los procedimientos operativos deben especificar claramente cada tarea, con la inserción de:

a) Procesamiento y el correcto uso de la información

b) Requerimientos de programación en lo que se incluya la interdependencia con otros sistemas de TI.
c) Normativas para la gestión de errores o eventos inesperados que podrían presentarse durante la ejecución de las tareas. Se deben restringir el uso de herramientas propias del sistema.
d) Contactos de terceros (proveedores, personal técnico) a los que se los pueda localizar en caso de presentarse dificultades operativas o técnicas que no hayan sido previstas.
e) Acciones de reinicio del sistema y procedimientos de recuperación en caso de presentarse fallas.

Se deben elaborara documentos sobre procedimientos referidos a las actividades de mantenimiento e instalaciones relacionadas a las aplicaciones de la información y comunicaciones, por ejemplo:

a) Procedimientos generales de inicio y cierre de los mantenimientos o instalaciones.
b) Respaldos de la información, previo a la ejecución de las actividades
c) Seguridad en la manipulación de la información

4.13.1.3. Control de cambios en las operaciones

Es importante que se mantengan controles sobre los cambios en los sistemas, mantenimientos e instalaciones de procesamiento de información, en virtud de que el control inadecuado de los cambios tiene como consecuencia las fallas de seguridad sobre los sistemas de información de las organizaciones.

En la UTIC se deberán designar responsabilidades y procedimientos formales aprobados los cuales permitan garantizar un control satisfactorio de los cambios que se realicen sobre el hardware y software disponible en la institución.

Toda aplicación disponible para uso de la Comunidad Politécnica podrá ser sujeta a un control estricto de cambios, por tal motivo; cuando una aplicación cambie, se debe obtener un registro que contenga toda la información relevante.

Para el control de cambios en las operaciones y aplicaciones, se debe:

a) Identificar y documentar los cambios significativos
b) Evaluar los posibles impactos que se puedan presentar al ejecutar los cambios
c) Aprobar los procedimientos formales de los cambios propuestos
d) Sociabilizar detalladamente, entre los afectados, los cambios propuestos; así como los posibles impactos detectados previamente
e) Identificar procedimientos que permitan cancelar los cambios debido a eventos fallidos e inesperados. Recuperación de los sistemas a un estado inicial.

Adicionalmente, se debe tomar en consideración que el control de cambios en las operaciones y aplicaciones se encuentre integrado con los procedimientos de control de cambios del dominio (8): Adquisición, desarrollo y mantenimiento de sistemas.

4.13.1.4. Procedimientos de manejo de incidentes

La UTIC, debe establecer responsabilidades y procedimientos adecuados para el correcto manejo de incidentes, con el fin de garantizar a la Comunidad Politécnica una respuesta rápida, eficaz y sistemática a los incidentes de seguridad que puedan presentarse, para lo cual se deben considerar los siguientes controles:

a) Establecer procedimientos que contemplen los probables incidentes que puedan presentarse en la institución:

   i. Ataques a los servicios de red datos institucionales (DoS)
   ii. Indisponibilidad de los sistemas de información
   iii. Pérdida de fluido eléctrico en el Data center
   iv. Mal uso de los recursos de TI por parte de los usuarios
   v. Pérdida de confidencialidad e integridad de la información

b) Adicionalmente al plan de contingencia, se deben establecer procedimientos que garanticen la recuperación de los sistemas en el menor tiempo posible:

   i. Identificación del origen de la incidencia
   ii. Analizar la incidencia ocurrida
   iii. Implementar una solución que evite la ocurrencia de la misma incidencia en otra ocasión
   iv. Registrar la solución de la incidencia en una base de conocimiento predefinida por la UTIC
   v. Analizar logs del sistema y pistas de auditoria
   vi. Difundir el incidente y la solución entre los ingenieros de la UTIC que se encuentren involucrados con un determinado sistema o servicio
   vii. Informar al director de TI sobre el incidente, tiempo de indisponibilidad (en caso de presentarse), impactos provocados por la incidencia y la solución empleada.

c) Los responsables de cada sistema o servicio deberán proteger los logs, pistas de auditoria y evidencia similar, la cual permita:

i. Identificar y analizar inconvenientes internos de los sistemas o servicios, esta información es útil tanto a los propios técnicos de la UTIC como a proveedores.
ii. Presentarlos como evidencia ante posibles procesos judiciales, civiles o criminales, o simplemente como un requisito establecido en las normativas internas de la institución

d) Es responsabilidad de la UTIC, plantear controles formales sobre las acciones adoptadas en la recuperación de violaciones de seguridad y de corrección de fallas del sistema:

i. El acceso a los sistemas de información, aplicaciones, servicios de red y demás recursos de TI, estará autorizado solo para usuarios de la Comunidad Politécnica y terceros. Éste ítem tienea relación con el objetivo de control Seguridad en los Accesos a Terceros del Dominio (2): Aspectos organizativos de la Seguridad de la información.
ii. Las soluciones emergentes, deben ser documentadas detalladamente y registradas en la base de conocimiento. Adicionalmente, estas acciones deben ser informadas a la dirección de TI y revisadas periódicamente.
iii. Revisar en un plazo mínimo la integridad de los controles y de los sistemas de información, aplicaciones y servicios institucionales.

4.13.1.5. Separación de funciones

Dentro de la UTIC se requiere realizar una separación de funciones, lo cual permitirá reducir el riesgo de mal uso, accidental o deliberado de los recursos de TI. Se debe considerar la separación de la gestión de acuerdo al área de

responsabilidades; con la finalidad de reducir las oportunidades de modificación no autorizada.

En caso de que para la UTIC éste método de control sea difícil de cumplir, se debe emplear otros controles como el monitoreo de las actividades, análisis de pistas de auditoría y la supervisión de la dirección de TI. Para la separación de funciones se deben considerar los siguientes puntos: connivencia

a) Es importante separar actividades que puedan ser consideradas foco de fraude.
b) Los controles deben ser diseñados de manera tal que; al menos dos personas estén involucradas en reducir la posibilidad de fraude, a través de conspiración.

4.13.1.6. Separación de los recursos de desarrollo e instalaciones operativas

La UTIC debe establecer una separación entre las instalaciones de desarrollo, prueba y operaciones a fin de detallar los roles de cada uno de los involucrados, para lo cual se debe definir y documentar las normativas para la publicación del sistema; desde el estado de desarrollo hacia el estado operativo.

La separación de las instalaciones se la debe realizar ya que las actividades que se realizan durante su desarrollo y pruebas pueden ocasionar problemas que compliquen el desempeño normal de los sistemas. Adicionalmente, se debe separar los ambientes (desarrollo, pruebas y operativos) con la finalidad de reducir los inconvenientes operativos en las aplicaciones y servicios institucionales; que se encuentren en producción. En este caso, se debe considerar la necesidad de implementar un ambiente en el cual se realicen pruebas significativas al cual se limite el acceso de los técnicos de desarrollo.

Esta separación de ambientes se la debe realizar en virtud de que, los ingenieros de desarrollo y de pruebas tienen el acceso a las aplicaciones que están operativas y por ende a su información; ingresando líneas de códigos no autorizados o no probados provocando la alteración de los datos de las operaciones. Adicionalmente, la exclusión de esta separación puede ser considerada como una amenaza a la confidencialidad de la información.

El mantener unificado los ambientes de desarrollo, pruebas y operaciones pueden provocar cambios no planificados en las aplicaciones y en la información. Por todo esto es imperiosa la separación de los ambientes, con la finalidad de minimizar el riesgo de cambios accidentales o accesos no autorizados al software operativo y a los datos de la institución, para lo cual se debe tener en consideración los siguientes controles:

a) El software de desarrollo y el que se encuentre en operación (producción), deberán ejecutarse sobre equipos físicos o bajo ambientes virtuales separados y que se encuentren en subredes diferentes.
b) Se debe detallar y documentar las actividades de desarrollo y de pruebas ya que estas deberán ser separadas e independientes.
c) No se podrá acceder y/o ejecutar aplicaciones o herramientas que permitan compilar código fuente, editores y otros utilitarios similares.
d) Se deberán utilizar diversos métodos de autenticación y conexión para las aplicaciones que se encuentren operativas y de prueba.
e) Se deberán promover a los usuarios a utilizar distintas contraseñas para el acceso a los sistemas. Los desarrollos deben contemplar que los menús muestren mensajes que describan su funcionalidad.

4.13.1.7. Administración de instalaciones externas

Actualmente, la ESPE mantiene contratos con terceros (proveedores) para mantenimientos, soportes y garantías de equipos de procesamiento de información considerados como críticos; sin embargo, esto puede ser un potencial de riesgo en el ámbito de seguridad. Es responsabilidad de la UTIC establecer e identificar los riesgos con la debida anticipación y debe acordarse formalmente los controles adecuados. Para el cumplimiento de este control se debe tener relación con el Dominio (2): Aspectos Organizativos de la Seguridad de la Información, el objetivo con de control: Seguridad en los Accesos a Terceros, los controles: Identificación de los riesgos derivados del acceso de terceros y Requisitos de seguridad en contratos con terceros (Outsourcing). Los acuerdos deben:

a) Identificar las aplicaciones sensibles o críticas que considere la UTIC mantener un contrato con terceros.
b) Obtener la aprobación de los responsables de las aplicaciones.
c) Establecer estándares de seguridad y definir un proceso de medición del cumplimiento
d) Asignar responsabilidades específicas y procedimientos que permitan monitorear las actividades de seguridad pertinentes.
e) Definir responsabilidades y procedimientos de comunicación y manejo de incidentes relativos a la seguridad de la información, en referencia al numeral 4.12.1.4 de esta investigación.

4.13.2. Planificación y aceptación del sistema

Se requiere una planificación y preparación anticipada que garantice la disponibilidad de capacidad y recursos adecuados, por lo que se debe realizar proyecciones para futuros requerimientos de capacidad para evitar una sobrecarga de los sistemas.

La UTIC; debe definir, documentar y hacer aprobar los requerimientos operativos de nuevos desarrollos o adquisición de sistemas antes de que estos sean aprobados y usados.

4.13.2.1. Objetivo

- Reducir las fallas en la operación de los sistemas

4.13.2.2. Planificación de la capacidad

Los responsables de cada sistema, aplicación, servicios, entre otros; deben mantener un monitoreo del crecimiento de la capacidad y las respectivas proyecciones a los futuros requerimientos, esto garantizará la disponibilidad de cada uno de ellos, tanto en procesamiento como en almacenamiento.

Para las proyecciones; los ingenieros responsables de los recursos de TI deben tomar en consideración las necesidades de la Comunidad Politécnica y de las tendencias globales, en función al nivel de procesamiento de cada una de ellos.

Las proyecciones que se realicen sobre la demanda de recursos de cada uno de los sistemas permitirán a la institución garantizar uno de los principios fundamentales de la seguridad de la información, evitando cuellos de botellas que pueden ser considerados como amenazas a la seguridad del sistema, aplicaciones, servicios de red, entre otros y principalmente planificar una adecuada acción correctiva.

4.13.2.3. Aceptación del sistema

Para la aceptación de nuevos desarrollos, adquisiciones, actualizaciones, implementación de nuevas versiones de sistemas de información para la ESPE, se deberán ejecutar pruebas que permitan avalar su aprobación, se deberá verificar lo siguiente:

a) Cumplimiento de las capacidades del hardware
b) Recuperación de errores y procedimientos de reinicio, y planes de contingencia
c) Pruebas de funcionalidad y operativos requeridos por la institución
d) Implementación y pruebas de controles de seguridad
e) Pruebas de continuidad del negocio, referenciando el Dominio (10): Gestión de la Continuidad del Negocio, el objetivo de control: aspectos de la gestión de la continuidad del negocio
f) Impacto que puede ocasionar el nuevo sistema sobre los recursos operativos de la institución
g) Capacitación y transferencia de conocimiento a los usuarios involucrados.

4.13.3. Protección contra software malicioso

La UTIC, debe considerar las medidas que permitan prevenir y detectar la introducción de software malicioso. La instalación descontrolada de sistemas y el desconocimiento de su origen provocan que sean vulnerables ante aplicaciones maliciosas como: virus informáticos, gusanos informáticos y virus “troyanos”.

Adicionalmente, para el fiel cumplimiento de este objetivo, es importante que se realicen jornadas concientización, a la Comunidad Politécnica y terceros, sobre los peligros de instalar software no autorizado o malicioso, enfatizando

sobre las precauciones que se deben tomar para detectar y prevenir virus informáticos en los computadores personales.

4.13.3.1. Objetivo

- Mantener la integridad de los sistemas de información de virus informáticos y software malicioso.

4.13.3.2. Protección contra software malicioso y descargable

La UTIC, deberá implementar los controles necesarios que permitan detectar y prevenir la introducción no autorizada de software malicioso y los correspondientes procedimientos que deben acatar los usuarios de la Comunidad Politécnica. Los controles a implementarse; deberán ser orientados a la concientización de la seguridad de la información, acceso a los sistemas y a la administración de cambios. Se describen los controles a ser tomados en cuenta:

a) Se deberá desarrollar una política formal en la que se indique la prohibición de usar software que no este autorizado y licenciado por la ESPE. Este control se lo deberá referenciar con el dominio (11): Cumplimiento, objetivo de control: Cumplimiento de los requisitos legales, control: Derechos de propiedad intelectual (DPI).
b) Desarrollar una política formal que tenga como fin eliminar los riesgos relacionados con la obtención de archivos y software, a través de redes externas de la ESPE o medios extraíbles; estableciendo medidas de protección que deberían tomarse. Este control se lo debe referenciar al dominio (8): Adquisición, desarrollo y mantenimiento de sistemas, objetivo de control: Seguridad en los procesos de desarrollo y soporte, el control: Desarrollo externo del software.

c) La UTIC, deberá instalar software de antivirus; con la finalidad de detectar y prevenir virus en los computadores personales de los usuarios de la Comunidad Politécnica. Se deberá planificar y registrar mantenimientos y actualizaciones periódicas del software de antivirus.
d) Se deberá realizar revisiones periódicas y depuración de software y de información que respaldan procesos críticos de la ESPE, será responsabilidad de la UTIC realizar investigaciones formales sobre instalaciones o actualizaciones no autorizadas.
e) Se deberá verificar la presencia de posible virus informáticos que se encuentren presentes en archivos de medios de almacenamiento extraíbles, que no haya sido identificado o autorizado su origen.
f) Se deberá verificar la presencia de virus informáticos que se encuentren presentes en archivos enviados a través de correo electrónico o que sean objetos de descarga de internet, este control se lo debe realizar antes de ejecutar el archivo. Será responsabilidad de la UTIC implementar una herramienta que permita este análisis en servidores de correo electrónico, computadores personales o al momento de acceder a la red institucional.
g) Se deberá establecer procedimientos y definir responsabilidades que gestionen la protección de virus sobre los sistemas, capacitación sobre su uso y principalmente la recuperación frente a ataques recibidos.
h) Se deberá establecer procedimientos que permitan identificar toda la información sobre software malicioso, y garantizar que correos informativos institucionales sean exactos.
i) Se deberá establecer medidas de recuperación y continuidad del negocio respecto a ataques de virus.

4.13.4. Copias de seguridad

La UTIC, deberá establecer procedimientos de respaldos de información y su respectiva restauración, registrar eventos, eventos y fallas, mantener un monitoreo continuo del entorno del equipamiento; con la finalidad de establecer una estrategia de respaldos adecuada.

4.13.4.1. Objetivo

- Garantizar la integridad, confiabilidad y disponibilidad de los sistemas de información y comunicación de la UTIC.

4.13.4.2. Copias de Seguridad de la Información

Se deberá obtener periódicamente respaldos de la información crítica y de la configuración de los servicios esenciales para la ESPE, para lo cual la UTIC deberá contar con las instalaciones que permitan garantizar que la información y los sistemas de información y comunicación puedan ser recuperados en caso de ocurrencia de un desastre o falla de los dispositivos.

Para el correcto desempeño de resguardo de cada uno de los sistemas de información, estos deberán ser probados periódicamente, lo cual permitirá probar el cumplimiento de los requerimientos de los planes de continuidad del negocio.

Para el correcto proceso de copias de seguridad de la información, se deben tener en cuenta los siguientes controles:

a) Se deberá definir una ubicación externa a la ESPE (Campus Matriz) con el objetivo de almacenar los respaldos de los sistemas de información y

comunicación. Deberá existir una distancia suficiente que permita evitar daños provocados por desastres naturales o externos.

b) Se deberá registra completamente los copias de seguridad y los correspondientes procedimientos documentados de restauración.
c) Los respaldos de seguridad de la información, deben contar con un nivel adecuado de protección física y ambiental, como referencia se debe tener en consideración el dominio (5): Seguridad Física y del Entorno.
d) Las pruebas de resguardo de la información garantizarán la confiabilidad de los resguardos de la información. Estas deberán ser sujetas a una periodicidad, siempre y cuando estas sean factible de su ejecución.
e) Se deberán verificar los procedimientos de restauración, estos deben verificarse y probarse (periódicamente) lo cual permitirá garantizar la eficacia y cumplimiento dentro del tiempo asignado a la recuperación en las actividades operativas.
f) La UTIC deberá determinar el período de almacenamiento de los archivos de información y de las configuraciones en la ubicación alterna.
g) Los registros de actividades deben contemplar un formato como el que se muestra en el Anexo 6. Los registros podrán ser sujetos a verificación por la dirección de TI.

   Anexo 6: Registro Copias de Seguridad de la Información
h) Se deben comunicar las fallas y las medidas correctivas tomadas. Se deberán registrar las fallas presentadas durante la ejecución de los procedimientos de respaldos de los sistemas de información y comunicación, restauración de los mismos y su correspondiente operatividad.

4.13.5. Gestión de la Seguridad de Redes

Es de suma importancia para la ESPE, mantener la administración sobre la seguridad de las redes que pueden atravesar el perímetro de la institución y

determinar controles que aseguren la información sensible que circule por redes públicas.

4.13.5.1. Objetivo

- Garantizar la seguridad de la información en las redes y la protección de la infraestructura.

4.13.5.2. Controles de redes

La UTIC, a través de la Administración de Servicios de Redes y Comunicaciones deberá desarrollar controles que garanticen la seguridad de datos y la protección de los servicios a los que tienen acceso los usuarios de la Comunidad Politécnica. Se deben considerar los siguientes puntos:

a) El desempeño y operación de la red de datos institucional deberá ser, en su mayoría, separada de acuerdo a lo mencionado en el literal 4.12.1.5 de la presente investigación.
b) Se deberán definir los procedimientos y las responsabilidades para la administración remota de los equipos de comunicación y networking, incluyendo los de acceso.
c) Se deberán establecer controles que aseguren la información que se transmite a través de redes públicas, con la finalidad de cumplir los principios fundamentales de seguridad de la información. Este control se lo debe referenciar con:
    a. Dominio (7): Control de Acceso, objetivo de control: Control de Acceso a la Red.
    b. Dominio (8): Adquisición, desarrollo y mantenimiento de Sistemas de Información, objetivo de control: Controles Criptográficos.

d) Las actividades de la dirección de TI, deberán estar relacionadas en optimizar los servicios a la actividad de la empresa, garantizando la ejecución de los controles sobre los recursos de procesamiento de la información de la ESPE.

4.13.5.3. Seguridad de los servicios de red

.

La UTIC, entrega a la Comunidad Politécnica un amplio catálogo de servicios de red; tanto privados como públicos, en tal virtud será su responsabilidad proveer una clara descripción de los atributos de seguridad de los servicios de red disponibles en la institución.

4.13.6. Manipulación de los Soportes

La UTIC, debe establecer procedimientos operativos apropiados para proteger documentos, medios de almacenamiento (cintas, discos, pen drives, entre otros), información de entrada/salida y documentación del sistema contra daño, robo y acceso no autorizado. Adicionalmente, es relevante la protección física de esto tipo de medios extraíbles.

4.13.6.1. Objetivo

- Minimizar el daño de los activos y las interrupciones en las actividades académicas, administrativas e investigativas de la ESPE.

4.13.6.2. Gestión de soportes extraíbles

Se deben definir procedimientos que definan el uso medios de almacenamiento externos tales como: cintas, discos duros externos, pen drives, CDs o DVDs. Se considera lo siguiente:

a) La información disponible en los medios de almacenamiento que ya no sean utilizados o que salgan de la ESPE, debe ser borrada o destruida (CDs o DVDs).
b) Se deberá registrar la salida de los medios de almacenamiento extraíbles que salgan de la institución; con la finalidad de mantener pistas de auditoría, de acuerdo a lo referenciado con el objetivo de control de soportes físicos en tránsito, del presente dominio.
c) Todos los medios extraíbles deberán ser almacenados en un ambiente físico seguro y protegido, a fin de garantizar los principios fundamentales de la seguridad de la información.
d) Se deberá gestionar la autorización de los procedimientos para el manejo de medios extraíbles.

4.13.6.3. Retirada de soporte

Los medios de almacenamiento extraíble cuando ya no son utilizados; deben ser retirados manteniendo un control adecuado, caso contrario, en caso de pérdida; la información crítica puede filtrarse entre personas ajenas a la institución.

Se deben considerar los siguientes controles:

a) Los medios extraíbles que contienen información sensible, deberán ser almacenados y eliminados siguiendo procedimientos seguros.
b) Los siguientes ítems podrían requerir una eliminación segura:

    a. Documentos en papel
    b. Grabaciones con información referente a la ESPE
    c. Documentos institucionales (Informes, decretos, resoluciones entre otros).

d. Cintas magnéticas
e. Discos o pen drives.
f. Medios de almacenamiento óptico
g. Listados de programas
h. Datos de prueba
i. Documentación referente a configuraciones de los sistemas

c) Se deberá registrar la eliminación de la información sensible, con la finalidad de mantener pistas de auditoría.
d) La UTIC, debe considerar el efecto de acumulación, que puede ocasionar que una gran cantidad de información no clasificada se torne más sensible que una pequeña cantidad de información clasificada.

4.13.6.4. Procedimientos de manipulación de la información

Se deberá establecer procedimientos para la manipulación y almacenamiento de la información; con la finalidad de protegerla contra el uso inadecuado y/o su divulgación no autorizada. Los procedimientos deberán ser enfocados de acuerdo a la clasificación de la información (ítem 4.9 de este documento). Se deben considerar los siguientes controles:

a) La UTIC, deberá manejar, estandarizar y mantener la rotulación de todos los medios extraíbles.
b) Se deberá restringir el acceso a los medios, a personas que no se encuentren debidamente autorizadas e identificadas para accederlos.
c) Se debe elaborar y mantener un registro formal de los usuarios autorizados para la recepción de la información.
d) Se debe verificar y garantizar que el ingreso de la información a los sistemas de información sea completa y coherente a los sistemas de

información. Este procedimiento también será aplicable para la información de salida.

e) Se debe almacenar los medios extraíbles en ambientes físicos que recomienden los proveedores y fabricantes, con la finalidad de asegurar su integridad física.
f) Los respaldos de la información deben ser claramente identificados a fin de que estas sean verificadas por el receptor autorizado.

Anexo 7: Acta de Confidencialidad

4.13.6.5. Seguridad de la documentación del sistema

La documentación de los sistemas puede contener información considerada como sensible, como por ejemplo: Descripción de procesos de aplicaciones, procedimientos, estructuras de datos, procesos de autorización; los cuales se encuentran referenciados con el dominio (7): Control de Accesos, el dominio de control: Requisitos de negocio para el control de acceso, entre otros. Se debe considerar los siguientes controles que garanticen la protección de documentación del sistema de accesos no autorizados.

a) Se debe verificar que la documentación del sistema sea almacenada de manera segura
b) Se debe restringir al máximo el acceso a la documentación del sistema. El propietario del sistema de información, aplicación y/o servicio es el único en autorizar su acceso.
c) Se debe proteger la documentación del sistema que es accedida o suministrada a través de una red pública.

4.13.7. Intercambio de información

La ESPE, al ser una institución de educación superior, se encuentra en la capacidad de intercambiar información con otras instituciones a fin de promover proyectos de investigación y cooperación, sin embargo; los intercambios deben llevarse a cabo en función de a acuerdos prestablecidos. La UTIC, como unidad que maneja la información; debe establecer procedimientos y estándares que permitan la protección de la información y los medios en tránsito.

4.13.7.1. Objetivo

- Reducir la pérdida, modificaciones o uso inadecuado de la información que intercambian las organizaciones.

4.13.7.2. Políticas y procedimientos del intercambio de información

A fin de dar cumplimiento a este control, se deben definir acuerdos de usos de claves, de confidencialidad, de uso de recursos y sistemas informáticos; para el intercambio de información entre instituciones y/o usuarios. Los parámetros de seguridad de los acuerdos de este tipo deben reflejar el grado de sensibilidad de la información.

4.13.7.3. Acuerdos de intercambio

La UTIC, deberá establecer acuerdos formales por el uso o acceso a los sistemas de información, software, aplicaciones, claves de acceso, entre otros; para su intercambio.

4.13.7.4. Soportes físicos en tránsito

La información es vulnerable a accesos no autorizados, al mal uso o adulteración durante su transporte físico, en tal virtud la UTIC deberá establecer controles que se enfoquen en garantizar los medios informáticos que se transporten de un lugar a otro, principalmente aquellos que contienen un alto grado de sensibilidad como lo es los respaldos de información y archivos de configuración.

a) La ESPE, debe establecer e implementar medios de transporte (mensajería) confiables, en el que se identifiquen los procedimientos para la transportación de información. Estos procedimientos deben ser sujetos de verificación.
b) Se debe prever todas las medidas de seguridad física para la transportación, a fin de garantizar que la integridad de la información no se vea afectada durante el traslado. Es aconsejable se acate las mejores prácticas que sugiere el fabricante o el proveedor.
c) Se deberá considerar la adaptación de controles especiales para la transportación de información crítica con el objetivo de evitar su divulgación o modificación no autorizada. Se pueden considerar los siguientes:

    a. Mantener seguridad física sobre los medios a ser transportados.
    b. Se debe registrar la información de la persona que entrega y recibe la información, lugar de origen y destino.
    c. Mantener un registro de los medios entregados y recibidos.
    d. Se debe realizar un procedimiento de embalaje de los medios e identificarlos con etiquetas que evidencie la prohibición de apertura no autorizada.

4.13.7.5. Mensajería electrónica

Este tipo de mensajería hace referencia al intercambio de información a través de medios electrónicos disponibles en redes públicas como internet. Las nuevas tendencias y la globalización impulsan su utilización, sin embargo son vulnerables a diversas amenazas que pueden tener como consecuencia de actividades fraudulentas, divulgación y/o modificación de la información. La UTIC debe considerar controles de seguridad que consideren la integridad, confidencialidad y disponibilidad:

a) El principio de autenticación, en relación con el acceso a los recursos de TI.
b) La autorización de cada usuario, de acuerdo a sus funciones, para emitir o formalizar documentos que contengan información sensible para la institución.
c) La divulgación de documentos que contengan información referente a procesos de contratación.
d) Documentos que contengan información a transacciones financieras, deberá prevalecer la confidencialidad e integridad de los datos suministrados con respecto a órdenes, pagos y direcciones de entrega y confirmación de recepción.
e) Información de verificación de ejecución de transacciones, antes mencionadas.
f) Documentos que contengan el cierre de las transacciones.
g) La protección que se requiere para mantener la confidencialidad e integridad sobre órdenes de compra.
h) Documentos en el que se designen responsabilidades, a fin de asumir riesgos eventuales en transacciones fraudulentas.

Para el cumplimiento de estas consideraciones, la ESPE debe implementar el uso de mecanismos criptográficos como se recomienda en el dominio (8): Adquisición, desarrollo y mantenimiento de sistemas de información, el objetivo de control: Controles criptográficos.

Los acuerdos de mensajería electrónica, deben ser respaldados por un acuerdo a los responsables al cumplimiento de términos y condiciones descritos. Adicionalmente, la UTIC debe considerar la implementación de acuerdos con terceros.

4.14. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

4.14.1. Requisitos de seguridad de los sistemas

Los acuerdos de mensajería electrónica, deben ser respaldados por un acuerdo a los responsables al cumplimiento de términos y condiciones descritos. Adicionalmente, la UTIC debe considerar la implementación de acuerdos con terceros.

4.14.1.1. Objetivo

La UTIC, debe establecer e identificar los requerimientos de seguridad con la finalidad de aprobarlos previamente al desarrollo de los sistemas de información. Es importante que se consideren todos los parámetros de seguridad, incluyendo, si es el caso; la necesidad de reiniciar la planificación y la ejecución de la adquisición, el desarrollo o mantenimiento de un determinado sistemas de información, para lo cual se requiere cumplir con los siguientes ítems:

a) Sobre todo proyecto de adquisición, desarrollo o mantenimiento de sistemas de información se debe realizar un levantamiento de requerimientos, justificarlos y estos deben ser aprobados por el director de la UTIC, a fin de documentarlos y agregarlos como parte de un sistema de información.

4.14.1.2. Análisis y especificación de los requisitos de seguridad

Se debe sociabilizar entre la Comunidad Politécnica la necesidad de definir los requerimientos para la elaboración de nuevos desarrollos de sistemas o mejoras sobre los existentes en la institución, principalmente en los controles automáticos o manuales que se requieran incorporar.

Los requerimientos de seguridad y los controles deben reflejar un valor agregado de los recursos de TI y realzar el impacto negativo que puede causar sobre la Comunidad Politécnica en caso de falla o falta de seguridad. Es importante considerar que considerar estos controles en una etapa inicial o de diseño serían mucho mas económicos de implementar y mantener para la ESPE, que aquellos que se incluyan post implementación.

4.14.2. Tratamiento correcto de las aplicaciones

La UTIC, en los diseños de desarrollos de aplicaciones debe considerar los controles respectivos y las pistas de auditoría o registros de actividad, los cuales incluyan datos de creación, modificación y salida de datos. Adicionalmente, se puede requerir la implementación de controles sobre sistemas que procesan o tienen impacto en los recursos críticos de la ESPE, para lo cual se debe tomar en consideración la base de requerimientos de seguridad definidos previamente y la evaluación del riesgo.

4.14.2.1. Objetivo

- Prevenir la pérdida, modificación o el uso inadecuado de la información de los usuarios de la Comunidad Politécnica en los sistemas y aplicaciones de información.

4.14.2.2. Validación de los datos de entrada

Con la finalidad de garantizar que la información ingresada a las aplicaciones institucionales sea correcta y coherente, ésta debe ser validada, a través de controles que la analice e identifique, en unaa etapa de diseño y desarrollo. Considerar los siguientes controles respecto a esta validación:

a) Verificación de datos de entrada que permitan detectar:
    a. Identificación de información obligatoria
    b. Control sobre información incoherente
    c. Valores fuera de rango
    d. Ingreso de caracteres inválidos en celdas de datos
    e. Cantidad de datos ingresados que superen el límite inferior o superior permitidos
b) Se debe mantener un control periódico de los contenidos de campos clave o archivos de datos para verificar su validez e integridad.
c) Se debe inspeccionar todos los documentos de entrada, a fin de detectar que no existan cambios no autorizados en la información de entrada. Es importante que todos los cambios en la documentación de entrada sea autorizada.
d) Se debe establecer y registrara las medidas correctivas para corrección de errores de validación

4.14.2.3. Control de procesamiento interno

La información ingresada en las aplicaciones institucionales, puede ser susceptible a vulnerabilidades debido a accesos deliberados. Es de suma relevancia que la ESPE implemente controles de validación con la finalidad de detectar errores que afecten a la integridad de la información.

Los diseños para la adquisición, desarrollo y mantenimiento de aplicaciones deben asegurar que las restricciones se implementen con el objetivo de minimizar los riesgos de fallas de procesamiento, la UTIC deberá considerar lo siguiente:

a) Se debe identificar y registrar las líneas de códigos en las aplicaciones, donde intervengan funciones de inserción, actualización o eliminación de la información o datos.
b) Se debe priorizar el uso de aplicaciones (autorizados) de recuperación de fallas, con la finalidad de garantizar el procesamiento correcto de la información.
c) Se debe prevenir la ejecución de las aplicaciones, cuando se detecta errores en su secuencia de procesamiento.

4.14.2.4. Integridad de los mensajes

La UTIC, debe considerar la verificación de la integridad de mensajes que han sido transmitidos electrónicamente, con el objetivo de detectar cambios no autorizados o alteraciones no autorizadas. Se debe considerar:

a) La UTIC, debe realizar la implementación de una herramienta (Hardware y/o Software) que permita garantizar la integridad de los mensajes transmitidos electrónicamente.

b) Es de importancia realizar una evaluación de riesgos de seguridad que determine la necesidad de implementar la autenticación de mensajes que identifiquen el método más adecuado.
c) Se debe mantener la autenticación de mensajes para aplicaciones en las cuales exista un requerimiento de seguridad, a fin de proteger la integridad de su contenido
d) Se debe implementar una adecuada autenticación de mensajes en la fase de diseño, para prevenir su divulgación no autorizada. Se debe referencia este control con el objetivo de control: Controles criptográficos.

4.14.2.5. Validación de los datos de salida

La salida de la información, desde una aplicación debe ser sujeta a validación con el fin de garantizar que el almacenamiento de su procesamiento sea el mas correcto y adecuado para las circunstancias. Normalmente, las aplicaciones deben ser desarrolladas suponiendo que al llevar una validación, verificación y pruebas, los resultados siempre serán los correctos. La validación de los datos de salida debe incluir:

a) Se debe verificar la coherencia de la información obtenida en los datos de salida.
b) Se debe proveer de información suficiente, a fin de que los usuarios de los sistemas de procesamiento determine la exactitud, totalidad, precisión y clasificación de la información.
c) La UTIC, debe realizar periódicas de validación de salidas de información.
d) Se debe definir las responsabilidades del personal involucrado en el proceso de salida de información.

4.14.3. Controles criptográficos

La institución debe realizar la implementación de sistemas o técnicas criptográficas para la protección de la información sensible y para aquella que otros controles no garanticen una protección eficiente.

4.14.3.1. Objetivo

- Garantizar los principios fundamentales (Confidencialidad, integridad y disponibilidad) de seguridad de la información.

4.14.3.2. Política de uso de controles criptográficos

La ESPE posee información sensible que requiere de una protección especial; a fin de minimizar el riesgo de pérdida, modificación o alteración no autorizada; para lo cual esta en la obligación de implementar técnicas criptográficas. Estas técnicas deben ser sujetas de evaluación para determinar que control debe aplicarse y con que propósito, en función a los procesos institucionales.

La institución, esta en la obligación de cumplir una política que evidencie beneficios y reduzca riesgos que ocasionen el uso técnicas criptográficas utilizadas para evitar un uso no permitido. Considerar lo siguiente:

a) Se debe realizar un análisis de la criticidad de la información que manejan los usuarios o áreas con la finalidad de determinar la necesidad de usar técnicas criptográficas. Es importante destacar que, en caso de requerirlo, la ESPE debe estar en la capacidad de implementar estas técnicas en todas las áreas y departamentos de la institución.

b) Se debe determinar la responsabilidad de la administración de claves, incluyendo los métodos para la recuperación de la información cifrada en caso de que esta haya sido perdida o dañada.
c) Determinar las funciones y las responsabilidades.

4.14.3.3. Gestión de claves

La gestión de claves criptográficas es esencial para el correcto uso de estas técnicas de seguridad, en tal virtud es imperiosa para la ESPE la implementación de un sistema de gestión que permita respaldar su uso por parte de los usuarios de la Comunidad Politécnica, se debe considerar los dos tipos de técnicas criptográficas que se describen a continuación:

a) Técnicas de clave secreta, esta debe ser utilizada cuando: más de un usuario comparte la misma clave y esta es utilizada tanto para cifrarla como para descifrarla. Es importante mencionar que esta clave debe mantenérsela en secreto; dado que una persona que tenga acceso a la misma podrá descifrar toda la información que haya sido encriptada con dicha clave, o agregar información no autorizada.
b) Técnicas de clave pública, esta puede ser revelada a cualquier usuario de la de la Comunidad Politécnica y pueden utilizarse para el cifrado y para la generación de firmas digitales, sin embargo estas deben mantener que controlen su modificación y destrucción.

Las 2 técnicas criptográficas necesitan protección y autorización para su divulgación. Adicionalmente, se debe proveer de protección física al hardware que se utilice para generar y almacenar las claves. Un sistema de gestión de claves debe enfocarse en normas, procedimientos y métodos seguros para:

a) Designar las claves a los usuarios según corresponda. Es importante que se incluya un manual para activar las claves cuando las reciban.
b) Generar y obtener certificados de clave pública.
c) Separar las claves de sistemas criptográficos de otras aplicaciones.
d) Guardar las claves que hayan sido asignadas a los usuarios autorizados.
e) Actualizar o cambiar las claves de los usuarios, en las que se indique un cuando y como pueden hacerlo.
f) Desactivar las claves que haya sido entregada a un usuario de la institución
g) Recuperar las claves en caso de pérdida.
h) Archivar las claves.
i) Destruir las claves en caso de ser necesario.
j) Registrar un log o pistas de auditoría que identifiquen las actividades realizadas con las claves.

4.14.4. Seguridad de los archivos de sistema

La UTIC, debe mantener un control de acceso a los archivos de los sistemas, en consecuencia; garantizar su integridad es responsabilidad del usuario que administra.

4.14.4.1. Objetivo

- Garantizar a la Comunidad Politécnica que los proyectos y las actividades de la UTIC se las realicen de manera segura.

4.14.4.2. Control de software en explotación

A fin de minimizar el riesgo de modificación o alteración del funcionamiento del software que se encuentre en explotación u operación, debe tener en cuenta los siguientes controles:

a) La actualización de las librerías de los Sistemas Operativos debe realizarla únicamente una persona, previa autorización de la dirección de UTIC.
b) En lo posible, los sistemas operativos que se encuentren en producción, únicamente debe almacenar el ejecutable.
c) No se debe implementar un archivo ejecutable en un Sistema Operativo hasta que no se obtenga la evidencia de la satisfacción de las pruebas y del usuario, y una vez que se hayan actualizado sus librerías.
d) Se debe mantener un registro de logs y pistas de las actualizaciones realizadas a las librerías de los sistemas operativos.
e) Se debe mantener “históricos” de las versiones implementadas como medidas de contingencia.

Se debe considerar el mantenimiento y soporte del software provisto por terceros, las actualizaciones de las versiones y parches deben referenciar los parámetros de seguridad establecidos en la ESPE, eliminando y reduciendo posibles vulnerabilidades existentes.

Adicionalmente, el acceso físico y lógico a los proveedores debe ser netamente con fines de soporte, debidamente autenticado y previa autorización de la dirección de UTIC. Es importante que toda actividad que realicen los proveedores deba ser monitoreada.

4.14.4.3. Protección de los datos de prueba del sistema

La información que sea objeto de prueba debe ser protegida y controlada. Las pruebas de aceptación del sistema se las debe realizar con datos muy parecidos a los que se encuentren en producción. Adicionalmente, es relevante evitar el uso de bases de datos que se encuentren en producción y que contengan información personal, caso contrario esta debe ser despersonalizado antes de uso. La UTIC deberá aplicar los siguientes controles que protejan los datos operativos, cuando se utilicen con propósito de pruebas:

a) El control de acceso que se aplique a los sistemas en producción, también se los debe aplicar a los sistemas que se encuentren en pruebas.
b) Se debe informar a la dirección de UTIC y registrar cada vez que se realice una copia de información que se encuentre en producción a un sistema de aplicación en ambiente de pruebas.
c) Una vez restaurada la información en el ambiente de pruebas, se la debe borrar completamente, con la finalidad de que esta pueda ser utilizada por personas no autorizadas.
d) El registro de la copia de la información de los sistemas de producción servirá como pistas de auditoría.

4.14.4.4. Control de acceso al código fuente de los programas

Con la finalidad de reducir la modificación o alteración no autorizada de los programas, el control de acceso al código fuente debe contemplar:

a) No se debe almacenar versiones del código fuente sobre sistemas que se encuentran en producción.

b) Únicamente la persona o grupo de personas autorizada para acceder al código fuente lo podrán hacer, el personal de soporte de la UTIC no debe tener acceso por ningún motivo.
c) Los programas en desarrollo o mantenimiento no podrán ser almacenadas en los sistemas que se encuentren producción.
d) Se debe mantener ambientes seguros para listar los programas que se encuentren en producción.
e) Se debe evidenciar un registro de acceso al código fuentes por parte de las personas autorizadas.
f) Las versiones antiguas de los códigos fuentes deben ser almacenadas debidamente identificadas.

4.14.5. Seguridad en los procesos de desarrollo y soporte

La UTIC, debe establecer controles sobre los entornos de proyectos y su respectivo soporte. Se debe garantizar que todos los cambios sobre los sistemas de información sean revisados con la finalidad de verificar que estos no afecten a la seguridad de la aplicación o del sistema operativo.

4.14.5.1. Objetivo

- Mantener la seguridad de las aplicaciones y de su información.

4.14.5.2. Procedimientos de control de cambios

Se debe minimizar la modificación de los sistemas de información, para lo cual se requiere la implementación y el cumplimiento obligatorio de controles formales de cambios, lo que permitirá a la institución garantizar que la institución no comprometa los procedimientos se seguridad y control, debido a que los ingenieros de soporte deberán acceder únicamente a las partes de los sistemas

que les corresponde para realizar sus actividades y principalmente que obtengan un acuerdo y aprobación formal para ejecutar cambios.

Se deberá referenciar los procedimientos de control de cambios operativos y de aplicaciones con las recomendaciones realizadas en el literal 4.13.1.3 de la presente investigación. Este proceso debe incluir:

a) Se deberá establecer niveles de acuerdo para la autorización de cambios en los sistemas de información.
b) Se debe verificar que los cambios planteados en los sistemas de información, sean realizados por usuarios autorizados en ejecutarlos.
c) Se debe garantizar que la integridad de la información no se vea afectada por los cambios realizados, en tal virtud se deberá verificar los controles y los procedimientos planteados en la UTIC.
d) Se debe identificar todo el software, la información, las entidades de las bases de datos y el hardware que se requieran correcciones.
e) Se debe obtener la autorización formal, previa a la ejecución de cambios.
f) La UTIC, debe garantizar que el usuario autorizado para hacer uso de las aplicaciones, acepte los cambios antes de que se realice su implementación.
g) Se debe garantizar que la implementación de los cambios propuestos, no afecten la disponibilidad de los sistemas de información de la ESPE.
h) Es responsabilidad de la UTIC mantener actualizada la documentación de los sistemas antes y después de una implementación de cambios.
i) Es importante que la UTIC, mantenga un control de versiones de las actualizaciones realizadas en un determinado sistema de información o aplicación.
j) A fin de mantener un control, se debe evidenciar pistas de auditoría de todos los cambios realizados sobre las aplicaciones.

k) La UTIC, debe garantizar a la Comunidad Politécnica que los cambios propuestos se los ejecute en función a una planificación, y que estos no alteren los procesos académicos, administrativos, investigativos de la institución.

4.14.5.3. Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo

Por seguridad informática, se debe evidenciar que los sistemas operativos sean constantemente sujetos a cambios, principalmente por la instalación de parches o instalación de actualizaciones. Como consecuencia, los sistemas de aplicaciones deben ser sujetos de revisión y sometidos a pruebas a fin de evitar que se produzcan incidentes incorrectos que afecten a su seguridad. Este control debe incluir:

a) Se debe mantener una revisión de los procedimientos de integridad y control de los sistemas de información; los cuales permitan evidenciar que estos no hayan sido afectados por los cambios realizados en los sistemas operativos.
b) Se debe incluir en el presupuesto y en la planificación anual de la UTIC, un soporte anual el cual cumplan con revisiones y pruebas de los sistemas que deban realizarse como consecuencia de cambios efectuados en los sistemas operativos. Este control se aplicará para aquellas aplicaciones que no se encuentren en un plan de soporte.
c) Se debe garantizar por la UTIC, que los cambios en los sistemas operativos se los realice antes de ejecutar los cambios propuestos.
d) Los cambios sobre los sistemas de información deben ser contemplados en el plan de continuidad de la UTIC.

4.14.5.4. Restricciones a los cambios en los paquetes de software

Se recomienda que el software suministrado por proveedores (No desarrollado en la ESPE) deba ser utilizado sin modificación a menos que se justifique que es esencial esta contradicción. En caso de requerir modificación se debe considerar lo siguiente:

a) Se debe cumplir con el cumplimiento de compromisos de la seguridad de la información y por ende con los controles establecidos.
b) Las modificaciones deben ser autorizadas por el proveedor, de preferencia se las debe realizar en conjunto. Verificar que se encuentre contemplado en el plan de soporte técnico.
c) Se debe analizar la posibilidad de adquirir al proveedor las actualizaciones referentes a la aplicación, para un tiempo determinado y con la opción de renovar.
d) Si una aplicación requiere necesariamente de modificaciones, se debe aplicar los cambios en un ambiente de prueba, el cual sea una copia exacta del que se encuentra en producción.
e) Se debe garantizar que los cambios aplicados a un sistema fueron probados y documentados exhaustivamente, con la finalidad de que estos se encuentren en la capacidad de aplicarse en un futuro.

4.14.5.5. Externalización del desarrollo de software

La externalización del desarrollo de software debe cumplir con los siguientes puntos:

a) La UTIC debe evidenciar certificados de la realización de trabajos similares (Mayor o igual complejidad) que se hayan realizado en otras organizaciones, preferiblemente en instituciones de educación superior.

b) Se debe establecer acuerdo de propiedad o custodia, esto en caso de que el proveedor cesara sus funciones.
c) La ESPE debe reservarse el derecho de acceso a una auditoría de la calidad de trabajos realizados.
d) Se debe realizar pruebas previas a la instalación, con el fin de detectar código mal intencionado.

4.14.6. Gestión de la vulnerabilidad técnica

La UTIC, debe definir las actividades y responsabilidades de cada uno de los involucrados en la administración de las aplicaciones, con el fin de mantener un seguimiento y control de las vulnerabilidades, analizar los posibles riesgos y establecer un continuo monitoreo y plan de mejora que permita minimizar las vulnerabilidades.

4.14.6.1. Objetivo

- Establecer controles que identifiquen las vulnerabilidades en los sistemas de información.

4.14.6.2. Control de vulnerabilidades técnicas

La UTIC debe establecer un control de las debilidades de los sistemas, el cual se lo registre sobre una base de conocimiento actualizada, a fin de que permita investigar sobre las vulnerabilidades técnicas y minimizar el ataques que atenten contra la confidencialidad, integridad y disponibilidad de la información de la ESPE.

Adicionalmente, se debe definir un tiempo en el que se realicen cambios de básicos de configuración (contraseñas, puertos, accesos, entre otros) lo cual permitirá hacerlo menos vulnerable.

4.15. Gestión de la continuidad del negocio

La institución debe incluir un proceso de gestión de la continuidad del negocio con el fin de reducir las fallas en la disponibilidad de los servicios, aplicaciones y sistemas de información de la ESPE, a causa de desastres naturales, mal funcionamiento de los equipos informáticos y acciones deliberadas con o sin conocimiento de causa.

Se debe establecer un nivel aceptable de disponibilidad, mediante una combinación de controles preventivos y de recuperación de desastre. Adicionalmente, la UTIC debe desarrollar e implementar planes de contingencia que permitan garantizar que los procesos institucionales puedan ser recuperados en los menores tiempos y plazos establecidos. Estos planes deben mantener una revisión constante y vigente a fin de que se conviertan en una parte fundamental del resto de procesos internos de la institución.

La gestión de la continuidad del negocio debe definir controles que identifiquen y reduzcan riesgos, amortiguar las efectos de los incidentes que atenten contra el desempeño normal de los recursos de TI y aseguren la reanudación oportuna de las operaciones críticas.

4.15.1.1. Objetivo

- Mantener la disponibilidad y continuidad de los servicios de TI de la institución y proteger los procesos críticos de fallas significativas o desastres.

4.15.1.2. Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio

Se debe implementar en la ESPE, un proceso controlado para el desarrollo y mantenimiento de la continuidad del negocio, el mismo que debe contemplar los siguientes aspectos para la gestión de la continuidad:

a) Identificación de los riesgos que podría enfrentar la organización en términos de probabilidad de ocurrencia e impacto. Es importante además identificar y priorizar los servicios críticos de la institución en relación a la Matriz de BCG de los servicios de UTIC identificados en la presente investigación.
b) Se debe identificar el impacto que puede ocurrir en la ESPE; a causa de la indisponibilidad de los servicios de TI. Sin embargo, la UTIC debe considerar una solución inmediata para para aquellos incidentes no menos significativos.
c) En lo posible, la ESPE debe considerar la contratación de seguros privados que podrían formar parte del proceso de BCP[17].
d) Se debe desarrollar de una estrategia de continuidad del negocio alineados con el plan estratégico de la ESPE.
e) Se debe realizar pruebas y mantener una actualización periódica de los planes y procesos implementados.
f) La responsabilidad por la concordancia de la Gestión de la Continuidad del Negocio debe ser asignada a un nivel jerárquico adecuado dentro de la Estructura Orgánica de la UTIC.

[17] BCP: Plan de Continuidad del Negocio

4.15.1.3. Continuidad del negocio y evaluación del riesgo

La continuidad del negocio se refiere a la identificación de eventos que puedan ocasionar interrupciones en los procesos de los negocios. Adicionalmente, se debe llevar a cabo una evaluación que determinen el impacto de dichas interrupciones; tanto en términos de magnitud como de daño como del período de recuperación. Es importante que estas definiciones se las realice en conjunto con la participación activa de los propietarios de los procesos y de los servicios de TI.

La evaluación del riesgo debe considerar todos los procesos internos de la ESPE y no se debe limitar a las instalaciones a las instalaciones de procesamiento de la información. Según los resultados de la evaluación, se debe desarrollar un plan estratégico que determine el enfoque global con el que se establecerá la continuidad del negocio. Este plan debe ser aprobado por la Unidad de Desarrollo Institucional.

4.15.1.4. Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información

Este plan debe ser desarrollado con el fin de mantener o restablecer las operaciones de los negocios en los plazos requeridos una vez ocurrida una interrupción o fallas en los procesos críticos de la UTIC. Se debe definir lo siguiente:

a) Se debe identificar y mantener un acuerdo respecto a todas las responsabilidades y procedimientos que se deben tener en presencia de una emergencia.
b) Se debe implementar procedimientos de emergencia que garanticen la recuperación de los servicios de TI, en el menor tiempo posible.

c) Es importante que se realice un plan de capacitación a los miembros de la UTIC.
d) Se debe mantener un plan de pruebas y actualización de los planes.
e) El proceso de planificación debe alinearse al sistema de valor de la ESPE, para lo cual debe considerarse los servicios y recursos que permitirán que esto ocurra como: disponibilidad de personal, recursos que no procesen información, acuerdos de reanudación de emergencia en sitios alternativos que garanticen el procesamiento de información.

4.15.1.5. Marco de referencia para la planificación de la continuidad del negocio

La UTIC, debe mantener un único marco de referencia para el BCP de la ESPE, esto con el fin de garantizar que los mismos sean uniformes e identificar prioridades de prueba y mantenimiento. Es relevante mencionar que el BCP debe especificar claramente las condiciones para su puesta en marcha, así como la identificación de las responsabilidades de su ejecución.

En caso de, identificar nuevos requerimientos, estos requerimientos deben modificarse de conformidad al plan de emergencia establecidos. El marco de referencia para la planificación de la continuidad del negocio debe considerar los siguientes puntos:

a) La condiciones de implementación del BCP deberá describir claramente: los procedimientos para evaluar un incidente, técnicos involucrados, acciones a tomar, tiempo de indisponibilidad, tiempo de recuperación, entre otras. Esto antes de su puesta en marcha.
b) Los procedimientos de emergencia, debe describir las acciones a tomar en caso de presentarse un incidente que ponga en riesgo las actividades normales de la ESPE y/o la integridad física de los seres humanos.

c) Se debe establecer los procedimientos que permitan la recuperación de las actividades operacionales de la ESPE.
d) Se deberá definir un cronograma en el que se planifique la aprobación del plan y su mantenimiento.
e) Se debe establecer el cronograma para la concientización e instrucción al personal de la UTIC, este debe propiciar la comprensión de los procesos de continuidad del negocio y que garanticen eficacia de los mismos.
f) Se deberá dar a conocer las responsabilidades de las personas que pondrán en ejecución el BCP.

4.15.1.6. Pruebas, mantenimiento y revaluación de planes de continuidad

El BCP, puede ser propenso a fallas en el curso de pruebas, por lo general esto se debe a la ejecución de acciones incorrectas, negligencias o cambios en el equipamiento y/o personal. En tal virtud, se requiere que se realicen pruebas periódicas que permitan garantizar que estos planes se encuentren actualizados y su ejecución se eficaz. Adicionalmente, las pruebas deben certificar que el personal de recuperación y el de apoyo conozcan claramente el plan.

El cronograma de pruebas deberá ser aprobado por el director de la UTIC y deberá especificar cómo y cuando se realizará su evaluación. Se recomienda que para cada prueba, se utilicen diferentes técnicas que garanticen que los planes funciones en la vida real, lo cual debe incluir:

a) Se deberá establecer pruebas de discusión, en la que se traten medidas para la recuperación del negocio, se requiere que tomen ejemplos de interrupciones reales.

b) Se deberá establecer simulaciones, principalmente para capacitar al personal en el cumplimiento de sus roles de gestión posterior a incidentes o crisis.
c) Se debe establecer pruebas de recuperación técnica, las cuales deben garantizar que los servicios, aplicaciones y sistemas de información se restablezcan con eficacia.
d) Se debe realizar pruebas de recuperación en un sitio alternativo.
e) Se debe realizar pruebas de instalaciones y servicios de proveedores, los mismos que garanticen que los sus servicios cumplan con el compromiso contraído.
f) Se debe realizar prueba con la Comunidad Politécnica, en medida de lo posible, el equipamiento las instalaciones y los procesos puedan afrontar las interrupciones.

Adicionalmente, el BCP de la ESPE debe mantener revisiones y actualizaciones periódicas que permitan garantizar su eficacia permanente. Se debe definir las responsabilidades por las revisiones periódicas del BCP. Entre las situaciones que podrían demandar la actualización del BCP se encuentran la adquisición de nuevo equipamiento o la actualización de los sistemas operacionales y los cambios de:

a) Personal
b) Direcciones o números de contactos del personal
c) Plan estratégico de la ESPE
d) Ubicación de los recursos de TI
e) Base legal
f) Proveedores
g) Procesos nuevos o eliminados en la ESPE
h) Riegos

“No hay garantía de que la alta tecnología y la riqueza nos vayan a traer la felicidad. Pero traen dos importantes cosas: seguridad creciente y mayor capacidad de elección”. ***Herman KAHN***

5. CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

Dado la presente investigación, se ha determinado las siguientes conclusiones:

a) La ESPE, carece de políticas y procedimientos de seguridad de la información que se encuentren estandarizados en una norma internacional. Los manuales y normativas vigentes en la UTIC, han sido desarrolladas en función a las experiencias de los ingenieros, adicionalmente, estos documentos no se encuentran aprobados por la Unidad de Desarrollo Institucional, como unidad de control.
b) Se evidenciado que la ESPE ha sido objetivo de ataques informáticos, según la organización zone-h durante el 9 y 15 de Abril del presente año, las páginas atacadas son: www3.espe.edu.ec y eduvirtual.espe.edu.ec respectivamente. Zone-h es una organización en la que se puede visualizar las “hackeadas” que han tenido los sitios web de las organizaciones.
c) Cumpliendo con el alcance planteado en este proyecto de investigación, se analizaron las políticas para los siguientes dominios:
    a. Dominio (1): Política de Seguridad
    b. Dominio (6): Gestión de Comunicaciones y Operaciones
    c. Dominio (8): Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.
    d. Dominio (10): Gestión de la Continuidad del Negocio

    Es importante para la UTIC, analizar la posibilidad de continuar y concluir con el desarrollo de los dominios de la ISO/IEC 27002 que no han sido objeto de la presente investigación. El cumplimiento de este literal tendrá como fin de fortalecimiento de los procesos internos de la

UTIC, mejorando la calidad del servicio entregado a la Comunidad Politécnicas. Los dominios faltantes se detallan a continuación:

a. Dominio (2): Aspectos Organizativos de la Seguridad de la Información.
b. Dominio (3): Gestión de Activos
c. Dominio (4): Seguridad Ligada a los Recursos Humanos
d. Dominio (5): Seguridad Física y del Entorno
e. Dominio (7): Control de Acceso
f. Dominio (9): Gestión de Incidentes en la Seguridad de la Información
g. Dominio (11): Cumplimiento.

d) La investigación analítica, realizado a través del cuestionario, únicamente el 15% de profesionales de la UTIC hace referencia a la existencia de un Manual de Políticas y Plan de Seguridad de la Informática, sin embargo no conocen de la ubicación física y tampoco la frecuencia de su actualización. Es importante aclarar que se tomo una muestra de 13 personas que trabajan en la Unidad de Tecnologías de la Información y Comunicaciones.

   Anexo 8: Matriz de Resultados de Cuestionario

e) En función al dominio (6): Gestión de Comunicaciones y Operaciones, el 92% de los ingenieros que respondieron el cuestionario, manifestaron que se realizan copias de seguridad de toda la información crítica regularmente, este control es el que más porcentaje de cumplimiento tiene la UTIC.

f) El dominio (7): Adquisición, desarrollo y mantenimiento de Sistemas de Información, se videncia que un 62% de los profesionales conocen que para evitar pérdidas, modificaciones o mal uso de los datos de usuario en las aplicaciones de la Institución; se verifican los datos de referencia, tablas de parámetros, entradas duplicadas, valores fuera de rango,

caracteres inválidos, definición de responsabilidades de los implicados en el proceso de ingreso de datos.

g) La investigación presenta a la UTIC, un marco de trabajo enfocado a la seguridad de la información en la ESPE, con la finalidad de implementar una norma internacional de manera confiable, segura y oportuna.
h) La ISO/IEC 27002 establece controles de operación a todos los sistemas de información y comunicación de la ESPE, así como a sus operaciones y proceso, tratando de prevenir o minimizar riesgos de problemas informáticos, atacando las vulnerabilidades existentes.
i) La ESPE, requiere la creación o formación de un Sistema de Gestión de la Seguridad de la Información el cual establezca políticas y procedimientos en relación a los objetivos de negocio de la institución, a fin mantener un nivel mínimo de riesgo que se pueda asumir.
j) Es importante para la institución; establecer una cultura que proteja la seguridad de la información, principal activo de la ESPE, en virtud de que no existen jornadas de orientación y capacitación para los usuarios internos y terceros.
k) El siguiente diagrama de flujo, muestra el trabajo realizado y el que debe realizarse en un futuro, a consideración de la dirección de la UTIC, adicionalmente las fases de implementación de la ISO/IEC 27002.

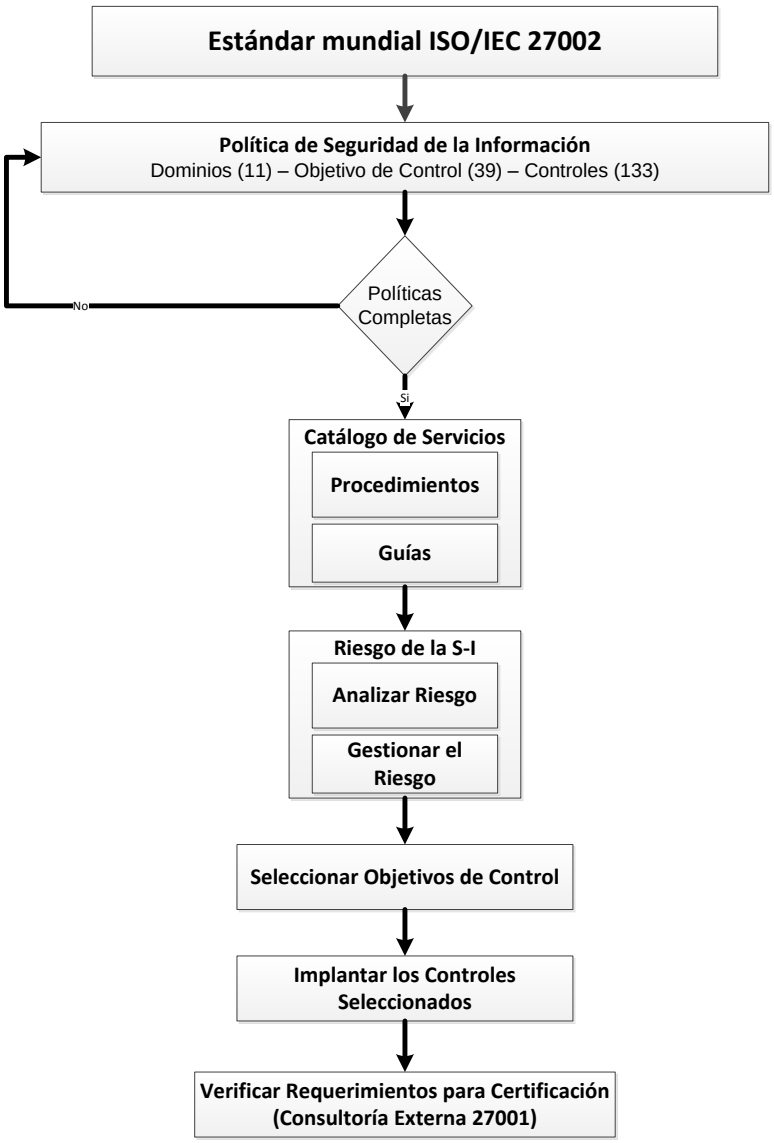


Figura 15: Flujo de Implementación ISO/IEC 27002

l) Como se muestra en la figura 15 de la presente investigación, una vez terminadas las políticas de los 11 dominios de la ISO/IEC 27002, se procede con la elaboración de las guías y procedimientos de los servicios de TI que ofrece la UTIC, para posteriormente realizar el análisis y la gestión de riesgos que puedan afectar con su normal funcionamiento. Finalmente, se debe considerar una asesoría externa

que permita la elaboración de requerimientos para la certificación en la norma ISO 27001, la misma que es certificable.

5.2. Recomendaciones

Una vez concluida la investigación del proyecto de tesis, se recomienda lo siguiente:

a) Se analice la posibilidad o factibilidad de crear un proceso que controle y regule las actividades de la Seguridad de la Información en la ESPE (SGSI).
b) Se realice un análisis integral de los riesgos físicos (eléctricos, fuego, inundaciones, entre otros) a fin de elaborar un plan de mejoras en la seguridad física del edificio donde se encuentra ubicado el Data Center institucional.
c) Se proponga a la UTIC, se considere la culminación de las políticas y procedimientos que recomienda la ISO/IEC 27002, con la finalidad de alcanzar una certificación.
d) Se conforme el SGSI, el cual debe ser dependiente de una Unidad de Control y Evaluación, como lo es la UDI (Ver: Figura 14: Estructura Organizacional SI Propuesto).
e) Se priorice la Seguridad de la Información a los servicios que se encuentren ubicados en el primer cuadrante de la Matriz BCG (Ver: Tabla 16: Matriz BCG de la UTIC).
f) Se realice jornadas de trabajo, en las que se muestre la importancia de mantener una cultura de protección de la información de la ESPE.
g) Se informe a la Comunidad Politécnica, la importancia del correcto uso de claves de acceso o contraseñas que el usuario debe utilizar para autenticarse en un sistema de información o servicio de red disponible en la institución.

h) Se mantenga una cultura de escritorios y pantallas limpias, así como de archivos compartidos y traslado de información crítica, pero principalmente sobre la ingeniería social, evitando responder preguntas sobre características de los sistemas, utilizar los recursos tecnológicos para fines académicos, administrativos, de investigación, entre otros.
i) Se mantenga actualizado de forma constante, transparente y de acuerdo a las necesidades, el manual de políticas y procedimientos establecidos en la presente investigación.
j) Se realicen jornadas de concientización, a los usuarios de la Comunidad Politécnica y terceros, sobre temas de seguridad de la información con la finalidad de hacerles sentir responsables y parte de la institución.

6. ACRÓNIMOS

- ✓ **ISO:** Organización Internacional de Normalización
- ✓ **IEC:** Comisión Internacional de Electrotecnia
- ✓ **CSIRT:** Computer Security Incident Response Team
- ✓ **DoS:** Denegación de Servicio
- ✓ **QoS:** Calidad de Servicio
- ✓ **TI:** Tecnología de la Información
- ✓ **UTIC:** Unidad de Tecnología de la Información
- ✓ **UDI:** Unidad de Desarrollo Institucional
- ✓ **SGSI:** Sistema de Gestión de la Seguridad de la Información
- ✓ **S-I:** Seguridad de la Información
- ✓ **Ingeniería Social:** Aprovechamiento de los conocimientos de las personas para convencerlas que ejecuten acciones o actos que puedan revelar información sensible.
- ✓ **Integridad:** Es el principio que busca mantener los datos libres de modificaciones no autorizadas.
- ✓ **Confidencialidad:** Es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados.
- ✓ **Disponibilidad:** La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones
- ✓ **Política:** Declaraciones de alto nivel sobre el propósito y la dirección de la gerencia.
- ✓ **Vulnerabilidad:** Es la falta y/o debilidad o falla de seguridad; es decir, indica que el activo es susceptible a recibir un daño a través de un ataque.
- ✓ **Amenaza:** Es cualquier cosa o evento que puede suceder y que, cuando ocurre, tiene consecuencias negativas sobre el valor los activos de una

organización. El daño es una forma de destrucción, revelación o modificación de datos.

- ✓ **Riesgo:** Es la probabilidad o posibilidad de que un evento desfavorable ocurra. El riesgo tiene un impacto negativo si este se materializara.
- ✓ **Impacto:** Es la “materialización” de un riesgo.
- ✓ **Control:** Es una medida o mecanismo para mitigar un riesgo. Este mecanismo permite establecer, detectar y reaccionar ante un evento de seguridad.

7. REFERENCIAS BIBLIOGRÁFICAS

Antonio Baquero, Luis Joyanes. (s.f.). *Libro Informática, Glosario de Términos y Siglas.* Mc. Graw Hill.

Ardita, L. J. (s.f.). EL ÁREA DE SEGURIDAD INFORMÁTICA.

CERT. (17 de 09 de 2008). *Software Engineering Institute.* Recuperado el 16 de 03 de 2012, de OCTAVE: http://www.cert.org/octave/

Comisión de Elaboración ESPE. (2008). *Reglamento Orgánico de la ESPE.* Sangolqui: ESPE.

CYBSEC S.A., S. S. (2011). Fundamento de Seguridad Informática. Buenos Aires, Argentina.

Development, M. S. (2009). *Estudio de Percepción: Seguridad en Informática .* México: JFS.

ESPE. (s.f.). Recuperado el 06 de 03 de 2012, de Sitio Web de la Escuela Politécnica del Ejército: www.espe.edu.ec

Gonzalo Álvarez Marañon, Pedro Pablo Pérez García. (2004). *Seguridad Informática para Empresas y Particulares.* Madrid: McGraw-Hill.

Guangalango Vega, Ricardo Napoleón; Moscoso Montalvo, Patricio Esteban. (2001). *Evaluación Técnica de la Seguridad Informática del Data Center de la Escuela Politécnica del Ejército.* Sangolqui: ESPE.

ISO ORG. (s.f.). Recuperado el 12 de 03 de 2012, de ISO 27000: www.ISO27000.es

IT Governance Institute. (2007). *COBIT 4.1.* IL 60008 USA: IT Governance Institute.

MAGERITv2. (09 de 03 de 2010). *Portal Administración electrónica*. Recuperado el 15 de 03 de 2012, de MAGERIT Versión 2: http://administracionelectronica.gob.es/

Palma, L. A. (2011). *Introducción Seguridad informática.* México: ITESM.

Pazmiño, N. P. Análisis de los Riesgos y Vulnerabilidaes de la Red de Datos de la Escuela Politécnica Nacional. *Tesis de Grado.* Escuela Politécnica Nacional, Quito.

PCWorld, E. (2012). Movistar obtiene la certficación ISO 27001. *PCWorld*.

SGC. (s.f.). Recuperado el 06 de 03 de 2012, de Mapa de Procesos de SGC de la ESPE: http://sgc.espe.edu.ec/Paginas/mapa.html

SRI. (2012). Departamento de Seguridad Corporativa Dirección Nacional de Planificación y Coordinación.

Telconet. (2012). *Sitio oficial*. Recuperado el 11 de 05 de 2012, de www.telconet.net

Vieites, Á. G. (2007). *Enciclopedia de la Seguridad Informática.* México D.F.: Alfaomega Grupo Editor, S.A. de C.V.

8. ANEXOS

ANEXO 1.
NUMÉRICO DE ESTUDIANTES POR CARRERA Y EXTENSIÓN

ANEXO 2.

MANUAL DE GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

ANEXO 3.

PLAN DE CONTINGENCIA DE TECNOLOGÍAS DE INFORMACIÓN

ANEXO 4.

MANUAL DE USO DEL SISTEMA DE VIDEO CONFERENCIA

ANEXO 5.

CUESTIONARIO Y RESPUESTAS DE POLÍTICAS DE S-I DE LA UTIC

ANEXO 6.

ACTA DE CONFIDENCIALIDAD

ANEXO 7.

COPIA DE LA INFORMACIÓN

ANEXO 8:

MATRIZ DE RESULTADOS DE CUESTIONARIO