ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"ESQUEMA DE SEGURIDAD INFORMÁTICA AL PROCESO DE ACTUALIZACIÓN Y DESARROLLO DE SOLUCIONES INFORMÁTICAS DEL DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN DE LA UNIVERSIDAD CATÓLICA DE CUENCA"

TRABAJO DE TITULACIÓN

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

CARLOS ANDRÉS TORRES SOTO

GUAYAQUIL - ECUADOR

AÑO: 2019

AGRADECIMIENTO

En primer lugar, a Dios por estar conmigo en cada etapa de mi vida, caminando a mi lado y llenándome de bendiciones.

A mi madre que con seguridad está observándome desde el cielo y sintiéndose orgullosa de su hijo, viéndome conseguir una nueva meta en mi vida.

A mi amada esposa por su amor, solidaridad e incondicional apoyo en todo proyecto que he emprendido en mi vida personal y profesional.

A mi hija Renata Mikaela, el motor de mi vida y mi vida misma.

A mis hijos Andreita y Josué, por brindarme el calor de una familia, y el orgullo de ser padre.

A mi tutor, por sus apreciados consejos y su apoyo incondicional para la culminación este proyecto académico.

DEDICATORIA

A Dios, a mi madre que en paz descanse, a mi amada esposa, a mis hijas e hijo, a mi familia, a mi tutor Ing. Lenín Freire, a mis profesores, compañeros de estudios y a todos quienes de alguna u otra forma han aportado un granito de arena para llegar a buen término.

TRIBUNAL DE GRADUACIÓN

MSIG. LENÍN FREIRE C.

DIRECTOR MSIA

MSIG. LENÍN FREIRE C.

DIRECTOR DEL PROYECTO DE GRADUACIÓN

MSIG. RONNY SANTANA E.

MIEMBRO DEL TRIBUNAL

DECLARACIÓN EXPRESA

"La responsabilidad por los hechos, ideas y doctrinas expuestas en este Trabajo de Titulación le corresponden exclusivamente, y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL"

Carlos Andrés Torres Soto

RESUMEN

El objetivo del trabajo de titulación es diseñar e implementar un esquema de seguridad informática al proceso de actualización y desarrollo de soluciones informáticas del Departamento de Tecnologías de la Información y Comunicación de la Universidad Católica de Cuenca; con el propósito de mitigar los riesgos relacionados con este proceso.

En el primer capítulo se detalla la problemática, y se manifiesta una solución por medio de la utilización y aplicación de normas internacionales, además se especifican el objetivo general y los objetivos específicos del trabajo de titulación.

El segundo capítulo se describe el marco teórico, así como conceptos relacionados acerca de la seguridad informática, en general, la normativa internacional ISO 27002, además incluye una exploración acerca de las metodologías para el análisis y gestión del riesgo informático.

El tercer capítulo contiene la información acerca de la Institución en donde se implementó el trabajo de titulación, el cual incluye el análisis del estado anterior

a la aplicación del esquema de seguridad al proceso de actualización y desarrollo de soluciones informáticas del Departamento de Tecnologías de la Información y Comunicación de la Universidad Católica de Cuenca; para este propósito se realizaron entrevistas con las áreas relacionadas con el desarrollo y manejo del sistema en niveles críticos, es decir, con las áreas que manejan información sensible de la Universidad con el fin de conocer acerca de eventos relacionados con seguridad informática, así como los de protección en los servicios de mayor relevancia.

El cuarto capítulo hace un análisis exhaustivo de los activos de información, entre ellos los de mayor grado de criticidad, así como el análisis de amenazas, vulnerabilidades y riesgos en general a los que están expuestos los activos de información.

El quinto capítulo contiene el análisis y diseño del esquema de seguridad que se implementó; en lo referente al análisis se especifican los dominios y controles de la norma ISO 27002, la selección de los controles y los parámetros de aplicación de cada uno de ellos con el propósito de mitigar los riesgos a los activos de la Universidad, de esta forma se concluye con la elaboración de la propuesta de esquema de seguridad.

El sexto capítulo hace referencia al plan de implementación de la política de seguridad. Finalmente, se exponen las respectivas conclusiones y recomendaciones.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

DBA	Administrador de Base de Datos
IEC	Comisión Electrotécnica Internacional
IP	Protocolo de Internet
ISO	Organización Internacional de Normalización
PC	Computador Personal
PDCA	Plan-do-check-act, (planificar-hacer-verificar-actuar) - Deming - espiral de mejora continua
TIC	Tecnologías de la Información y Comunicación
SGSI	Sistema de Gestión de Seguridad de la Información
UCACUE	Universidad Católica de Cuenca
UNE-EN 50174-2	Tecnología de la información. Instalación del cableado. Parte 2: Métodos y planificación de la instalación en el interior de los edificios

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Desde la aparición de las computadoras en nuestro medio, que data de la época de los ochentas hasta inicios del 2000, no parecía ser un verdadero problema las amenazas como el malware, pues éste se transmitía en medios movibles como lo eran los discos y disquetes, pero por la época del 2005, con la llegada del internet el problema ya se volvió serio, pues las amenazas se globalizaron y su transferencia ya no era en discos extraíbles sino por medio de la red mundial y se agregó otra amenaza adicional, el delincuente cibernético.

Por este motivo, si bien es cierto que en ese entonces ya existía el concepto de seguridad de la información, este era prácticamente de uso exclusivo de entornos militares y gubernamentales, así como de muy pocas empresas que de alguna u otra forma estaban obligadas a asegurar sus información, tal es el caso de los bancos; este término y su incorporación en las empresas hoy en día se ha vuelto una obligación, pues actualmente se considera que la información es el activo más valioso en una empresa o institución, sea del tipo que sea.

Este activo intangible que poseen las empresas, al ser tan valioso, amerita su protección, y es en este punto en el que muchas empresas no saben cómo hacerlo o tienen ideas vagas y no estructuradas [11].

Debido a esto existen muchas organizaciones y comunidades que se han dedicado a estandarizar y recomendar controles y buenas prácticas respectivamente, para mantener niveles aceptables de riesgo informático en las organizaciones dependiendo del tipo de negocio de las mismas, entre ellas están cobit, itil y la que se trata en esta tesis la ISO con su normativa 27002. Es necesario aclarar que no es posible eliminar completamente los riesgos informáticos, pero si mitigarlos y llevarlos a niveles, como ya se mencionó anteriormente, aceptables de tolerancia.

La Norma ISO 27002 tiene como principal objetivo la salvaguarda de los 3 pilares de la seguridad de la información como son: la integridad, confidencialidad y disponibilidad, por medio de la proposición de métodos de control de los riesgos informáticos, los cuáles deben estar en constante

revisión y, de ser necesario, actualizándose de acuerdo a nuevos riesgos y amenazas que día a día se crean a nivel mundial, y contenidos en un esquema de seguridad de la información llamado “políticas de seguridad”

La implementación de políticas de seguridad de la información, así como sus controles y métodos para evaluación y análisis de riesgos estarán siempre en función del tipo de negocio de la Organización, y utilizará controles específicos para las respectivas áreas de la empresa en donde se vea involucrado el manejo de la información y con mayor énfasis en donde esa información sea crítica para la organización.

Conjuntamente con la implementación de estas políticas de seguridad debe venir la socialización de las mismas a todos los empleados de la organización, pues la seguridad de la información es responsabilidad de todos no solo del personal encargado de salvaguardarla, y además es imperativo mantener a todo el personal capacitado en cuanto a cómo evitar encontrarse frente a una amenaza o un riesgo informático y, dado el caso, cómo actuar cuando suceda.

Las instituciones educativas a nivel superior han sido uno de los blancos preferidos de atacantes informáticos, en su gran mayoría empleados o estudiantes propios de la institución educativa como se puede comprobar, por citar unos pocos: “Diario Semanario Universidad” de la Universidad de Costa Rica [2], registro de títulos falsos en la Senescyt en Ecuador [8], la universidad de Los Andes en Colombia [10], la Universidad de Málaga en España [1], todos ejemplos de instituciones que han sido blancos de ataques a sus sistemas informáticos o robo y manipulación de la información.

CAPÍTULO 1

GENERALIDADES

1.1 ANTECEDENTES

La seguridad informática se preocupa de la protección de los activos de información, para este propósito se han creado estándares, métodos, protocolos, herramientas, reglas y leyes diseñadas para minimizar los riesgos de pérdida de estos. Entendiendo por activos de la información la infraestructura física tecnológica, el software y obviamente, la información.

Con el paso de los años, desde que se generalizó la automatización de los procesos, las empresas e instituciones se han enfocado en perfeccionar

los sistemas informáticos y en las arquitecturas cliente – servidor, con este tipo de arquitectura, de la mano, creció el uso de las redes hasta llegar a un punto de su globalización como es el caso de internet.

Desafortunadamente, si bien es cierto que el acceso a la información se facilitó notablemente, no obstante, también se hizo más vulnerable a ataques informáticos con las consecuencias catastróficas que puede generar el hecho del “fácil acceso a la información”.

De esto nace la necesidad de que los sistemas de información y la información en sí, sea protegida a través de algún tipo de normativa o controles basados en buenas prácticas de uso de la información, esto en general, se refiere al conjunto de normas, procedimientos y mecanismos basados en algún estándar alineados para garantizar los tres pilares de la seguridad informática integridad, confidencialidad y disponibilidad de la información.

Bajo estas consideraciones, es transcendental definir los procesos más críticos de una empresa o institución y realizar un análisis de seguridad de los sistemas con el propósito de detectar vulnerabilidades, amenazas que pudieran afectar a alguno de los pilares de la seguridad de la información.

1.2 DESCRIPCIÓN DEL PROBLEMA

Actualmente el departamento de Tecnologías de la Información y Comunicación de la Universidad Católica de Cuenca carece de una política de seguridad informática que establezca procedimientos y controles de aseguramiento respecto de la información y uso de sus activos informáticos.

La constitución de este departamento de tecnologías de la información y comunicación dentro del orgánico funcional de la Universidad ha permitido el incremento significativo de activos físicos como son los equipos de cómputo, servidores equipos de networking, storage entre otros y lógicos como los sistemas entre los cuales destacan el erpuniversity que es un sistema integrado de los principales módulos de gestión de la Universidad, sistema de aulas virtuales, seguimiento a graduados entre otros y, sumando a todo esto está el mejoramiento de la infraestructura de red cableada e inalámbrica, el crecimiento de la cobertura inalámbrica, la ampliación de los anchos de banda de acceso a internet, la creación de nuevos servicios informáticos, suponen también la necesidad de una mayor calidad en la forma de protección de la información.

Esto hace que sea indispensable la elaboración y ejecución de controles de aseguramiento de los activos informáticos para, en niveles aceptables, garantizar la integridad, confidencialidad y disponibilidad de dichos activos.

El no mantener una política de seguridad de la información, aumenta el riesgo de que ocurran eventos perjudiciales contra los activos relacionados con la información; incidentes de seguridad, que tengan afectación directa contra la disponibilidad, integridad y confidencialidad de los sistemas y servicios con los que cuenta la Universidad, lo que implica, directamente, pérdidas económicas, interrupción de los procesos administrativos, académicos, laborales, etc.; pero lo que es peor, podría causar pérdida parcial o total de información relevante de la Universidad, todo ello por falta de control de los activos tecnológicos.

Cabe mencionar que la Universidad Católica de Cuenca ha sufrido la afectación en varios de sus servicios, así como a sus sistemas a través del tiempo, como, por ejemplo: infecciones de malware por mal uso de los dispositivos extraíbles y accesos a sitios fraudulentos, problemas de pérdida de información por descargas de ficheros infectados y no analizados, daños de computadoras por mal manejo de las mismas, ingresos no autorizados, entre otros.

El mal manejo de la seguridad de la información ha perjudicado a empresas muy pequeñas, hasta a empresas muy grandes y que de alguna forma se creían muy seguras contra ataques informáticos, en este tema, las universidades no han sido la excepción; por citar un ejemplo, en uno

de los departamentos de la Universidad, en el mes de agosto del año 2015, la computadora de un funcionario que manejaba información de alta responsabilidad, fue infectada con ransomware (cryptolocker) causando la pérdida de parte de la información del departamento y como consecuencia el retraso en los procesos administrativos de dicho departamento; este suceso se produjo por no existir una política de seguridad de protección de la información mediante controles establecidos por algún estándar internacional de seguridad de la información.

Es indispensable contar con estos controles de aseguramiento de la información y sobre todo que la Seguridad Informática se parte de sus líneas de investigación, pues las estadísticas son alarmantes en las universidades del Ecuador que ni siquiera se preocupan por el aseguramiento de la información.

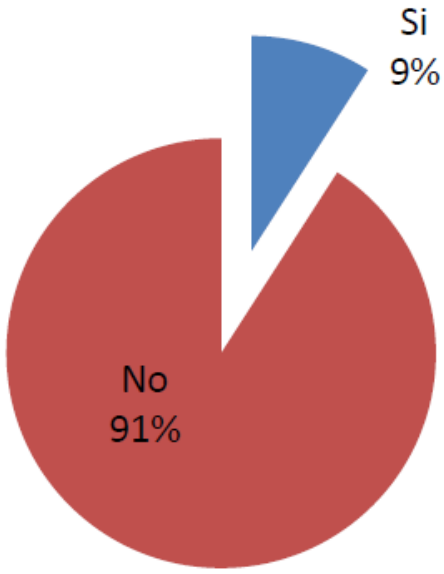

FIGURA 1. 1 Universidades que incluyen en su línea de investigación el Aseguramiento de la Información.

Autor: CEDIA (Año 2014)

Por lo tanto, se espera que un gran porcentaje de universidades en nuestro país no aplique controles esenciales como los de acceso a los sistemas.

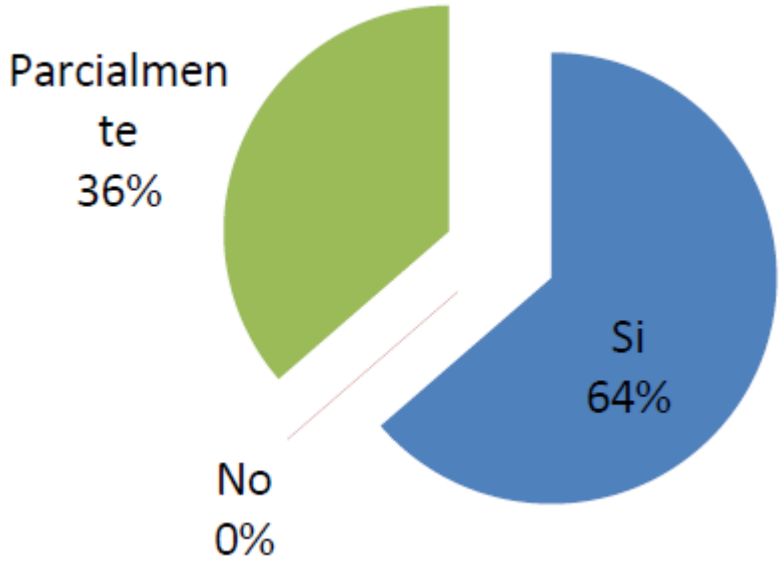

FIGURA 1.2 Controles esenciales de Seguridad de la Información aplicados.

Autor: CEDIA (Año 2014)

Actualmente, el proceso de actualización y desarrollo de soluciones informáticas del Departamento de Tecnologías de la Información y Comunicación de la Universidad Católica de Cuenca no cuenta con un esquema de seguridad informática que incluya una política, controles sobre la organización y aplicación de la seguridad, controles de utilización del software, controles sobre la continuidad del negocio, controles sobre los activos y controles de accesos.

La Organización con el paso de los años ha tenido un crecimiento acelerado tanto en personal como en activos informáticos con lo cual, ha existido también un incremento en los niveles de riesgos.

El no mantener un esquema de seguridad de la información, aumenta el riesgo de que ocurran pérdidas de información o en el mejor de los casos, paralizaciones de los servicios en la universidad, ante esta situación se debe trabajar en los diferentes áreas del departamento de tecnología, como son el área de desarrollo, infraestructura, servicios y comunicaciones así como con los usuarios finales, con el objetivo de proveer políticas o normas que ayuden a mitigar el riesgo, para llevarlo hasta los niveles de aceptación.

Dentro de los incidentes que se han presentado en los dos últimos años tenemos los siguientes:

- Errores por subida de información de prueba en ambiente de producción.
- Borrado de información por no tener escalamiento de permisos.
- Pérdida de información por falta de procedimiento de respaldo.
- Ejecución de scripts en ambientes de producción con errores.
- Accesos al sistema con usuarios que ya no se encuentran en el departamento.
- Acceso utilizando usuarios por defecto.
- Uso de claves de acceso con bajo nivel de dificultad o complejidad.
- Falta de procedimiento para el uso de dispositivos removibles.

- Máquinas infectadas de virus.
- Fuga de información.
- Detención de los servicios críticos.
- Entre otros.

1.3 SOLUCIÓN PROPUESTA

Con base a lo expuesto en la situación actual, la propuesta es crear un esquema de seguridad informática al proceso de actualización y desarrollo de soluciones informáticas del Departamento de Tecnologías de la Información y Comunicación extraída del estándar ISO 27002 cuyo contenido se enfoque a la elaboración de procedimientos que garanticen, en un nivel aceptable, la seguridad de los activos informáticos relacionados con este proceso.

La aplicación de estos controles, se enfocarán netamente en la seguridad de la información, aplicando a los siguientes dominios: organizativos, manejo de medios, continuidad del negocio, controles sobre los activos, control de accesos, y tratamiento del riesgo.

Esta norma internacional suministra información relacionada con buenas prácticas de gestión de la seguridad de la información, cuyo foco principal es la integridad, confidencialidad, y disponibilidad de la información.

Puesto que el estándar ISO/27002 especifica controles adaptables a varios ambientes informáticos permitiendo que se acople a cualquier esquema relacionado con el aseguramiento de la información, es por este motivo que se ha elegido como norma base para el diseño del esquema de seguridad propuesto, para cumplir con las necesidades y requerimientos del proceso de actualización y desarrollo de soluciones informáticas del Departamento de Tecnologías de la Información y Comunicación.

Además, podría servir como una guía a implementarse en otros procesos o áreas de la Universidad con el fin de dotar de políticas de seguridad, así como de las mejores prácticas de la gestión de la seguridad de la información. El estándar es lo suficientemente bueno para dar inicio a una cultura de seguridad en la Universidad Católica de Cuenca.

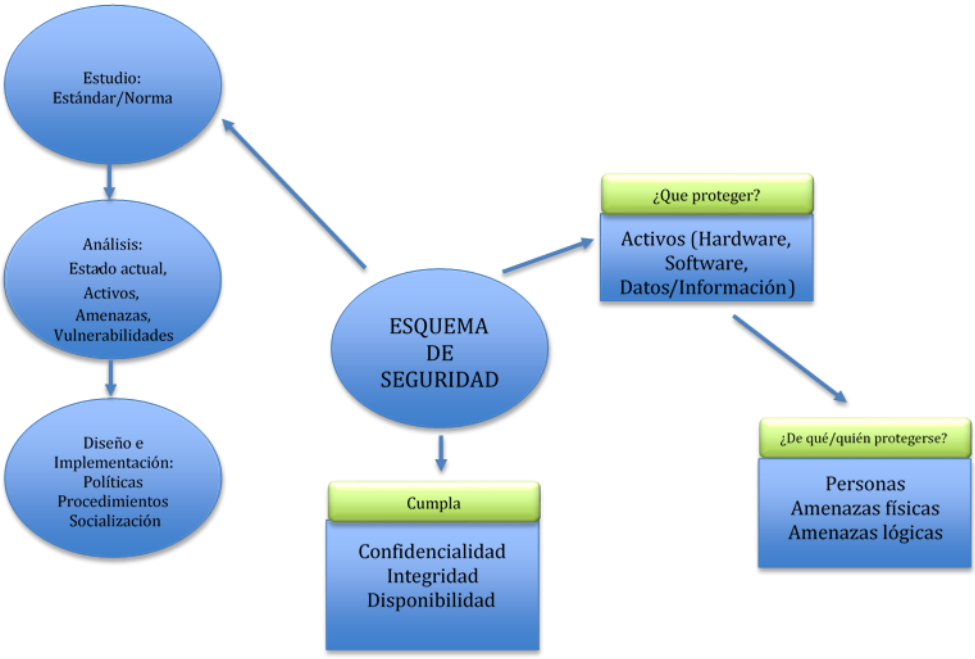

FIGURA 1.3 Esquema de Seguridad de la Información.

1.4 OBJETIVO GENERAL

Implementar un esquema de seguridad informática al proceso de actualización y desarrollo de soluciones informáticas del Departamento de Tecnologías de la Información y Comunicación de la Universidad Católica de Cuenca basado en el estándar ISO/IEC 27002:2013; con el propósito de mitigar los riesgos relacionados con el uso de los activos informáticos en el proceso en mención.

1.5 OBJETIVOS ESPECÍFICOS

- Identificar los activos de información relacionados con el proceso de actualización y desarrollo de soluciones informáticas y gestión de bases de datos del Departamento de Tecnologías de la Información y Comunicación.

- Identificar las amenazas potenciales, vulnerabilidades y riesgos de seguridad de la información relacionados a los activos de información que estén vinculados con el proceso de actualización y desarrollo de soluciones informáticas y gestión de bases de datos del Departamento de Tecnologías de la Información y Comunicación.

- Diseñar un esquema de seguridad, mediante la definición de los controles adecuados con base en la norma ISO 27002 con el propósito de llevar a niveles aceptables de aseguramiento de los activos físicos y lógicos asociados al proceso de actualización y desarrollo de soluciones informáticas y gestión de bases de datos del Departamento de Tecnologías de la Información y Comunicación.

- Proponer un Plan de Implementación de los controles de aseguramiento de los activos informáticos relacionados con el proceso de actualización y desarrollo de soluciones informáticas y gestión de

bases de datos del Departamento de Tecnologías de la Información y Comunicación de la Universidad Católica de Cuenca.

1.6 ALCANCE

Este proyecto de tesis cubre la implementación de un esquema de seguridad informática al proceso de actualización y desarrollo de soluciones informáticas del Departamento de Tecnologías de la Información y Comunicación de la Universidad Católica de Cuenca basado en la Norma ISO 27002; el diagnóstico, evaluación de riesgos y selección de controles comprende los siguientes componentes de la norma:

- Política de Seguridad.
- Aspectos de la Organización de la seguridad de la información.
- Gestión de los incidentes de seguridad.
- Gestión de activos físicos y lógicos.
- Gestión sobre la continuidad del negocio.
- Controles de acceso.

Con los resultados de la aplicación de este proyecto, se pretende que el proceso de actualización y desarrollo de soluciones informáticas y gestión

de bases de datos, como parte el Departamento de Tecnologías de la Información y Comunicación, disponga de un sistema de seguridad informática confiable y basado en las mejores prácticas que recomienda la norma ISO 27002, el cual, pueda ser actualizado a medida de las necesidades y posibles cambios que se pudieran presentar en el proceso.

CAPÍTULO 2

FUNDAMENTACIÓN TEÓRICA

2.1 SEGURIDAD INFORMÁTICA

La seguridad informática, es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable [7], por otro lado [3] considera a la seguridad informática como “una disciplina del conocimiento donde se busca cerrar la brecha de los eventos inesperados que puedan comprometer los activos de una organización y así contar con estrategias para avanzar ante cualquier eventualidad”, entonces se puede deducir que

implica todos los activos de computación en los cuales se incluye la información como el principal.

Es necesario diferenciar del concepto de seguridad informática, que se mencionó en el texto que antecede, del concepto de seguridad de la información, que según [5], desde un enfoque comercial, manifiesta que consiste en asegurar la continuidad del negocio mediante la protección de un considerable número de amenazas, minimizando el riesgo, en este caso, comercial, y maximizando el retorno de la inversión y generando oportunidades comerciales”

Para este fin, se han diseñado una serie de estándares aceptados internacionalmente con propósito de minimizar los posibles riesgos de deterioro de alguno de los tres pilares fundamentales de la seguridad informática que están constituidos por la disponibilidad, la confidencialidad e integridad de la información. Entre los cuales destaca el estándar ISO 27002. La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial.

Los conceptos de seguridad de la información y seguridad informática difieren en que la primera hace referencia a cualquier medio lógico o físico

que entregue información y el segundo enmarca a la información contenida en algún medio informático.

FIGURA 2. 1 Objetivos de la Seguridad de la Información.

Autor: Universidad de Buenos Aires – Facultad de Agronomía

En la figura 2.1 engloba los principales objetivos de la seguridad de la información según la IS0 27002, La seguridad de la información está formada por tres pilares fundamentales: confidencialidad, disponibilidad e integridad, a continuación, una breve descripción de cada uno de ellos:

• Confidencialidad: Se encarga de asegurar que el acceso a la información está adecuadamente autorizado.

• Integridad: Verifica que información se mantenga completa, coherente, sin modificaciones que no hayan sido autorizadas por el responsable de la misma.

• Disponibilidad: Asegura que la información esté disponible y pueda ser accedida, cuando lo requiera el usuario autorizado para hacerlo.

En otra de las definiciones de lo seguridad informática se manifiesta que Seguridad Informática son las medidas y controles que aseguran la confidencialidad, integridad y disponibilidad de los activos de los sistemas de información, incluyendo hardware, software, firmware y aquella información que procesan, almacenan y comunican [9].

De estas definiciones se puede deducir que los principales objetivos de la seguridad informática son:

• Confidencialidad: consiste en la capacidad de garantizar que la información, almacenada en el sistema informático o transmitida por la red, solamente va a estar disponible para aquellas personas autorizadas a acceder a dicha información, es decir que, si los contenidos cayesen en manos ajenas, estas no podrían acceder a la información o a su interpretación. Este es uno de los principales problemas a los que se enfrentan muchas empresas; en los últimos años se ha incrementado el robo de los portátiles con la consecuente pérdida de información confidencial, de clientes, líneas de negocio …etc.

• Disponibilidad: Se define como la capacidad de garantizar que tanto el sistema como los datos van a estar disponibles al usuario en todo

momento. Pensemos, por ejemplo, en la importancia que tiene este objetivo para una Universidad que tiene una plataforma virtual de enseñanza, en la que pone a disposición de los estudiantes recursos como videos, bibliografía, enlaces de interés, exámenes, etc. Entonces será indispensable que siempre esté disponible para sus estudiantes.

• Integridad: Es la capacidad de garantizar que los datos no han sido modificados desde su creación sin autorización. La información es válida y consistente; este objetivo es muy importante cuando estamos realizando trámites en línea, por ejemplo, de una institución financiera, se deberá garantizar que ningún intruso pueda capturar y modificar los datos en tránsito.

2.2 ESTÁNDARES Y NORMAS APLICABLES

Actualmente existen varios estándares de seguridad informática, entre los cuales están:

ISO 15408 es un estándar mejor conocido como “Criterio Común” y que se alinea más a las aplicaciones de software permitiendo que puedan ser integradas y probadas de forma segura.

También está la **RFC 2196** que consiste en un memorándum expedido por el Internet Engineering Task Force que se centra en la creación de políticas y procedimientos de seguridad para aquellos sistemas de

información con acceso a Internet; este estándar es bastante generalizado pues además de la proporcionar normas de seguridad de la información también se incluye a las redes de datos para su aseguramiento.

Para el campo industrial, se inició en el año 2007, con el grupo de trabajo de la International Society for Automation (ISA),

El **ISA/IEC 62443** es un estándar que fue creado y se ha ido actualizando a través del tiempo, para aseguramiento de la información cuyo campo de acción es netamente el industrial, la numeración de su documentación está asociada con los estándares correspondientes de la IEC (International Electrotechnical Commission).

El grupo de estándares **ISO/IEC 27000**, estos determinan un sistema de administración de seguridad de la información bajo un estricto control administrativo de la misma.

Este último es el que se ha elegido para la aplicación de las políticas de seguridad para el presente trabajo de tesis.

2.2.1 ISO/IEC 27000

Con respecto los estándares relacionados con la seguridad de la información, tiene bastante peso la familia de los estándares ISO/IEC 27000, que son un conjunto de controles específicos para

gestionar la seguridad informática o de la información con la característica de que puede ser aplicado a cualquier organización, independientemente de su tipo, tamaño o actividad.

La ISO 27000 incluye varios estándares en su familia, a continuación, un pequeño resumen de cada uno de ellos.

ISO 27000: Engloba el vocabulario en el cual se basan el resto de normas. Se podría comparar con un diccionario que describe los términos o enunciados de todas las normas incluidas en esta familia.

ISO 27001: es el conjunto de requisitos para implementar un SGSI. Es la única norma certificable de las que se incluyen en la lista y consta de una parte principal basada en el ciclo de mejora continua y un Anexo A, en el que se detallan las líneas generales de los controles propuestos por el estándar. [14]

ISO 27002: se trata de una recopilación de buenas prácticas para la Seguridad de la Información que describe los controles y objetivos de control. Actualmente cuentan con 14 dominios, 35 objetivos de control y 114 controles [15].

ISO 27003: es una guía de ayuda en la implementación de un SGSI. Sirve como apoyo a la norma 27001, indicando las directivas generales necesarias para la correcta implementación de un SGSI.

Incluye instrucciones sobre cómo lograr la implementación de un SGSI con éxito.

ISO 27004: describe una serie de recomendaciones sobre cómo realizar mediciones para la gestión de la Seguridad de la Información. Especifica cómo configurar métricas, qué medir, con qué frecuencia, cómo medirlo y la forma de conseguir objetivos.

ISO 27005: es una guía de recomendaciones sobre cómo abordar la gestión de riesgos de seguridad de la información que puedan comprometer a las organizaciones. No especifica ninguna metodología de análisis y gestión de riesgos concreta, pero incluye ejemplos de posibles amenazas, vulnerabilidades e impactos.

ISO 27006: es un conjunto de requisitos de acreditación para las organizaciones certificadoras.

ISO 27007: es una guía para auditar SGSIs. Establece qué auditar y cuándo, cómo asignar los auditores adecuados, la planificación y ejecución de la auditoría, las actividades claves, etc.

2.3 METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGO

Primero, se define el riesgo de seguridad como una combinación de amenazas, vulnerabilidades e impactos. Las amenazas son eventos que

aprovechan las vulnerabilidades (debilidades) y pueden causar daños. El impacto es el resultado de una vulnerabilidad al ser explotada por una amenaza [12].

La gestión del riesgo constituye en un conjunto de técnicas con la utilización de herramientas de apoyo con el propósito de tomar las decisiones más adecuadas, de forma lógica, sin dejar de lado la incertidumbre, la posibilidad de que se puedan producir futuros sucesos y las consecuencias sobre los objetivos planteados; se preocupa de la prevención de eventos de seguridad con el fin de evitar la corrección y la mitigación de daños causados cuando el evento ya ha causado consecuencias [6].

En materia de gestión del riesgo, a continuación, se dan algunas definiciones [12]:

- La gestión del riesgo incluye todas las medidas adoptadas para controlar los riesgos en una organización, incluyendo el análisis/ evaluación, el tratamiento, la aceptación y la comunicación de los riesgos.

- El análisis de riesgos identifica y estima los riesgos, teniendo en cuenta el uso sistemático de la información. Abarca el análisis de las

amenazas, vulnerabilidades e impactos y se considera el punto clave de la política de seguridad de la información de una organización.

- La evaluación del riesgo compara el riesgo estimado en el análisis con los criterios predefinidos con el fin de identificar la importancia de cada riesgo para la organización.

- Aceptación de riesgos incluye la identificación del nivel aceptable de riesgos para una organización en función de sus necesidades específicas de negocio y seguridad.

- El tratamiento del riesgo corresponde a la selección y la aplicación de medidas para modificar un determinado riesgo.

Una gestión del riesgo eficaz se logra, identificando, las amenazas y el impacto que alcanzaría de materializarse, la probabilidad de que se produzcan las amenazas y los riesgos potenciales. Es recomendable que los riesgos sean clasificados de acuerdo a los siguientes parámetros: importancia, nivel de pérdidas y costos de la prevención y / o de la recuperación de desastres.

Con base en este enunciado habría que tomar en cuenta, que, si el costo para prevenir una amenaza resulta mayor que el daño potencial, se debería contemplar otras medidas de solución. En consecuencia, para tomar una decisión de estas, se deberían tener en cuenta cual es el nivel

de importancia del activo amenazado respecto de la continuidad del negocio de la empresa o institución.

De aquí la importancia del objetivo del análisis de las vulnerabilidades y amenazas el cual se resume en identificar la probabilidad de que ocurran los eventos contra la seguridad de los activos de información y el impacto en daños, además se debería tomar en cuenta el análisis de este impacto con el fin de identificar los recurso o activos críticos para la institución; es decir, los que más daños causara su afectación.

A sabiendas de que es una labor muy difícil la de definir con exactitud la probabilidad de que se materialice una amenaza y el nivel de daños de producirse, se recomienda establecer una lista de activos y las amenazas potenciales a estos activos, de los recursos o servicios afectados y del nivel de impacto que puede alcanzar (ejemplo, muy bajo, bajo, moderado, alto y muy alto).

El análisis de riesgos básicamente consiste en identificar, calificar y cuantificar los riesgos, alineado con los objetivos de la organización. Involucra además la priorización de los riesgos, para este paso se tomará en cuenta los conceptos de riesgo aceptable.

Algunos criterios de análisis y evaluación de los riesgos de la seguridad de la información que deberán tenerse en cuenta son [12]:

- Deben ser llevados a cabo de manera sistemática con el fin de identificar los riesgos (análisis) y calificar el riesgo (evaluación).

- Debe utilizar métodos específicos para permitir la comparación entre los resultados obtenidos y su reproducción.

- Debe realizarse periódicamente o cuando los requisitos de seguridad, activos, vulnerabilidades y / o los objetivos de negocio sufren algún cambio.

Fórmula para el cálculo del riesgo:

En el cálculo de los riesgos, existe la relación entre el nivel de impacto y la probabilidad de ocurrencia a través de la siguiente fórmula:

Riesgo = Impacto x Probabilidad

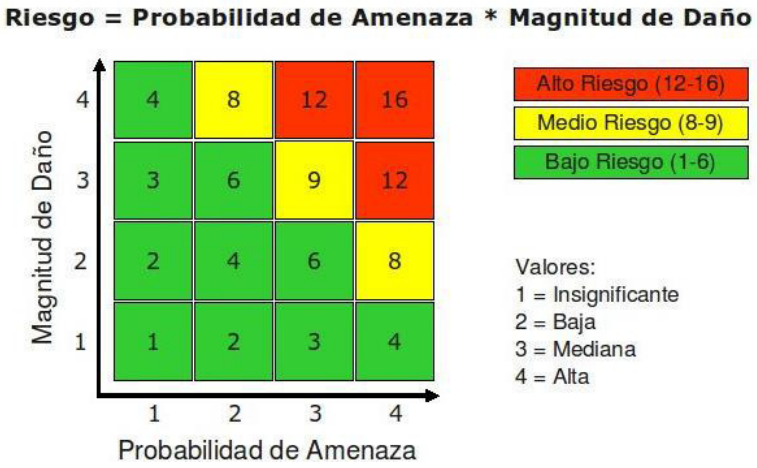

FIGURA 2. 2 Matriz de Riesgo.

2.4 ESTADÍSTICAS ACTUALES SOBRE SEGURIDAD INFORMÁTICA

En una publicación de La Unión Internacional de Telecomunicaciones (UIT) se dio a conocer el resultado de un estudio respecto de la preparación que tienen los países en ciberseguridad. Es un estudio realizado a 193 países, la temática es verificar el grado de compromiso en cinco pilares asociados a la seguridad informática como son: medidas jurídicas, técnicas, organizativas, y creación de capacidades y cooperación. Para realizar la evaluación, la UIT elaboró una serie de preguntas en donde cada pilar representa un área específica de evaluación [4].

En el caso del pilar legal, este mide la presencia de instituciones y marcos legales respecto a ciberseguridad y cibercriminalidad. El segundo, el apartado técnico, evalúa la existencia de instituciones técnicas que puedan enfrentar amenazas de ciberseguridad e implementar acciones al respecto. En el tema organizacional, lo que se mide es la existencia de instituciones de coordinación de políticas y estrategias para el desarrollo de la ciberseguridad a escala nacional. El cuarto pilar, referente a la creación de capacidades, evalúa la existencia de educación, investigación y desarrollo, y programas de entrenamiento, así como la existencia de profesionales certificados e instituciones públicas que promuevan estas buenas prácticas.

La última rama, la de la cooperación, mide la existencia de redes de intercambio de información interinstitucionales y con otros países. Tras la evaluación, se estableció una división general de los países en 3 categorías: países líderes en materia de ciberseguridad, países que están madurando todavía, y países que se encuentran en etapas iniciales de su desarrollo de políticas de seguridad informática. Entre los países líderes, el primer lugar lo ocupa Singapur, seguido por Estados Unidos y Malasia.

Country	GCI Score	Legal	Technical	Organizational	Capacity Building	Cooperation
Singapore	0.92	0.95	0.96	0.88	0.97	0.87
United States	0.91	1	0.96	0.92	1	0.73
Malaysia	0.89	0.87	0.96	0.77	1	0.87
Oman	0.87	0.98	0.82	0.85	0.95	0.75
Estonia	0.84	0.99	0.82	0.85	0.94	0.64
Mauritius	0.82	0.85	0.96	0.74	0.91	0.70
Australia	0.82	0.94	0.96	0.86	0.94	0.44
Georgia	0.81	0.91	0.77	0.82	0.90	0.70
France	0.81	0.94	0.96	0.60	1	0.61
Canada	0.81	0.94	0.93	0.71	0.82	0.70

FIGURA 2. 3 Los diez países más comprometidos con la Seguridad de la Información.

Autor: Unión Internacional de Telecomunicaciones

Entre los 10 países con mejores políticas de ciberseguridad están Omán, Estonia, República de Mauricio, Australia, Georgia, Francia, Canadá y Rusia. Ecuador ocupa el puesto 66 en el listado global de los 193 países.

MATURING		
Albania	Ghana	Peru
Algeria	Greece	Philippines
Argentina	Hungary	Poland
Austria	Iceland	Portugal
Azerbaijan	India	Qatar
Bahrain	Indonesia	Romania
Bangladesh	Iran (Islamic Republic of)	Rwanda
Belarus	Ireland	Saudi Arabia
Belgium	Israel	Senegal
Botswana	Italy	Serbia
Brazil	Jamaica	Slovakia
Brunei Darussalam	Kazakhstan	Slovenia
Bulgaria	Kenya	South Africa
Cameroon	Laos	Spain
Chile	Latvia	Sri Lanka
China	Lithuania	Tanzania
Colombia	Luxembourg	Thailand
Costa Rica	Malta	The Former Yugoslav Rep. of Macedonia
Côte d'Ivoire	Mexico	Tunisia
Croatia	Moldova	Turkey
Cyprus	Montenegro	Uganda
Czech Republic	Morocco	Ukraine
Dem. People's Rep. of Korea	Nigeria	United Arab Emirates
Denmark	Pakistan	Uruguay
Ecuador	Panama	Venezuela
Germany	Paraguay	

FIGURA 2. 4 Países en estado de maduración de seguridad informática.

Autor: Unión Internacional de Telecomunicaciones

Entre los países de Latinoamérica, Ecuador ocupa el sexto lugar. El primero es México, seguido por Uruguay, Brasil, Colombia y Argentina. Por debajo de Ecuador en la región se encuentran, en ese orden, Perú, Venezuela, Chile, Paraguay, El Salvador, Nicaragua y Bolivia.

AMERICAS Region	Score	Global Rank
United States of America	0.919	2
Canada	0.818	9
Mexico	0.660	28
Uruguay	0.647	29
Brazil	0.593	38
Colombia	0.569	46
Panama	0.485	62
Argentina	0.482	63
Ecuador	0.466	66
Peru	0.374	79
Venezuela	0.372	80
Chile	0.367	81

FIGURA 2. 5 Países de región americana con mejores políticas de seguridad.

Autor: Unión Internacional de Telecomunicaciones

En lo que respecta a las tres categorías generales, Ecuador esté en estado intermedio: no figura entre los líderes, pero tampoco está en la lista de países que se encuentran en etapas iniciales de su desarrollo [4].

Es necesario también analizar cuál es la situación dentro de Ecuador y específicamente en las Instituciones de Educación Superior (IES), y aunque no existe un estudio actualizado sobre el estado de salud de las Universidades respecto de la Seguridad Informática, en el 2014 la Corporación Ecuatoriana para el Desarrollo de la Investigación y la Academia (CEDIA) realizó un estudio acerca de la Seguridad de la

Información en las Universidades Ecuatorianas [16], el cual obtuvo los siguientes resultados:

- Sobre si existe un presupuesto exclusivo para la gestión de la seguridad de la información en las Universidades, el 82% no posee un presupuesto y solo el 18% si lo posee.

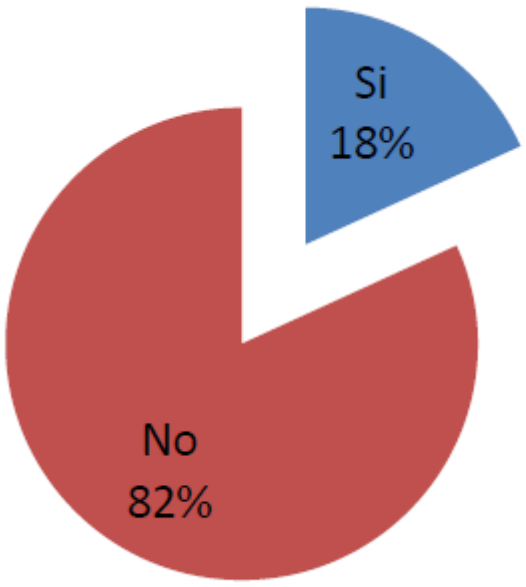

FIGURA 2. 6 Presupuesto específico para la Seguridad de la Información en las IES.

Autor: CEDIA (Año 2014)

- Al consultar sobre si las IES han implementado o están en proceso de implementación de políticas de seguridad en sus procesos, se ha obtenido como resultado que el 82% ya ha implementado o lo está haciendo mientras que un 18% no ha trabajado en ello ni está en

proceso; esto demuestra que las Universidades tienen plena conciencia de que es indispensable el aseguramiento de la información.

Gráfico Su Universidad cuenta con políticas de seguridad de la información

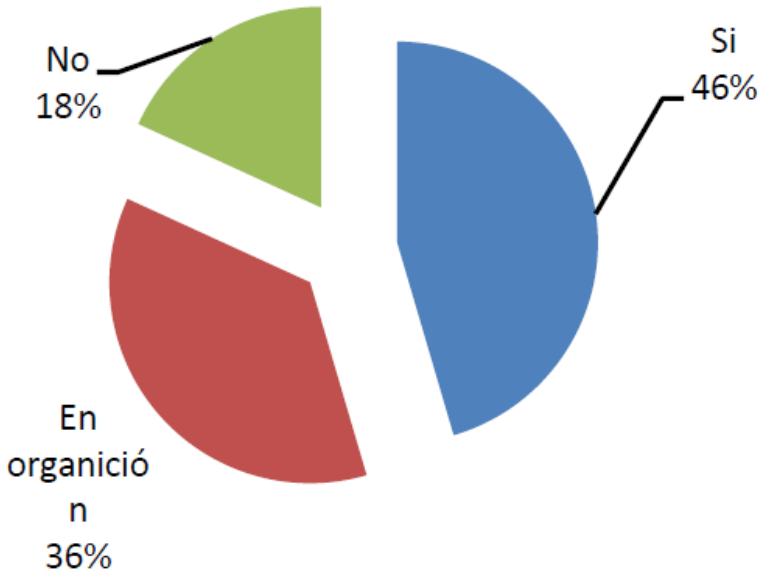

FIGURA 2. 7 Implementación de políticas de seguridad de la información en las IES.

Autor: CEDIA (Año 2014)

- A continuación, se muestra un claro apego por el estándar ISO 27001/27002 para la Gestión de la Seguridad de la Información pues el 100% de las Universidades que tienen algún nivel de implementación de controles de seguridad de la información lo han realizado bajo este estándar.

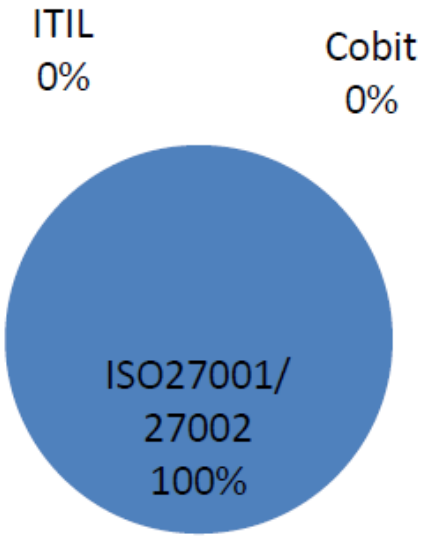

FIGURA 2. 8 Estándar que utilizan IES para la aplicación de políticas de seguridad.

Autor: CEDIA (Año 2014)

- Al ser consultas las IES sobre el tipo de incidentes de los que han sido víctimas, las Universidades han respondido que han sido tres los principales: Malware en su gran mayoría, Accesos no autorizados a los sistemas casi al mismo nivel de malware y Phishing también con un valor bastante preocupante.

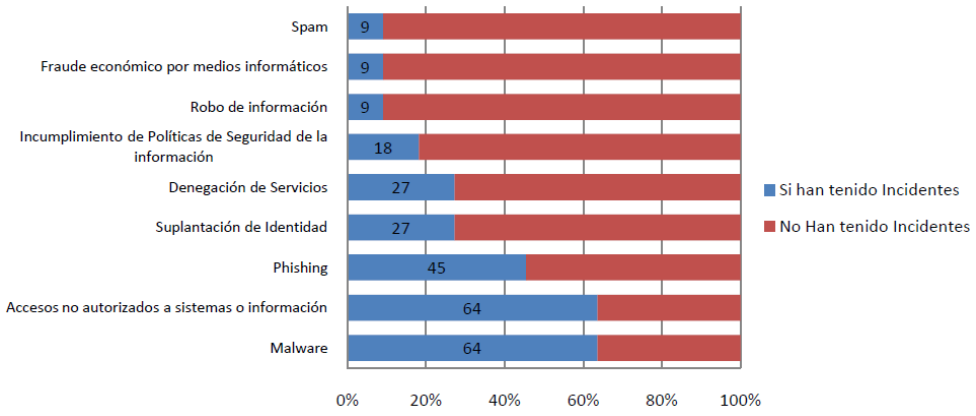

FIGURA 2. 9 Tipo de Incidentes de Seguridad que han tenido las IES.
Autor: CEDIA (Año 2014)

CAPÍTULO 3

SITUACIÓN ACTUAL

3.1 CONTEXTUALIZACIÓN.

La Organización: La Universidad Católica de Cuenca, fue creada con principios cristianos, que tiene como fin la de formar profesionales con altos conocimientos técnicos y científicos dependiendo del área de estudio, profesionales que generen nuevos conocimientos basándose en procesos investigativos, cuya premisa es la vinculación con la sociedad, respetando el medio ambiente y productores de soluciones a los problemas de nuestras sociedades y del país en general [13].

Dirección de Tecnologías de la Información y Comunicación – TIC: La Dirección de Tecnologías de Información y Comunicación, se encarga de coordinar, administrar y gestionar los productos y servicios tecnológicos, a través de sus áreas, asegurando la calidad, funcionalidad y disponibilidad.

Organigrama del Departamento de TIC

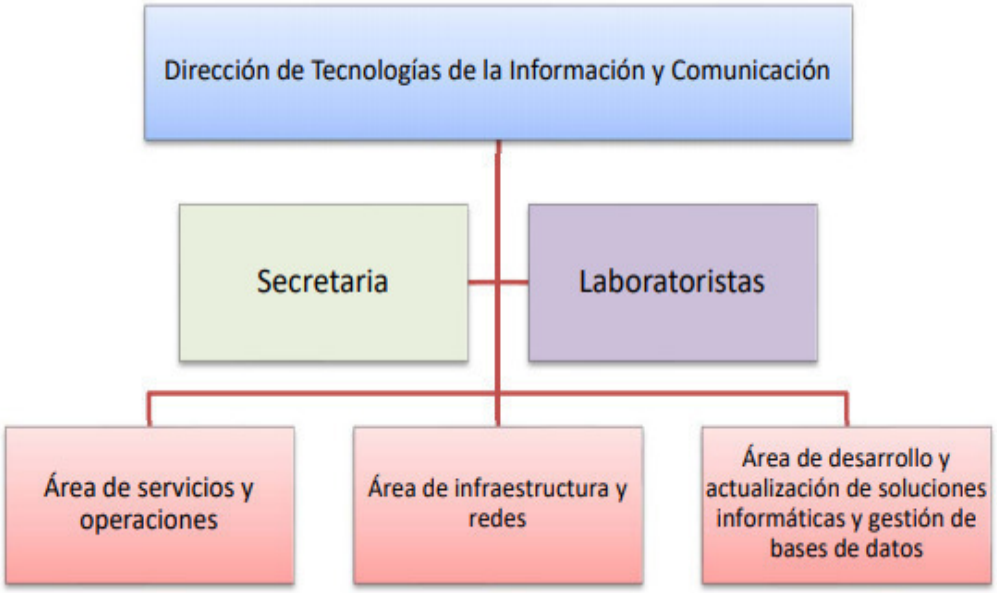

FIGURA 3. 1 Organigrama del departamento de TIC.

Autor: UCACUE

Productos del Departamento de TIC: La dirección de TIC está compuesto por 3 áreas específicas:

Área de Servicios y Operaciones.

Área de Infraestructura y Redes.

Área de Desarrollo y actualización de soluciones informáticas y gestión de Bases de Datos.

Productos del Área de Desarrollo y actualización de soluciones informáticas y gestión de Bases de Datos

Esta área tiene a su cargo el análisis, actualización y desarrollo de soluciones informáticas de necesidad institucional, además de la gestión de las bases de datos de los aplicativos desarrollados por él Área.

Su objetivo principal es la agilización de procesos institucionales, a través de aplicativos y herramientas informáticas ágiles y dinámicas, basadas en normativas, estándares y el uso de las mejores prácticas.

Servicios de Tecnología:

- Aplicaciones Informáticas
- Aulas Virtuales
- Ofimática
- Repositorios digitales
- Seguridad informática
- Conectividad
- Sitios Web
- Producción
- Soporte Técnico

- Gestión de Software

Servicios del área de desarrollo y actualización de soluciones informáticas y gestión de bases de datos:

- Desarrollo y actualización del sistema ERP UNIVERSITY
- Desarrollo y actualización de aplicativos y soluciones informáticas
- Gestión de las bases de datos

3.2 IDENTIFICACIÓN DE LOS INTERESADOS DEL PROCESO DE ACTUALIZACIÓN Y DESARROLLO DE SOLUCIONES INFORMÁTICAS.

La dirección de TIC es un departamento transversal a todos los departamentos de la UCACUE, y una de sus tres áreas consta la de desarrollo y actualización de soluciones informáticas que es donde se desarrolla, actualiza y gestiona el sistema de información core de la Universidad como lo es el ErpUniversity, el cual se está compuesto por todos los módulos de gestión de todos los departamentos de la Universidad, entre los más importantes podemos citar a los siguientes:

- Departamento Académico.
- Departamento Administrativo.
- Departamento Financiero.

- Gestión de Internacionalización.
- Gestión de Infraestructura.
- Departamento de Investigación, Posgrados y Vinculación con la Sociedad.
- Departamento de Vinculación.

FIGURA 3. 2 Áreas de apoyo de TIC.

Autor: UCACUE

3.3 DEFINICIÓN DEL PROCESO DE DESARROLLO Y SOLUCIONES TECNOLÓGICAS.

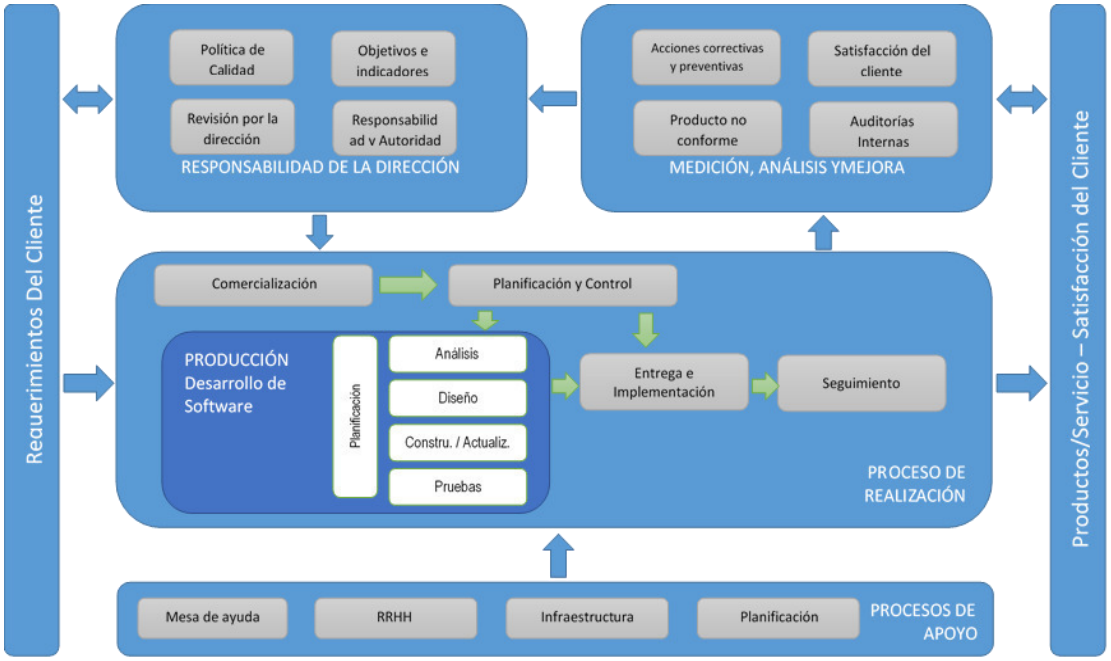

FIGURA 3. 3 Proceso de Desarrollo y Actualización de Software.

3.4 IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN DEL PROCESO DE ACTUALIZACIÓN Y DESARROLLO DE SOLUCIONES INFORMÁTICAS.

Teniendo en cuenta que un activo son todos los elementos de una entidad que se requieren para el correcto desarrollo de sus procesos misionales y de soporte y los cuales son objeto de tratamiento en la gestión de riesgos durante la implementación del sistema de gestión de seguridad de la información en el UCACUE.

El proceso de identificación de activos de información es esencial, éste nos permite identificar los activos que asociados a los procesos de la de la institución, en este caso particular, los activos específicos asociados al proceso de desarrollo y actualización de soluciones informáticas de la UCACUE.

Lista general de activos: El listado de activos de la institución es el siguiente:

Tabla 1 Lista general de activos. Fuente: Autor

NUM.	ACTIVO	TIPO
1	BASE DE DATOS	Información
2	RESPALDOS	Información
3	CODIGOS FUENTES	Información
4	SISTEMA ERP PRODUCCIÓN	Software
5	SISTEMA ERP CERTIFICACION	Software
6	SISTEMA ERP DESARROLLO	Software
7	CONECTIVIDAD (HW)	Comunicaciones
8	SERVIDORES ERP DESARROLLO	Hardware
9	SERVIDORES ERP CERTIFICACIÓN	Hardware
10	SERVIDORES ERP PRODUCCIÓN	Hardware
11	FIREWALLS (HW)	Hardware

NUM.	ACTIVO	TIPO
12	RED DE ÁREA LOCAL E INALÁMBRICA	Comunicaciones
13	GENERADOR (HW)	Hardware
14	UPS (HW)	Hardware
15	SISTEMA DE CLIMATIZACION (HW)	Hardware
16	ESTUDIANTES	Usuarios
17	FUNCIONARIOS	Usuarios
18	SOPORTE	Usuarios
19	SERVICIO DE INTERNET COMERCIAL	Servicio
20	SERVICIO DE CORREO ELECTRÓNICO	Servicio
21	TELEFONÍA IP	Comunicaciones
22	COPUTADORAS DE ESCRITORIO	Hardware
23	IMPRESORAS	Hardware

Resumen de activos en función de su tipo:

Tabla 2 Activos por tipo. Fuente: Autor

Tipo de activo	Activos
Comunicaciones	3
Hardware	9
Información	3
Servicio	2

Software	3
Usuarios	3
TOTAL	**23**

3.5 CATEGORIZACIÓN DE LOS ACTIVOS DE INFORMACIÓN DEL PROCESO DE ACTUALIZACIÓN Y DESARROLLO DE SOLUCIONES INFORMÁTICAS EN FUNCIÓN DE SU CRITICIDAD.

3.5.1 Importancia de los activos

Los activos serán clasificados en función de las siguientes tablas de valoración:

Tabla 3 Activos por importancia. Fuente: Autor

IMPORTANCIA DEL ACTIVO		
Valoración Cuantitativa	**Valoración Cualitativa**	**Descripción**
1	No Aplica	No aplica el criterio de la importancia para el activo
2	Muy Bajo	El activo no afecta procesos
3	Bajo	El activo puede afectar una tarea aislada de la operación y el proceso. Las pérdidas o afectación sería menores y no incurrirían en sanciones pecuniarias.

4	Medio	El activo puede afectar de forma parcial el proceso de actualización y desarrollo de soluciones informáticas y bases de datos. La pérdidas y afectación pueden ser moderadas.
5	Alto	Uno o varios procesos pueden ser afectados, las pérdidas o afectación causan sanciones.
6	Crítico	La Institución se ve seriamente afectada puede generar sanciones elevadas y afectar la credibilidad de la institución y su proceso de actualización y desarrollo de soluciones informáticas y bases de datos.

CONFIDENCIALIDAD		DISPONIBILIDAD		INTEGRIDAD		IMPORTANCIA	
1	No Aplica	1	No Aplica	1	No Aplica	1	No Aplica
2	Pública	2	Muy bajo	2	Muy bajo	2	Muy Bajo
3	Uso Interno	3	Bajo	3	Bajo	3	Bajo
4	Uso Restringido	4	Medio	4	Medio	4	Medio
5	Confidencial	5	Alto	5	Alto	5	Alto
6	Secreto	6	Crítico	6	Crítico	6	Critica

FIGURA 3. 4 Niveles de Criticidad de los Activos.

3.5.2 Inventario de activos en función de su criticidad

Tabla 4 Activos por criticidad. Fuente: Autor

N°	Activo	Tipo	Propietario	Custodio	C	D	I	Ẋ	Impor-tancia
1	Base de datos	Información	Proceso de desarrollo	CEDIA	5	4	6	5	ALTO
2	Respaldos	información	proceso de desarrollo	CEDIA	4	2	3	3	BAJO
3	Códigos fuentes	información	proceso de desarrollo	CEDIA	5	2	6	4	MEDIO
4	Sistema ERP producción	software	proceso de desarrollo	CEDIA	5	4	6	5	ALTO
5	Sistema ERP certificación	software	proceso de desarrollo	infraestructura	4	2	3	3	BAJO
6	Sistema ERP desarrollo	software	proceso de desarrollo	infraestructura	3	2	3	3	BAJO
7	conectividad (hw)	comunicaciones	área de redes e infraestructura	redes/infraestructura	4	5	3	4	MEDIO
8	servidores ERP desarrollo	hardware	área de redes e infraestructura	redes/infraestructura	4	4	4	4	MEDIO

N°	Activo	Tipo	Propietario	Custodio	C	D	I	Ẋ	Impor-tancia
9	servidores ERP certificación	hardware	área de redes e infraestructura	redes/infraestructura	3	2	3	3	BAJO
10	servidores ERP producción	hardware	área de redes e infraestructura	CEDIA	3	2	3	3	BAJO
11	firewall (hw)	hardware	área de redes e infraestructura	cedia /redes e infraestructura	5	5	4	5	ALTO
12	red de área local e inalámbrica	comunicaciones	área de redes e infraestructura	redes/infraestructura	3	5	3	4	MEDIO
13	generador (hw)	hardware	departamento de obras	departamento de obras	1	5	2	3	BAJO
14	ups (hw)	hardware	área de redes e infraestructura	redes/infraestructura	1	5	4	3	BAJO
15	sistema de climatización (hw)	hardware	área de redes e infraestructura	redes/infraestructura	1	3	2	2	MUY BAJO
16	estudiantes	usuarios	n/a	n/a	4	3	4	4	MEDIO
17	Funcionarios	usuarios	n/a	n/a	4	4	4	4	MEDIO
18	Soporte	usuarios	n/a	n/a	3	4	2	3	BAJO

N°	Activo	Tipo	Propietario	Custodio	C	D	I	Ẋ	Impor-tancia
19	servicio de internet	servicio	área de redes e infraestructura	redes/infraestructura	3	5	4	4	MEDIO
20	servicio de correo electrónico	servicio	área de operaciones y servicios	operaciones / servicios	5	3	5	4	MEDIO
21	telefonía ip	comunicaciones	área de redes e infraestructura	redes/infraestructura	1	3	1	2	MUY BAJO
22	computadoras de escritorio	hardware	área de redes e infraestructura	Usuario Final	3	4	2	3	BAJO
23	impresoras	hardware	área de redes e infraestructura	Usuario Final	N/A	N/A	N/A	N/A	N/A

CAPÍTULO 4

ANÁLISIS Y GESTIÓN DE RIESGOS DE SEGURIDAD.

4.1 ANÁLISIS DE AMENAZAS Y VULNERABILIDADES DE LOS ACTIVOS INFORMÁTICOS DEL PROCESO DE ACTUALIZACIÓN Y DESARROLLO DE SOLUCIONES INFORMÁTICAS.

El análisis de las amenazas y vulnerabilidades es quizá el proceso más importante un proyecto de implementación de un esquema de seguridad informática en una empresa o institución, pues es el que nos permite

conocer el nivel de protección de una empresa frente a amenazas a la seguridad de su información.

Todavía en la actualidad; muchas empresas tienen la percepción de que sus activos digitales se encuentran bien resguardados al instalar un antivirus corporativo; e instruir a los empleados en la creación de claves y contraseñas seguras en conjunto con otras prácticas centradas en el usuario. Lo cierto es que estas medidas son escasamente un escaño a escalar para la mitigación integral del riesgo informático, por lo que cabe ser muy minucioso al analizar y relacionar los activos con las amenazas y su nivel de vulnerabilidad.

4.1.1 Identificar las Amenazas en función de su probabilidad e impacto.

Para este efecto se tendrán en cuenta las siguientes escalas:

Tabla 5 Probabilidad de ocurrencia. Fuente: Autor

Valor		Probabilidad
Valor cualitativo	Valor cuantitativo	
Casi seguro	5	Se espera que el evento ocurra en la mayoría de las circunstancias. Más de 1 vez al año.
Probable	4	El evento probablemente ocurrirá en la mayoría de las circunstancias. Al menos de 1 vez en el último año.
Posible	3	El evento podría ocurrir en algún momento. Al menos de 1 vez en los últimos 2 años.
Improbable	2	El evento puede ocurrir en algún momento. Al menos de 1 vez en los últimos 5 años.
Raro	1	El evento puede ocurrir solo en circunstancias excepcionales. No se ha presentado en los últimos 5 años.

Tabla 6 Probabilidad de ocurrencia. Fuente: Autor

Valor Cualitativo	Valor Cuantitativo	Impacto
Catastrófico	5	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad.
Mayor	4	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad
Moderado	3	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad.
Menor	2	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad
Insignificante	1	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad.

Probabilidad vs impacto

PROBABILIDAD	IMPACTO - CONSECUENCIA				
	INSIGNIFICANTE	MENOR	MODERADO	MAYOR	CATASTRÓFICO
RARO	BAJO	BAJO	MODERADO	ALTO	ALTO
IMPROBABLE	BAJO	BAJO	MODERADO	ALTO	EXTREMO
POSIBLE	BAJO	MODERADO	ALTO	EXTREMO	EXTREMO
PROBABLE	MODERADO	ALTO	ALTO	EXTREMO	EXTREMO
CASI SEGURO	ALTO	ALTO	EXTREMO	EXTREMO	EXTREMO

FIGURA 4. 1 Probabilidad Vs Impacto.

Niveles de aceptación del riesgo

Tabla 7 Niveles de aceptación del riesgo. Fuente: Autor

Niveles de aceptación del Riesgo	
Niveles	**Objetivo**
Bajo	No aplica controles
Moderado	Aplica controles para llevar a nivel de aceptación
Alto	Aplica controles para llevar a nivel bajo
Extremo	Aplica controles para llevar a nivel medio

4.1.2 Asociación del activo de las amenazas y vulnerabilidades

Tabla 8 Activos, amenazas y vulnerabilidades. Fuente: Autor

ACTIVO	VALOR DEL ACTIVO	AMENAZA	VULNERABILIDAD ASOCIADA
BASE DE DATOS	5	Acceso no autorizado	Elevación de privilegios
			Contraseñas Débiles
			Cuentas de usuario sin auditar
		Pérdida de información	Procedimientos de Backup
			Inyección SQL
		Plataforma	Actualización de software no aplicado
			Uso de software no licenciado
			Software malicioso
			Negación de servicio
CODIGOS FUENTES	4	Pérdida	Copias de seguridad no apropiadas
		Acceso no autorizado	Elevación de privilegios
		Almacenamiento	Plataforma no adecuada
		Robo de información	Sustracción de fuentes no autorizado
SISTEMA ERP PRODUCCIÓN (SW)	**5**	Acceso no autorizado	Robo de credenciales
			Suplantación de identidad
			Expiración de sesión insuficiente

ACTIVO	VALOR DEL ACTIVO	AMENAZA	VULNERABILIDAD ASOCIADA
			Fuerza bruta
			Acceso de usuarios inactivos o externos
			Autenticación Insuficiente
		Error entrada de datos	Ejecución de código arbitrario
			Poca validación en la entrada de datos
		Pérdida de información	Manipulación de entradas (URL´s, campos)
			Manipulación de información sensible académica (registros, notas, títulos, etc)
			Manipulación de información sensible financiera (saldos, cxc, cxp, etc)
			Abuso de funcionalidad
		Plataforma	Actualización de software no aplicado
			Softawre malicioso
			Software no licenciado
			Programación inadecuada
			Predicción de ubicación de recursos
			Canal inseguro
			Negación de servicio

ACTIVO	VALOR DEL ACTIVO	AMENAZA	VULNERABILIDAD ASOCIADA
SISTEMA ERP CERTIFICACIÓN (SW)	5	Acceso no autorizado	Robo de credenciales
			Suplantación de identidad
			Expiración de sesión insuficiente
			Fuerza bruta
			Acceso de usuarios inactivos o externos
			Autenticación Insuficiente
		Error entrada de datos	Ejecución de código arbitrario
			Poca validación en la entrada de datos
		Pérdida de información	Manipulación de entradas (URL´s, campos)
			Manipulación de información sensible académica (registros, notas, títulos, etc)
			Manipulación de información sensible financiera (saldos, cxc, cxp, etc)
			Abuso de funcionalidad
		Plataforma	Actualización de software no aplicado
			Softawre malicioso
			Software no licenciado
			Programación inadecuada

ACTIVO	VALOR DEL ACTIVO	AMENAZA	VULNERABILIDAD ASOCIADA
			Predicción de ubicación de recursos
			Canal inseguro
			Negación de servicio
SISTEMA ERP DESARROLLO (SW)	**4**	Acceso no autorizado	Robo de credenciales
			Suplantación de identidad
			Expiración de sesión insuficiente
			Fuerza bruta
			Acceso de usuarios inactivos o externos
			Autenticación Insuficiente
		Error entrada de datos	Ejecución de código arbitrario
			Poca validación en la entrada de datos
		Pérdida de información	Manipulación de entradas (URL´s, campos)
			Manipulación de información sensible académica (registros, notas, títulos, etc)
			Manipulación de información sensible financiera (saldos, cxc, cxp, etc)
			Abuso de funcionalidad

ACTIVO	VALOR DEL ACTIVO	AMENAZA	VULNERABILIDAD ASOCIADA
		Plataforma	Actualización de software no aplicado
			Softawre malicioso
			Software no licenciado
			Programación inadecuada
			Predicción de ubicación de recursos
			Canal inseguro
			Negación de servicio
SERVIDORES (HW)	4	Acceso FTP sin autenticación	Utilización de puerto 21 para accesar
		Acceso Telnet sin autenticación	Utilización de puerto 23 para accesar
		Conexiones sin cifrar	No uso de certificados SSL firmados
		Accesos no autorizados	Ataque de fuerza bruta y elevación de privilegios
CONECTIVIDAD	4	Ingresos por Telnet	Ataques de Fuerza Bruta
		No filtrar paquetes ICMP	DOS
		Accesos VTY sin restricción	Ataque de Fuerza bruta
FIREWALL (HW)	5	No asignación de zonas	Descubrimiento de la red interna
		OS no actualizado	Exploits para OS antiguos
		Protocolo ICMP abierto	DOS
RED DE ÁREA LOCAL E INLÁMBRICA	4	Atacantes externos	Puntos expuestos o redes inalámbricas abiertas o con accesos frágiles

ACTIVO	VALOR DEL ACTIVO	AMENAZA	VULNERABILIDAD ASOCIADA
		Falla Humana	Falta de capacitación del personal técnico
		Personal no autorizado acceda al rack de comunicación	Falta de control de acceso al rack de comunicaciones
		Tiempos altos en arreglos de problemas de red	Falta de diagrama de conexiones de red
		Accesos no autorizados a la red inalámbrica	Políticas de acceso deficientes para acceso a la red inalámbrica
ESTUDIANTES	**4**	Ingeniería social	Usuarios no capacitados en seguridad informática
			Acceso a usuarios con información sensible
			Acceso a redes sociales desde redes internas
			Claves de acceso a los sistemas expuestas
		Acceso no autorizado a la plataforma	Poco apego a la políticas de seguridad informática
			Sistemas operativos sin software antivirus
			Actualización de software no aplicado
			Acceso a redes inalámbricas no confiables

ACTIVO	VALOR DEL ACTIVO	AMENAZA	VULNERABILIDAD ASOCIADA
			Uso de software no licenciado
FUNCIONARIOS	4	Disconformidad laboral en personal retirado de sus funciones	Roles de acceso no retirados inmediatamente
		Falla humana	Personal no capacitado en el rol que desempeña
		Amenazas externas (hackers, crackers, etc.)	Falta de políticas de control de acceso
		Robo de información	Falta políticas de monitoreo
		Negligencia	Falta de políticas de uso de sistemas
SERVICIO DE INTERNET	4	Falla de servidor de internet	No alta disponibilidad en servidores
		Caída de enlace de ISP	No poseer más de un ISP
		Lentitud en las transacciones	Ancho de banda deficiente
		Corte de servicio de energía eléctrica	No poseer un generador de energía de altas prestaciones
SERVICIO DE CORREO ELECTRÓNICO	4	Infecciones a través de correo electrónico	Desconocimiento de los usuarios acerca de uso de correo electrónico seguro.
		Software malicioso	Falla de configuración en seguridades de servidor de correo electrónico

ACTIVO	VALOR DEL ACTIVO	AMENAZA	VULNERABILIDAD ASOCIADA
		Spam	Desconocimiento de la política de seguridad sobre correo electrónico institucional

FIGURA 4. 2 Causa, probabilidad y efecto.

4.2 IDENTIFICACIÓN DE RIESGOS Y AMEZANAS.

Con las entrevistas realizadas con cada uno de los líderes de los procesos, se pudo identificar cualitativamente la probabilidad de ocurrencia de las amenazas y el impacto de las mismas por cada activo y tipo de activo identificado, para determinar en qué categoría de riesgo se ubica.

49 Amenazas para los 13 Activos:

Tabla 9 Asociación de activos, amenazas y vulnerabilidades, probabilidad e impacto.

Fuente: Autor

TIPO DE RIESGO	TIPO DE ACTIVO	ACTIVO	AMENAZA	VULNERABILIDAD ASOCIADA	APLICA	PROBABILIDAD	IMPACTO
Riesgo operativo	INFORMACIÓN	BASE DE DATOS	Acceso no autorizado	Elevación de privilegios	Si	Posible	Mayor
Riesgo operativo				Contraseñas Débiles	Si	Improbable	Moderado
Riesgo operativo				Cuentas de usuario sin auditar	Si	Posible	Mayor
Riesgo operativo			Pérdida de información	Procedimientos de Backup	Si	Improbable	Menor
Riesgo operativo				Inyección SQL	Si	Probable	Moderado
Riesgo operativo			Plataforma	Actualización de software no aplicado	Si	Probable	Moderado

TIPO DE RIESGO	TIPO DE ACTIVO	ACTIVO	AMENAZA	VULNERABILIDAD ASOCIADA	APLICA	PROBABILIDAD	IMPACTO
Riesgo operativo				Uso de software no licenciado	Si	Probable	Moderado
Riesgo operativo				Software malicioso	Si	Probable	Moderado
Riesgo operativo				Negación de servicio	Si	Probable	Moderado
Riesgo operativo		CÓDIGO FUENTE	Pérdida	Copias de seguridad no apropiadas	Si	Improbable	Menor
Riesgo operativo			Acceso no autorizado	Elevación de privilegios	Si	Probable	Mayor
Riesgo Tecnológico			Almacenamiento	Plataforma no adecuada	Si	Improbable	Menor
Riesgo operativo			Robo de información	Sustracción de fuentes no autorizado	Si	Probable	Moderado
Riesgo operativo	SOFTWARE	SISTEMA ERP PRODUCCIÓN (SW)	Acceso no autorizado	Robo de credenciales	Si	Posible	Moderado
Riesgo operativo				Suplantación de identidad	Si	Posible	Moderado
Riesgo operativo				Expiración de sesión insuficiente	Si	Improbable	Moderado
Riesgo operativo				Fuerza bruta	Si	Probable	Moderado

TIPO DE RIESGO	TIPO DE ACTIVO	ACTIVO	AMENAZA	VULNERABILIDAD ASOCIADA	APLICA	PROBABILIDAD	IMPACTO
Riesgo operativo				Acceso de usuarios inactivos o externos	Si	Probable	Moderado
Riesgo operativo				Autenticación Insuficiente	Si	Probable	Menor
Riesgo operativo			Error entrada de datos	Ejecución de código arbitrario	Si	Probable	Menor
Riesgo operativo				Poca validación en la entrada de datos	Si	Posible	Menor
Riesgo operativo			Pérdida de información	Manipulación de entradas (URL´s, campos)	Si	Probable	Moderado
Riesgo operativo				Manipulación de información sensible académica (registros, notas, títulos, etc)	Si	Probable	Mayor
Riesgo operativo				Manipulación de información sensible financiera (saldos, cxc, cxp, etc)	Si	Probable	Mayor

TIPO DE RIESGO	TIPO DE ACTIVO	ACTIVO	AMENAZA	VULNERABILIDAD ASOCIADA	APLICA	PROBABILIDAD	IMPACTO
Riesgo operativo				Abuso de funcionalidad	Si	Posible	Menor
Riesgo operativo			Plataforma	Actualización de software no aplicado	Si	Improbable	Menor
Riesgo operativo				Software malicioso	Si	Probable	Moderado
Riesgo operativo				Software no licenciado	Si	Improbable	Menor
Riesgo operativo				Programación inadecuada	Si	Probable	Moderado
Riesgo operativo				Predicción de ubicación de recursos	Si	Probable	Menor
Riesgo operativo				Canal inseguro	Si	Probable	Moderado
Riesgo operativo				Negación de servicio	Si	Probable	Moderado
Riesgo operativo		SISTEMA ERP CERTIFICACIÓN (SW)	Acceso no autorizado	Robo de credenciales	Si	Posible	Moderado
Riesgo operativo				Suplantación de identidad	Si	Posible	Moderado
Riesgo operativo				Expiración de sesión insuficiente	Si	Improbable	Moderado
Riesgo operativo				Fuerza bruta	Si	Probable	Moderado

TIPO DE RIESGO	TIPO DE ACTIVO	ACTIVO	AMENAZA	VULNERABILIDAD ASOCIADA	APLICA	PROBABILIDAD	IMPACTO
Riesgo operativo				Acceso de usuarios inactivos o externos	Si	Probable	Moderado
Riesgo operativo				Autenticación Insuficiente	Si	Probable	Menor
Riesgo operativo			Error entrada de datos	Ejecución de código arbitrario	Si	Probable	Menor
Riesgo operativo				Poca validación en la entrada de datos	Si	Posible	Menor
Riesgo operativo			Pérdida de información	Manipulación de entradas (URL´s, campos)	Si	Probable	Moderado
Riesgo operativo				Manipulación de información sensible académica (registros, notas, títulos, etc)	Si	Probable	Mayor
Riesgo operativo				Manipulación de información sensible financiera (saldos, cxc, cxp, etc)	Si	Probable	Mayor

TIPO DE RIESGO	TIPO DE ACTIVO	ACTIVO	AMENAZA	VULNERABILIDAD ASOCIADA	APLICA	PROBABILIDAD	IMPACTO
Riesgo operativo				Abuso de funcionalidad	Si	Posible	Menor
Riesgo operativo			Plataforma	Actualización de software no aplicado	Si	Improbable	Menor
Riesgo operativo				Software malicioso	Si	Probable	Moderado
Riesgo operativo				Software no licenciado	Si	Improbable	Menor
Riesgo operativo				Programación inadecuada	Si	Probable	Moderado
Riesgo operativo				Predicción de ubicación de recursos	Si	Probable	Menor
Riesgo operativo				Canal inseguro	Si	Probable	Moderado
Riesgo operativo				Negación de servicio	Si	Probable	Moderado
Riesgo operativo		SISTEMA ERP DESARROLLO (SW)	Acceso no autorizado	Robo de credenciales	Si	Posible	Menor
Riesgo operativo				Suplantación de identidad	Si	Posible	Menor
Riesgo operativo				Expiración de sesión insuficiente	Si	Improbable	Menor
Riesgo operativo				Fuerza bruta	Si	Improbable	Insignificante

TIPO DE RIESGO	TIPO DE ACTIVO	ACTIVO	AMENAZA	VULNERABILIDAD ASOCIADA	APLICA	PROBABILIDAD	IMPACTO
Riesgo operativo				Acceso de usuarios inactivos o externos	Si	Improbable	Insignificante
Riesgo operativo				Autenticación Insuficiente	Si	Probable	Menor
Riesgo operativo			Error entrada de datos	Ejecución de código arbitrario	Si	Probable	Menor
Riesgo operativo				Poca validación en la entrada de datos	Si	Posible	Menor
Riesgo operativo			Pérdida de información	Manipulación de entradas (URL´s, campos)	Si	Probable	Menor
Riesgo operativo				Manipulación de información sensible académica (registros, notas, títulos, etc)	Si	Probable	Menor
Riesgo operativo				Manipulación de información sensible financiera (saldos, cxc, cxp, etc)	Si	Probable	Menor

TIPO DE RIESGO	TIPO DE ACTIVO	ACTIVO	AMENAZA	VULNERABILIDAD ASOCIADA	APLICA	PROBABILIDAD	IMPACTO
Riesgo operativo				Abuso de funcionalidad	Si	Posible	Insignificante
Riesgo operativo			Plataforma	Actualización de software no aplicado	Si	Improbable	Menor
Riesgo operativo				Software malicioso	Si	Probable	Menor
Riesgo operativo				Software no licenciado	Si	Improbable	Menor
Riesgo operativo				Programación inadecuada	Si	Probable	Menor
Riesgo operativo				Predicción de ubicación de recursos	Si	Probable	Menor
Riesgo operativo				Canal inseguro	Si	Probable	Menor
Riesgo operativo				Negación de servicio	Si	Probable	Menor
Riesgo operativo	HARDWARE	SERVIDORES (HW)	Acceso FTP sin autenticación	Utilización de puerto 21 para acceder	Si	Improbable	Menor
Riesgo operativo			Acceso Telnet sin autenticación	Utilización de puerto 23 para acceder	Si	Improbable	Menor

TIPO DE RIESGO	TIPO DE ACTIVO	ACTIVO	AMENAZA	VULNERABILIDAD ASOCIADA	APLICA	PROBABILIDAD	IMPACTO
Riesgo operativo			Conexiones sin cifrar	No uso de certificados SSL firmados	Si	Improbable	Menor
Riesgo operativo			Accesos no autorizados por webmin	Ataque de fuerza bruta y elevación de privilegios	Si	Probable	Mayor
Riesgo operativo		FIREWALL (HW)	No asignación de zonas	Descubrimiento de la red interna	Si	Improbable	Menor
Riesgo operativo			OS no actualizado	Exploits para OS antiguos	Si	Improbable	Menor
Riesgo operativo			Protocolo ICMP abierto	DDOS	Si	Improbable	Menor
Riesgo operativo		RED DE ÁREA LOCAL E INLÁMBRICA	Cableado mal ponchado	Cableado en mal estado	Si	Probable	Insignificante
Riesgo operativo			Falla Humana	Falta de capacitación del personal técnico	Si	Probable	Menor
Riesgo operativo			Personal no autorizado acceda al rack de	Falta de control de acceso al rack de comunicaciones	Si	Improbable	Mayor

TIPO DE RIESGO	TIPO DE ACTIVO	ACTIVO	AMENAZA	VULNERABILIDAD ASOCIADA	APLICA	PROBABILIDAD	IMPACTO
			comunicación				
Riesgo operativo			Falta de diagrama de conexiones de red	Falta de documentación técnica	Si	Improbable	Menor
Riesgo operativo			Políticas de acceso deficientes para acceso a la red inalámbrica	accesos no autorizados a la red inalámbrica	Si	Improbable	Menor
Riesgo operativo	USUARIOS	ESTUDIANTES	Ingeniería social	Robo de identidad	Si	Probable	Menor
Riesgo operativo				Fraude informático	Si	Posible	Menor
Riesgo operativo				Intercepción ilícita	Si	Probable	Menor
Riesgo operativo				Phishing	Si	Probable	Moderado
Riesgo operativo			Plataforma	Poco apego a la políticas de seguridad informática	Si	Probable	Menor
Riesgo operativo				Software malicioso	Si	Probable	Moderado

TIPO DE RIESGO	TIPO DE ACTIVO	ACTIVO	AMENAZA	VULNERABILIDAD ASOCIADA	APLICA	PROBABILIDAD	IMPACTO
Riesgo operativo				Actualización de software no aplicado	Si	Probable	Menor
Riesgo operativo				Acceso a redes inalambricas no confiables	Si	Probable	Menor
Riesgo operativo				Software no licenciado	Si	Probable	Menor
Riesgo operativo		FUNCIONARIOS	Despidos al personal	Disconformidad laboral	Si	Probable	Mayor
Riesgo operativo			Falla humana	Impericia en el manejo del software	Si	Probable	Moderado
Riesgo operativo			Amenazas externas (hackers, crackers, etc.)	Falta de control de acceso	Si	Probable	Mayor
Riesgo operativo			Robo de información	Falta de monitoreo	Si	Probable	Moderado
Riesgo operativo			Negligencia	Falta de políticas de uso de sistemas	Si	Probable	Moderado
Riesgo operativo	COMUNICACIONES	SERVICIO DE	Falla de servidor de internet	No alta disponibilidad en servidores	Si	Improbable	Mayor

TIPO DE RIESGO	TIPO DE ACTIVO	ACTIVO	AMENAZA	VULNERABILIDAD ASOCIADA	APLICA	PROBABILIDAD	IMPACTO
Riesgo operativo		INTERNET	Caída de enlace de ISP	No poseer más de un ISP	Si	Improbable	Moderado
Riesgo operativo			Lentitud en las transacciones	Ancho de banda deficiente	Si	Improbable	Moderado
Riesgo Tecnológico			Corte de servicio de energía eléctrica	No poseer un generador de energía de altas prestaciones	Si	Improbable	Moderado
Riesgo operativo		CONECTIVIDAD	Ingresos por Telnet	Ataques de Fuerza Bruta	Si	Improbable	Mayor
Riesgo operativo			No filtrar paquetes ICMP	DDOS	Si	Probable	Moderado
Riesgo operativo			Accesos VTY sin restricción	Ataque de Fuerza bruta	Si	Improbable	Mayor
Riesgo operativo		SERVICIO DE CORREO ELECTRÓNICO	Falta de Capacitación de uso de correo electrónico	Desconocimiento de buenas prácticas de utilización de correo electrónico	Si	Posible	Menor

TIPO DE RIESGO	TIPO DE ACTIVO	ACTIVO	AMENAZA	VULNERABILIDAD ASOCIADA	APLICA	PROBABILIDAD	IMPACTO
Riesgo operativo			Falla de configuración en seguridades de servidor de correo electrónico	Software malicioso	Si	Improbable	Moderado
Riesgo operativo			Spam	Desconocimiento de la política de seguridad sobre correo electrónico institucional	Si	Probable	Menor

4.3 CLASIFICACIÓN DE LOS RIESGOS

Tabla 10 Clasificación de los riesgos. Fuente: Autor

TIPO DE RIESGO	TIPO DE ACTIVO	ACTIVO	AMENAZA	V. ASOCIADA	APLICA	P	I	CLASIFICACIÓN
Riesgo operativo	INFORMACIÓN	BASE DE DATOS	Acceso no autorizado	Elevación de privilegios	Si	Alta	Alto	Muy alto
Riesgo operativo				Contraseñas Débiles	Si	Baja	Medio	Bajo

TIPO DE RIESGO	TIPO DE ACTIVO	ACTIVO	AMENAZA	V. ASOCIADA	APLICA	P	I	CLASIFICA-CIÓN
Riesgo operativo				Cuentas de usuario sin auditar	Si	Alta	Alto	Muy alto
Riesgo operativo			Pérdida de información	Procedimientos de Backup	Si	Baja	Bajo	Muy bajo
Riesgo operativo				Inyección SQL	Si	Media	Medio	Medio
Riesgo operativo			Plataforma	Actualización de software no aplicado	Si	Media	Medio	Medio
Riesgo operativo				Uso de software no licenciado	Si	Baja	Medio	Bajo
Riesgo operativo				Software malicioso	Si	Media	Medio	Medio
Riesgo operativo				Negación de servicio	Si	Media	Medio	Medio
Riesgo operativo		CÓDIGO FUENTE	Pérdida	Copias de seguridad no apropiadas	Si	Baja	Bajo	Muy bajo
Riesgo operativo			Acceso no autorizado	Elevación de privilegios	Si	Media	Alto	Alto
Riesgo Tecnológico			Almacenamiento	Plataforma no adecuada	Si	Baja	Bajo	Muy bajo
Riesgo operativo			Robo de información	Sustracción de fuentes no autorizado	Si	Media	Medio	Medio

TIPO DE RIESGO	TIPO DE ACTIVO	ACTIVO	AMENAZA	V. ASOCIADA	APLICA	P	I	CLASIFICA-CIÓN
Riesgo operativo	SOFTWARE	SISTEMA ERP PRODUCCIÓN (SW)	Acceso no autorizado	Robo de credenciales	Si	Alta	Medio	Alto
Riesgo operativo				Suplantación de identidad	Si	Alta	Medio	Alto
Riesgo operativo				Expiración de sesión insuficiente	Si	Baja	Medio	Bajo
Riesgo operativo				Fuerza bruta	Si	Media	Medio	Medio
Riesgo operativo				Acceso de usuarios inactivos o externos	Si	Media	Medio	Medio
Riesgo operativo				Autenticación Insuficiente	Si	Media	Bajo	Bajo
Riesgo operativo			Error entrada de datos	Ejecución de código arbitrario	Si	Media	Bajo	Bajo
Riesgo operativo				Poca validación en la entrada de datos	Si	Alta	Bajo	Medio
Riesgo operativo			Pérdida de información	Manipulación de entradas (URL´s, campos)	Si	Media	Medio	Medio
Riesgo operativo				Manipulación de información sensible	Si	Media	Alto	Alto

TIPO DE RIESGO	TIPO DE ACTIVO	ACTIVO	AMENAZA	V. ASOCIADA	APLICA	P	I	CLASIFICA-CIÓN
				académica (registros, notas, títulos, etc)				
Riesgo operativo				Manipulación de información sensible financiera (saldos, cxc, cxp, etc)	Si	Media	Alto	Alto
Riesgo operativo				Abuso de funcionalidad	Si	Alta	Bajo	Medio
Riesgo operativo			Plataforma	Actualización de software no aplicado	Si	Baja	Bajo	Muy bajo
Riesgo operativo				Software malicioso	Si	Media	Medio	Medio
Riesgo operativo				Software no licenciado	Si	Baja	Bajo	Muy bajo
Riesgo operativo				Programación inadecuada	Si	Media	Medio	Medio
Riesgo operativo				Predicción de ubicación de recursos	Si	Media	Bajo	Bajo
Riesgo operativo				Canal inseguro	Si	Media	Medio	Medio
Riesgo operativo				Negación de servicio	Si	Media	Medio	Medio

TIPO DE RIESGO	TIPO DE ACTIVO	ACTIVO	AMENAZA	V. ASOCIADA	APLICA	P	I	CLASIFICA-CIÓN
Riesgo operativo		SISTEMA ERP CERTIFICACIÓN (SW)	Acceso no autorizado	Robo de credenciales	Si	Alta	Medio	Alto
Riesgo operativo				Suplantación de identidad	Si	Alta	Medio	Alto
Riesgo operativo				Expiración de sesión insuficiente	Si	Baja	Medio	Bajo
Riesgo operativo				Fuerza bruta	Si	Media	Medio	Medio
Riesgo operativo				Acceso de usuarios inactivos o externos	Si	Media	Medio	Medio
Riesgo operativo				Autenticación Insuficiente	Si	Media	Bajo	Bajo
Riesgo operativo			Error entrada de datos	Ejecución de código arbitrario	Si	Media	Bajo	Bajo
Riesgo operativo				Poca validación en la entrada de datos	Si	Alta	Bajo	Medio
Riesgo operativo			Pérdida de información	Manipulación de entradas (URL´s, campos)	Si	Media	Medio	Medio
Riesgo operativo				Manipulación de información sensible académica	Si	Media	Alto	Alto

TIPO DE RIESGO	TIPO DE ACTIVO	ACTIVO	AMENAZA	V. ASOCIADA	APLICA	P	I	CLASIFICA-CIÓN
				(registros, notas, títulos, etc)				
Riesgo operativo				Manipulación de información sensible financiera (saldos, cxc, cxp, etc)	Si	Media	Alto	Alto
Riesgo operativo				Abuso de funcionalidad	Si	Alta	Bajo	Medio
Riesgo operativo			Plataforma	Actualización de software no aplicado	Si	Baja	Bajo	Muy bajo
Riesgo operativo				Software malicioso	Si	Media	Medio	Medio
Riesgo operativo				Software no licenciado	Si	Baja	Bajo	Muy bajo
Riesgo operativo				Programación inadecuada	Si	Media	Medio	Medio
Riesgo operativo				Predicción de ubicación de recursos	Si	Media	Bajo	Bajo
Riesgo operativo				Canal inseguro	Si	Media	Medio	Medio
Riesgo operativo				Negación de servicio	Si	Media	Medio	Medio

TIPO DE RIESGO	TIPO DE ACTIVO	ACTIVO	AMENAZA	V. ASOCIADA	APLICA	P	I	CLASIFICA-CIÓN
Riesgo operativo		SISTEMA ERP DESARROLLO (SW)	Acceso no autorizado	Robo de credenciales	Si	Alta	Bajo	Medio
Riesgo operativo				Suplantación de identidad	Si	Alta	Bajo	Medio
Riesgo operativo				Expiración de sesión insuficiente	Si	Baja	Bajo	Muy bajo
Riesgo operativo				Fuerza bruta	Si	Baja	Bajo	Muy bajo
Riesgo operativo				Acceso de usuarios inactivos o externos	Si	Baja	Bajo	Muy bajo
Riesgo operativo				Autenticación Insuficiente	Si	Media	Bajo	Bajo
Riesgo operativo			Error entrada de datos	Ejecución de código arbitrario	Si	Media	Bajo	Bajo
Riesgo operativo				Poca validación en la entrada de datos	Si	Alta	Bajo	Medio
Riesgo operativo			Pérdida de información	Manipulación de entradas (URL´s, campos)	Si	Media	Bajo	Bajo
Riesgo operativo				Manipulación de información sensible académica	Si	Media	Bajo	Bajo

TIPO DE RIESGO	TIPO DE ACTIVO	ACTIVO	AMENAZA	V. ASOCIADA	APLICA	P	I	CLASIFICA-CIÓN
				(registros, notas, títulos, etc)				
Riesgo operativo				Manipulación de información sensible financiera (saldos, cxc, cxp, etc)	Si	Media	Bajo	Bajo
Riesgo operativo				Abuso de funcionalidad	Si	Alta	Bajo	Medio
Riesgo operativo			Plataforma	Actualización de software no aplicado	Si	Baja	Bajo	Muy bajo
Riesgo operativo				Software malicioso	Si	Media	Bajo	Bajo
Riesgo operativo				Software no licenciado	Si	Baja	Bajo	Muy bajo
Riesgo operativo				Programación inadecuada	Si	Media	Bajo	Bajo
Riesgo operativo				Predicción de ubicación de recursos	Si	Media	Bajo	Bajo
Riesgo operativo				Canal inseguro	Si	Media	Bajo	Bajo
Riesgo operativo				Negación de servicio	Si	Media	Bajo	Bajo

TIPO DE RIESGO	TIPO DE ACTIVO	ACTIVO	AMENAZA	V. ASOCIADA	APLICA	P	I	CLASIFICA-CIÓN
Riesgo operativo	HARDWARE	SERVIDORES (HW)	Acceso FTP sin autenticación	Utilización de puerto 21 para accesar	Si	Baja	Bajo	Muy bajo
Riesgo operativo			Acceso Telnet sin autenticación	Utilización de puerto 23 para accesar	Si	Baja	Bajo	Muy bajo
Riesgo operativo			Conexiones sin cifrar	No uso de certificados SSL firmados	Si	Baja	Bajo	Muy bajo
Riesgo operativo			Accesos no autorizados por webmin	Ataque de fuerza bruta y elevación de privilegios	Si	Media	Alto	Alto
Riesgo operativo		FIREWALL (HW)	No asignación de zonas	Descubrimiento de la red interna	Si	Baja	Bajo	Muy bajo
Riesgo operativo			OS no actualizado	Exploits para OS antiguos	Si	Baja	Bajo	Muy bajo
Riesgo operativo			Protocolo ICMP abierto	DDOS	Si	Baja	Bajo	Muy bajo
Riesgo operativo		RED DE ÁREA LOCAL E INLÁMBRICA	Cableado mal ponchado	Cableado en mal estado	Si	Media	Bajo	Bajo
Riesgo operativo			Falla Humana	Falta de capacitación del personal técnico	Si	Media	Bajo	Bajo
Riesgo operativo			Personal no autorizado	Falta de control de acceso al	Si	Baja	Alto	Medio

TIPO DE RIESGO	TIPO DE ACTIVO	ACTIVO	AMENAZA	V. ASOCIADA	APLICA	P	I	CLASIFICA-CIÓN
			acceda al rack de comunicación	rack de comunicaciones				
Riesgo operativo			Falta de diagrama de conexiones de red	Falta de documentación técnica	Si	Baja	Bajo	Muy bajo
Riesgo operativo			Políticas de acceso deficientes para acceso a la red inalámbrica	accesos no autorizados a la red inalámbrica	Si	Baja	Bajo	Muy bajo
Riesgo operativo	USUARIOS	ESTUDIANTES	Ingeniería social	Robo de identidad	Si	Media	Bajo	Bajo
Riesgo operativo				Fraude informático	Si	Alta	Bajo	Medio
Riesgo operativo				Intercepción ilícita	Si	Media	Bajo	Bajo
Riesgo operativo				Phishing	Si	Media	Medio	Medio
Riesgo operativo			Plataforma	Poco apego a la políticas de seguridad informática	Si	Media	Bajo	Bajo
Riesgo operativo				Software malicioso	Si	Media	Medio	Medio

TIPO DE RIESGO	TIPO DE ACTIVO	ACTIVO	AMENAZA	V. ASOCIADA	APLICA	P	I	CLASIFICA-CIÓN
Riesgo operativo				Actualización de software no aplicado	Si	Media	Bajo	Bajo
Riesgo operativo				Acceso a redes inalámbricas no confiables	Si	Media	Bajo	Bajo
Riesgo operativo				Software no licenciado	Si	Media	Bajo	Bajo
Riesgo operativo		FUNCIONARIOS	Despidos al personal	Disconformidad laboral	Si	Media	Alto	Alto
Riesgo operativo			Falla humana	Impericia en el manejo del software	Si	Media	Medio	Medio
Riesgo operativo			Amenazas externas (hackers, crackers, etc.)	Falta de control de acceso	Si	Media	Alto	Alto
Riesgo operativo			Robo de información	Falta de monitoreo	Si	Media	Medio	Medio
Riesgo operativo			Negligencia	Falta de políticas de uso de sistemas	Si	Media	Medio	Medio
Riesgo operativo	COMUNICACIONES	SERVICIO DE INTERNET	Falla de servidor de internet	No alta disponibilidad en servidores	Si	Baja	Alto	Medio

TIPO DE RIESGO	TIPO DE ACTIVO	ACTIVO	AMENAZA	V. ASOCIADA	APLICA	P	I	CLASIFICA-CIÓN
Riesgo operativo			Caída de enlace de ISP	No poseer más de un ISP	Si	Baja	Medio	Bajo
Riesgo operativo			Lentitud en las transacciones	Ancho de banda deficiente	Si	Baja	Medio	Bajo
Riesgo Tecnológico			Corte de servicio de energía eléctrica	No poseer un generador de energía de altas prestaciones	Si	Baja	Medio	Bajo
Riesgo operativo		CONECTIVIDAD	Ingresos por Telnet	Ataques de Fuerza Bruta	Si	Baja	Alto	Medio
Riesgo operativo			No filtrar paquetes ICMP	DOS	Si	Media	Medio	Medio
Riesgo operativo			Accesos VTY sin restricción	Ataque de Fuerza bruta	Si	Baja	Alto	Medio
Riesgo operativo		SERVICIO DE CORREO ELECTRÓNICO	Falta de Capacitación de uso de correo electrónico	Desconocimiento de buenas prácticas de utilización de correo electrónico	Si	Alta	Bajo	Medio
Riesgo operativo			Falla de configuración en	Software malicioso	Si	Baja	Medio	Bajo

TIPO DE RIESGO	TIPO DE ACTIVO	ACTIVO	AMENAZA	V. ASOCIADA	APLICA	P	I	CLASIFICA-CIÓN
			seguridades de servidor de correo electrónico					
Riesgo operativo			Spam	Desconocimiento de la política de seguridad sobre correo electrónico institucional	Si	Media	Bajo	Bajo

4.4 IDENTIFICACIÓN DE RIESGOS CON MAYOR INCIDENCIA.

No aplica, pues la institución no tiene un historial de los riesgos con mayor incidencia.

4.5 EVALUACIÓN DE LOS RIESGOS.

Nivel de riesgo aceptable:

En este caso solo se hará notar el riesgo inherente porque aún no se han aplicado controles para mitigar el riesgo.

Riesgo Inherente: 106

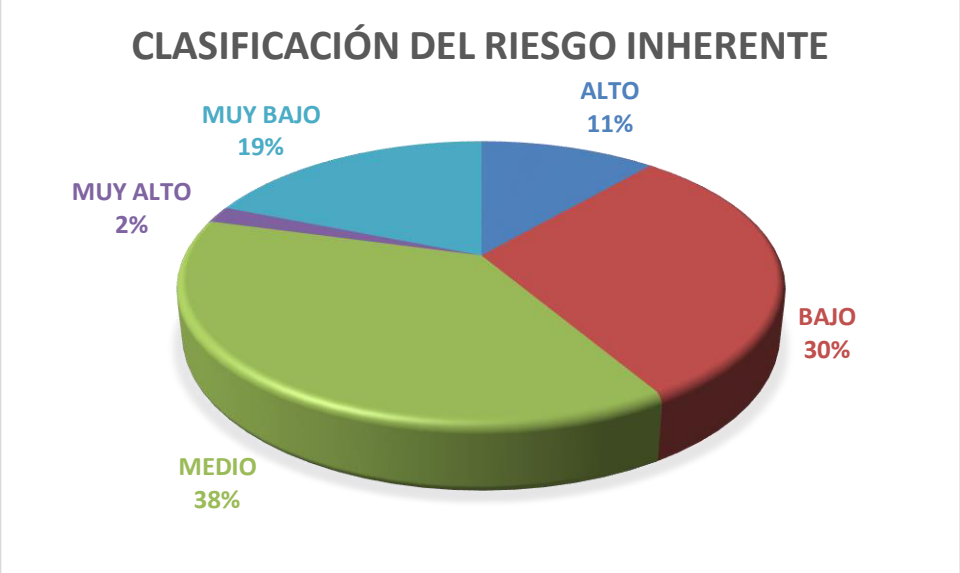

FIGURA 4. 3 Riesgo Inherente

CAPÍTULO 5

DISEÑO DE LA POLÍTICA

5.1 ESTADO ACTUAL FRENTE A LA SEGURIDAD

El área de Actualización y desarrollo de soluciones informáticas y Bases de Datos ha implementado iniciativas no documentadas relacionadas con la seguridad de la información entorno al cumplimiento de las mejores prácticas dictadas en la Norma ISO27002.

- No cuenta con un Sistema de Gestión de seguridad de la Información de manera formal.
- Las actividades de seguridad implantadas han sido iniciativas de la Dirección de Tecnología y el Área de Redes e Infraestructura.
- No existe un grupo o área específica cuya función sea la de gestionar la seguridad informática íntegramente.

Algunas de las actividades implementadas de manera informal son:

- Definir algunas de las políticas de seguridad de la Información de la entidad.
- Implementar estrategias de concienciación y divulgación de la seguridad de la información anual.
- Definición y gestión de una matriz de controles básica alineada a la norma ISO/IES 27002.
- Levantamiento inicial de un Inventario de activos de Información.
- Implementación de herramientas para garantizar la seguridad de la información como: Database firewall y Data Lost Prevention (DLP).
- Creación de ambientes de desarrollo, certificación y producción de las soluciones informáticas.

5.2 ALCANCE DE LA POLÍTICA

El alcance del plan para la implementación del SGSI se focaliza en el proceso actualización y desarrollo de soluciones informáticas y bases de datos, en el cuál se concentra uno de los tres ejes estratégicos del Departamento de TIC, con los siguientes subprocesos y procedimientos:

Tabla 11 Proceso, subproceso y procedimiento del área de actualización y desarrollo de soluciones informáticas y bases de datos. Fuente: Autor

PROCESO	SUBPROCESO	PROCEDIMIENTO
Desarrollo y actualización del sistema ERP UNIVERSITY	Requerimiento de opciones o reportes que no figuran en el ERP University	Se aplica proceso de control de cambios
	Creación de módulos Informáticos en el ERP University	Se aplica proceso de control de cambios
	Otras modificaciones o configuraciones que el usuario requiera para el ERP University	Se aplica proceso de control de cambios
Desarrollo y actualización de	Requerimiento de opciones o reportes que	Se aplica proceso de control de cambios

PROCESO	SUBPROCESO	PROCEDIMIENTO
aplicativos y soluciones informáticas	no figuran en la plataforma actual	
	Creación de aplicativos o nuevas herramientas de plataformas informáticas	1. Se verifica cumplimiento de normativa de aplicabilidad. 2. Se aplica metodología para el desarrollo de nuevas aplicaciones (Análisis, Diseño, Desarrollo, Pruebas y Entrega)
	Otras modificaciones o configuraciones que el usuario requiera para las plataformas actuales	Se aplica proceso de control de cambios

Proceso de control de cambios

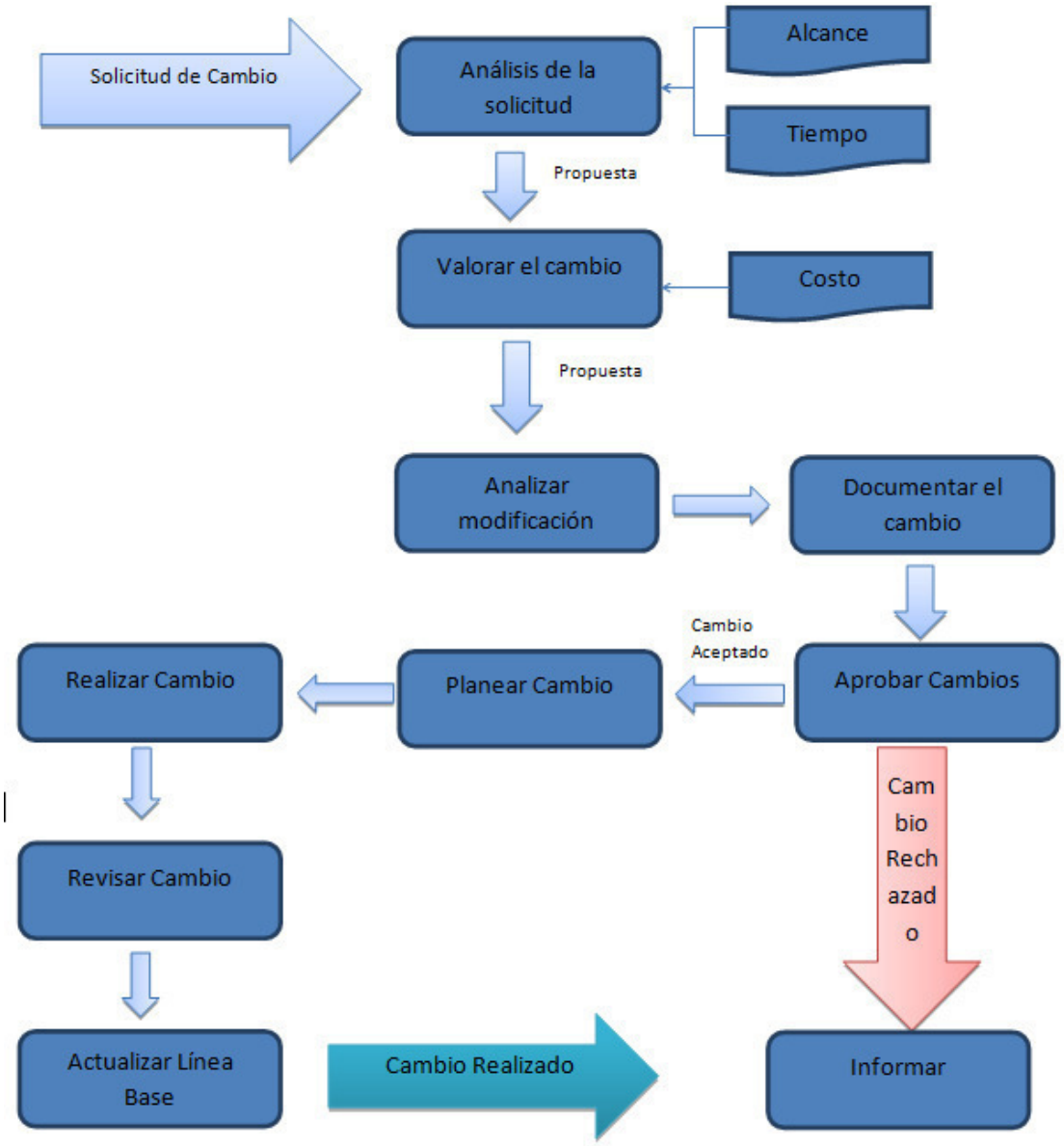

FIGURA 5. 1 Proceso de control de cambios.

5.3 OBJETIVOS DE LA POLÍTICA

- Definir los planes de acción a corto, mediano y largo plazo, que el Departamento de Tecnologías de la Información y Comunicación debe implementar en su proceso de actualización y desarrollo de soluciones informáticas y bases de datos, para garantizar la correcta gestión de un sistema de seguridad de la información cuyo fin es evitar la materialización de incidentes de seguridad y de los riesgos ya identificados.

- Definir la ruta para la implementación de las medidas de seguridad en el proceso de actualización y desarrollo de soluciones informáticas y bases de datos, así como los tiempos, costos y recursos necesarios para la misma.

5.4 ROLES Y RESPONSABILIDADES

La seguridad de la información en una institución de educación superior es factor clave para determinar la habilidad de la Institución para proteger la información, por lo que definir un equipo encargado del SGSI es fundamental para la correcta gestión del sistema. Teniendo en cuenta la naturaleza de la UCACUE, que no tiene operaciones en diferentes países y que las leyes y normas que le aplican son las adoptadas y establecidas

para Ecuador, se plantea una Estructura Organizacional Centralizada de acuerdo al siguiente esquema.

FIGURA 5. 2 Estructura organizacional centralizada de la gestión de seguridad de la información.

5.5 POLÍTICA GENERAL

5.5.1 Objetivo de la política

Establecer un marco de seguridad como estrategia, que defina los riegos de seguridad en el proceso de actualización y desarrollo de soluciones informáticas y bases de datos, así como el tratamiento de los mismos con el objetivo de proteger los activos de información

más sensibles de la entidad alineada a una metodología de riegos establecida.

5.5.2 Aplicación de la política

La presente política de gestión de la seguridad de la información, se plantea de cumplimiento obligatorio para todos los funcionarios y terceros que mantengan relación con accesos a la información de la Universidad.

5.5.3 Sanciones por incumplimiento

El funcionario que no cumpla con lo expuesto en la presente política, deberá sujetarse a las disposiciones disciplinarias por el ente competente en la Universidad previa investigación y comprobación del cometimiento de la falta.

5.5.4 Actualización de la política

La presente política será sometida a revisión y de ser el caso, a actualización, con una periodicidad semestral por el oficial de seguridad, si el caso amerita una actualización o reforma de la política, este deberá ser aprobado por la dirección de tic en conjunto con las representantes de todas las áreas del departamento de TIC de la UCACUE.

5.5.5 Socialización de la política

La difusión de la Política estará a cargo de la Dirección de TIC en coordinación con el departamento de comunicación de la UCACUE.

5.5.6 Aplicación de los controles de seguridad

5.5.6.1. Seguridad ligada a los recursos humanos

Antes de la contratación

Objetivo:

El objetivo de este dominio es definir claramente el cargo, las responsabilidades de este cargo y el perfil del postulante respecto de la seguridad de la información.

Controles

Antes de la contratación:

1. El departamento de Talento Humano será responsable de solicitar y analizar los siguientes requisitos al nuevo aspirante:
    - Referencias de honorabilidad actualizadas de trabajos anteriores en los que haya prestado sus servicios, si fuere el caso de que el postulante no

posea experiencia laboral, deberá presentar certificados de honorabilidad actualizados de personas con datos de localización adecuada como dirección de domicilio y/o trabajo, número de teléfono convencional y móvil, correo electrónico.

- Hoja de vida actualizada y verificada.
- Verificación de las aptitudes para el cargo a contratarse mediante la solicitud de certificados de estudios académicos.
- Verificación de los títulos profesionales obtenidos.
- Certificado y verificación de antecedentes penales actualizado emitido por el Ministerio del interior en el siguiente enlace: http://www.mdi.gob.ec.

2. El postulante que haya salido favorecido para ocupar el cargo solicitado, deberá firmar un acuerdo de confidencialidad de la información que cite, por lo menos, los siguientes requisitos:
    - El empleado o contratista deberá someterse a las políticas de seguridad de la información, dentro y fuera de la institución.

- Los activos a él asignados, deberán ser protegidos contra accesos no autorizados, fuga, pérdida o modificación de la información, que esté bajo su custodia.
- Informar formalmente los eventos, amenazas o riesgos relacionados con la seguridad de la información de los cuales pueda presentar evidencia.
- El presente acuerdo de confidencialidad tiene un carácter de indefinido, es decir no finaliza con la terminación del contrato.

3. Una copia digitalizada de los acuerdos de confidencialidad de los funcionarios deberá ser entregada a la dirección de TICs para su respectivo resguardo y sustentabilidad.

Durante el contrato

Objetivo:

El objetivo de este dominio es asegurar que los funcionarios y personas contratadas para alguna actividad específica estén al tanto y den cumplimiento con sus responsabilidades en materia de seguridad de la

información, así como las consecuencias disciplinarias en el caso de incumplimiento de las mismas, con el fin de minimizar los riesgos de seguridad.

Controles:

1. El funcionario que por cualquier razón no haya firmado el acuerdo de confidencialidad de la información al momento de su contratación deberá hacerlo en un plazo no más allá de quince días se su notificación o llamamiento a firmarlo en el departamento de talento humano de la UCACUE, este acuerdo estará sustentado bajo las premisas descritas en el numeral 2 de la política de seguridad relativa a Seguridad ligada a los recursos humanos - antes de la contratación.

2. Todos los funcionarios y personal de apoyo de la Institución, y cuando la pertinencia lo amerite, los contratistas, deberán ser capacitados en el uso y manejo adecuado de los procedimientos y políticas de seguridad de la información.

3. El Departamento de Procuraduría de la UCACUE, deberá crear y socializar un proceso disciplinario formal

amparados en ley, respecto de violaciones a las políticas de seguridad de la información por parte de los funcionarios y contratistas.

4. El funcionario que incurriere en una violación a la presente política de seguridad, será notificado y sancionado formalmente como manda el reglamento de sanciones.

Durante la terminación del contrato

Objetivo:

El objetivo de este dominio es asegurar la correcta gestión de salida de los empleados o contratistas respecto de la seguridad de la información de la institución.

Controles:

1. Notificar al empleado saliente sobre las responsabilidades respecto del acuerdo de confidencialidad de la información firmado con la UCACUE.

2. El funcionario saliente deberá entregar formalmente todos los activos físicos a él asignados mediante actas

de entrega – recepción por parte del departamento administrativo de la UCACUE tales como: equipos de cómputo, dispositivos de almacenamiento de información, dispositivos móviles, tarjetas de acceso, tarjetas de crédito, entre otros.

3. El funcionario saliente deberá entregar formalmente todos los activos lógicos a él asignados mediante actas de entrega – recepción o de forma informal propios de su cargo o de sus actividades laborales tales como: licencias, códigos fuente, información propia de su actividad laboral, entre otros.

4. El departamento de talento humano deberá notificar a la dirección de TICs de la UCACUE, sobre el cese de las funciones o cambio de puesto del empleado para su inmediata cancelación o modificación de permisos y accesos a los respectivos sistemas como son: erpuniversity, códigos fuente, servidores, sistemas de colaborativos, repositorios digitales institucionales, correo electrónico institucional, sistemas operativos, red cableada, telefonía ip, acceso a la red inalámbrica institucional y eduroam, entre otros.

5.5.6.2. Seguridad ligada a la gestión de activos

Responsabilidad sobre los activos

Objetivo:

Identificar los activos de la organización y asignar roles y responsabilidades de uso y protección adecuada sobre estos.

Controles:

1. La dirección de TIC deberá elaborar inventario de activos de información de la UCACUE como:

    - Bases de datos.
    - Contratos con proveedores.
    - Acuerdos de confidencialidad de empleados y proveedores.
    - Documentación de los sistemas.
    - Licencias informáticas.
    - Manuales de usuario.
    - Registros de auditorías.
    - Información de evaluación institucional.
    - SLAs de proveedores.

- Planes de continuidad del negocio.
- Políticas de seguridad informática.
- Proyectos de investigación.

2. La dirección de TIC deberá elaborar inventario de activos de software de la UCACUE como:

- Software de gestión.
- Software de Aulas virtuales.
- Software de virtualización.
- Software de seguridad informática.
- Software de monitoreo y control.
- Software de Sistemas operativos.
- Software de soporte.
- Software de comunicación.
- Software de desarrollo.

3. La dirección de TIC deberá elaborar inventario de activos de servicios informáticos de la UCACUE como:

- Portales web.
- Servicios de mensajería electrónica.
- Servicios de video conferencia.
- Servicios de Autenticación centralizada.

- Servicios de mesa de ayuda.
- Servicios de soporte a usuarios.
- Servicios de backups de bases de datos.

4. El departamento administrativo de la UCACUE deberá elaborar y mantener un inventario de activos informáticos físicos, clasificados por tipo y por nivel de criticidad, este nivel de criticidad del activo deberá ser elaborado por la dirección de TIC basado en una metodología aceptada de análisis de criticidad de activos, entre estos activos están:

   - Servidores.
   - Storage.
   - Equipos de escritorio.
   - Equipos de networking.
   - Equipos de soluciones de redes inalámbricas.
   - Equipos de comunicaciones.
   - Equipos de seguridad informática.

5. El departamento de Talento Humano deberá elaborar un inventario de activos de capacidades del empleado de la UCACUE, tomando como características relevantes:

- Calificaciones de concursos de ingreso a la institución.
- Habilidades y experiencia en el uso y manejo de las TICs.
- Capacitaciones en temas relevantes a el desarrollo y manejo de la información en función de su área de trabajo.
- Actividades que realiza en la Institución en función de la criticidad de las mismas.
- Responsabilidades dentro del área de trabajo.
- Disponibilidad y flexibilidad en relación a su horario de trabajo.
- Si hay quien le reemplace en caso de ausencia.

6. Los activos mantenidos en el inventario deben tener un responsable asignado bajo los siguientes criterios:
   - La responsabilidad será asignada formalmente con un acta de entrega - recepción del activo.
   - El propietario será el responsable del uso adecuado y la protección del activo, a él, asignado.
   - El activo puede ser asignado a un proceso definido, a un proyecto, a una aplicación o a cualquier entidad

dentro de la organización que tenga uno o varios funcionarios responsables.

Clasificación de la información.

Objetivo:

Asegurar que la información sea clasificada de forma correcta con el fin de que reciba un nivel adecuado de protección de acuerdo a su grado de criticidad en la organización.

1. La información se deberá clasificar en función de los siguientes parámetros:
   - Requisitos legales
   - Importancia para la Institución.
   - Nivel de Criticidad
   - Susceptibilidad a divulgación
   - Susceptibilidad de modificación no autorizada.

2. El o los encargados de clasificar la información, será el o los dueños de este activo y en consecuencia será el o los responsables de la misma.

3. La información deberá ser etiquetada en función del grado de criticidad bajo las siguientes directrices:
    - Etiqueta blanca: Información pública
    - Etiqueta amarilla: Información privada con acceso a los funcionarios del área o departamento donde se genera o se necesita acceso a la información.
    - Etiqueta naranja: Información privada con accesos especiales asignados por el generador de la información.
    - Etiqueta roja: Información clasificada y que deberá ser resguardada en un lugar seguro cuya autorización de acceso a la misma, solo puede ser dada por el Consejo Universitario.

5.5.6.3. Política de control del acceso

Gestión de acceso de usuarios

Objetivo:

Definir la reglas y controles de acceso necesarios para determinar con claridad qué usuarios tendrán acceso a los diferentes servicios y sistemas, así como a las redes.

1. La dirección de TIC será la encargada de asignar los y revocar los accesos a todos los sistemas y servicios informáticos de la UCACUE en función de los siguientes parámetros:
    - Entrega y revocación de credenciales formalmente.
    - Revisión de que no existan inconsistencias o errores en el acuerdo de confidencialidad del empleado para con la Institución.
    - Asignación de accesos de a acuerdo al cargo y responsabilidad del usuario.
    - Generación de una identificación de usuario único, es decir, username y password por cada funcionario o usuario de sistema.
    - Capacitar al usuario en el uso y manejo del o los sistemas a los que tendrá acceso.
    - Notificar al usuario formalmente sobre sanciones a las que se atiene por violación de la política de seguridad.
    - Revocar los accesos y autorizaciones a los usuarios que hayan cambiado de cargo o en su defecto que ya no pertenezcan a la Institución.

- El departamento de TIC será el encargado de asignar los privilegios de acceso de los usuarios teniendo en cuento, por lo menos, las siguientes menciones:
- El privilegio de acceso dependerá estará asociado directamente con del cargo o la asignación de funciones que posea el usuario dentro de la Institución.
- No se asignará privilegios por petición verbal de ninguna persona por más importante que sea su cargo dentro de la Institución.
- Los privilegios para las personas que estén reemplazando a un usuario serán los mismos que las del usuario reemplazado, pero con diferentes credenciales de autenticación.
- Realizar auditoría de privilegios constante a los usuarios.

Responsabilidades del usuario

Objetivo:

Garantizar que los usuarios se hagan responsables de salvaguardar su información de autenticación.

1. Los usuarios de los sistemas deberán salvaguardar en lugar seguro las credenciales de acceso al sistema entregadas por el departamento de TIC.

2. Los usuarios deberán ingresar al sistema con especial precaución al ingresar sus credenciales de acceso al sistema con el fin de que sean reveladas a terceros.

Control de acceso a los sistemas y aplicaciones

Objetivo:

Restringir los accesos a los sistemas de información, que no estén formalmente autorizados por el responsable de esa información.

1. El usuario deberá ingresar sus credenciales en sistema siempre y cuando el certificado del sitio esté presente y activo.

2. El sistema exigirá al usuario a ingresar contraseñas que al menos cumplan con las siguientes características:
    - Deberá estar compuesta con al menos 8 caracteres.
    - Deberá contener caracteres alfanuméricos y al menos un símbolo especial.

- Deberá contener caracteres alfabéticos con al menos dos letras mayúsculas.
- No deberá contener en ella su nombre, apellido, fecha de nacimiento o algún tipo de información personal.
- No deberá ser igual a las últimas 3 contraseñas ingresadas.
- Tendrá una validez de acuerdo al rol del usuario:
  - Dos meses para roles críticos.
  - Seis meses para roles con algún nivel de criticidad.
  - Un año para roles no críticos.
- La contraseña deberá ser cambiada de inmediato si se sospechare de alguna anomalía o por divulgación a terceros y deberá ser comunicado al líder de área de desarrollo de manera formal.
- El sistema bloqueará al usuario al tercer intento infructuoso de ingreso al sistema y deberá solicitar formalmente la reactivación de sus credenciales.

3. Se prohíbe la instalación y uso de programas utilitarios que cualquier índole que no hayan sido formalmente autorizados por el líder del área.

4. El acceso a los códigos fuente del sistema será entregado formalmente por el líder del área al usuario dependiendo de su rol y competencia.

5.5.6.4. Política de cifrado

Objetivo:

Implementar los controles criptográficos necesarios para Garantizar la buena gestión de protección de la confidencialidad, disponibilidad e integridad de la información.

1. Es responsabilidad de la Dirección de TIC, desarrollar, implementar y hacer cumplir una política sobre la implementación de controles criptográficos cuya finalidad la protección de la información, esta política al menos debe contener las siguientes reglas:
    - Un responsable formal del análisis de necesidad de controles criptográficos en los respectivos medios de acceso, manipulación y transporte de la información.

- Un responsable de la creación e implementación de claves criptográficas para los diferentes sitios y medios de transporte de la información cuyo algoritmo deberá tener en cuenta los siguientes aspectos:
  - Criticidad del sitio web.
  - Frecuencia de acceso al sitio web.
  - Criticidad de la información.
  - Frecuencia de acceso a la información.
  - Medio de transporte de la información.
  - Acceso remoto a través de VPN.

5.5.6.5. Política de seguridad física y del entorno

Objetivo:

Evitar los accesos sin autorización, los daños e interferencia a la información de la institución y a los recursos de tratamiento de la información.

1. Perímetro de seguridad: La dirección de TIC definirán perímetros de seguridad de acceso a usuarios y con el propósito de limitar el acceso a críticas que manejen información de gran valor o confidencial.

2. Controles de acceso físicos: El acceso físico a la infraestructura que contenga servicios o información crítica de la Institución deberá ser restringido de acuerdo a los siguientes parámetros:
    - El único autorizado de acceso a la infraestructura será el responsable del área de infraestructura y redes de la Institución.
    - Se establecerá un área de admisión, en donde se gestione eficientemente el acceso físico a los lugares críticos de la Institución.
    - Se llevará una bitácora que registre la fecha y hora de entrada y salida de visitantes.
    - El respectivo acceso a los visitantes, será aprobado previamente; y se les asignará un carnet o distintivo el cual se les retirará cuando ya haya cumplido con el propósito de la visita.
    - El acceso a los cuartos de equipos como servidores y telecomunicaciones deberá será través de algún medio seguro como tarjetas electrónicas, sistemas de control biométrico, etc.
    - Los derechos de acceso a las áreas le serán retirados inmediatamente posterior al retiro de las

funciones o cambio de cargo del empleado en la empresa.

5.5.6.6. Política de seguridad de los equipos

Objetivo:

El objetivo es evitar el daño, pérdida, robo que puedan terminar con la interrupción de las operaciones o servicios de la institución.

1. Ubicación y protección de los equipos: Los equipos deberán cumplir con los siguientes parámetros de seguridad:
    - Los equipos deberán estar ubicados de forma que se evite que estén comprometidos a amenazas tales como: robo, tropezones, fallas en suministros de agua o energía, polvo, calor, humedad, entre otros.
    - Los equipos que posean o manejen información crítica de la Institución se ubicarán en zonas de acceso restringido.

2. Servicios de suministro:
    - Los equipos deberán estar protegidos con un correcto sistema eléctrico, como por ejemplo energía

regulada, instalaciones de para rayos, puestas a tierra, balanceos de cargas, etc.

- Los equipos deberán estar protegidos por sistemas de backups de energía eléctrica como generadores eléctricos y UPS.
- El cableado estructurado de datos y eléctrico deberá cumplir con los estándares que manda la norma UNE-EN 50174-2.

3. Mantenimiento de los equipos: Los equipos se deberán recibir mantenimiento preventivo y correctivo de acuerdo a los siguientes parámetros:
    - Solo el área de soporte e infraestructura de la Institución será la única autorizada a realizar el mantenimiento de los equipos.
    - La solicitud de mantenimiento correctiva de los equipos deberá ser registrada únicamente a través de las siguientes vías:
        - A través del sistema de soporte de incidencias tecnológicas https://soporte.ucacue.edu.ec
        - A través de correo electrónico a la dirección soportetic@ucacue.edu.ec

  - A través de solicitud escrita dirigida a la dirección de TIC.
- El área de soporte llevará una bitácora de los incidentes e historial de los equipos atendidos.
- Todas las dependencias de la Universidad contarán con ingenieros de soporte de planta para el soporte de primer nivel.
- El personal de soporte de primer nivel deberá generar informes anuales sobre el mantenimiento preventivo y correctivo realizado en los equipos que posee a su cargo y remitirlos a la dirección de TIC.

5.5.6.7. Política de seguridad en la operativa

Objetivo:

Asegurar el funcionamiento correcto y seguro de las instalaciones de tratamiento de la información.

1. Procedimientos de operación de documentos: En función de las actividades o el rol asignado a un funcionario, se deberá definir y detallar documentadamente los siguientes procedimientos:
   - Procesamiento y manejo de la información.

- Procedimiento y periodicidad de copias de respaldo.
- Procedimiento documentado de uso y manejo del sistema en relación con la asignación de funciones.
- Procedimiento documentado de manejo de errores y notificación de vulnerabilidades y amenazas.
- Documento con niveles de soporte y datos de personal técnico en el área.

2. Gestión de cambios: Los cambios serán gestionados que se produzcan en los procesos de negocio, organizativos, desarrollo y testeo incluyendo la planificación y comunicación con las personas directamente afectadas por los cambios.

3. Gestión de capacidades:
   - El líder de área de desarrollo notificará formalmente al área de infraestructura la proyección de crecimiento en capacidades de procesamiento, memoria y almacenamiento en los servidores cada inicio de año.
   - El líder del área de infraestructura se encargará de gestionar y documentar la implementación de las capacidades proyectadas por el área de desarrollo

en los servidores, previa notificación de mantenimiento planificado.

- Los mantenimientos de cambio programados por el área de infraestructura, deberán calendarizarse para fechas y horas que presenten el menor impacto en los servicios afectados.

4. Separación de los ambientes de desarrollo, pruebas, y operación:
    - Con el propósito de evitar problemas de indisponibilidad o fallos en los servicios, el proceso de desarrollo y actualización de soluciones informáticas estará compuesto por tres ambientes: desarrollo, certificación y producción de soluciones informáticas.
    - El ambiente de desarrollo no deberá contener los datos reales ni actuales manejados en el ambiente de producción, salvo en casos excepcionales que el proceso lo amerite.
    - El ambiente de certificación es el más importante y es aquí que se aplicarán métodos de auditoría de errores y de código malicioso para evitar riesgos o

brechas de seguridad en los sistemas en producción, además en este ambiente se podrá usar datos actualizados del sistema.

- Con el fin de garantizar la integridad, confidencialidad y disponibilidad de la información y los sistemas, el ambiente de producción se encontrará en servidores seguros con SLAs acuerdo a las características del servicio.
- El código fuente no será estará presente en el servidor de ambiente de producción sino en algún lugar remoto con los respectivos controles de seguridad en cuanto a accesos indebidos se refiere.

5. Protección contra código malicioso con el propósito de evitar la propagación de código malicioso que conlleve a problemas de disponibilidad, integridad confidencialidad de la información se deberán cumplir con los siguientes parámetros:
    - La Institución adquirirá una solución contra software malicioso que cubrirá la totalidad de los equipos de cómputo de la Universidad.

- El área de Infraestructura y soporte será la única autorizada para la instalación, desinstalación y monitoreo de la solución antivirus.
- La dirección de TIC capacitará periódicamente a los usuarios finales sobre el correcto tratamiento de la información con el propósito de que éstos, sepan identificar posibles amenazas informáticas.
- Queda terminantemente prohibido la utilización de software no autorizado o licenciado con el aval de la dirección de TIC.
- Los dispositivos de almacenamiento móvil deberán ser analizados por la solución antivirus instalada en la estación de trabajo previo a su utilización.
- El responsable del monitoreo de la solución antivirus deberá notificar formalmente a los técnicos si encontrase algún problema en algún sistema o equipo con el fin de que sea mitigado de inmediato.
- Los servicios que se contraten con alojamiento externo, deberán documentar en su contratación los parámetros sobre seguridad de la información de forma clara y específica.

- Se realizarán auditorías de seguridad periódicas para con el fin de revisar la integridad y efectividad de las soluciones de seguridad.

6. Copias de seguridad:
    - La Dirección de TIC contratará almacenamiento para backups de copias de seguridad en algún proveedor remoto como por ejemplo S3 de Amazon.
    - El área de infraestructura se encargará de realizar y mantener en repositorios con características de disponibilidad, integridad y confidencialidad adecuadas, las copias de seguridad de los sistemas de la Institución.
    - Para el sistema erpuniversity alojado en los servidores de CEDIA:
        - El proveedor hará una copia diaria de todo el servidor virtual con un almacenamiento de por lo menos un mes.
        - El área de infraestructura realizará una copia de seguridad remota de la base de datos de producción diaria en horario que no afecte el performance del mismo y la almacenará en la

infraestructura de la Universidad durante al menos los tres últimos meses.

- La última copia de seguridad será enviada al repositorio remoto contratado por la Universidad.
- Con el propósito de probar la integridad del respaldo alojado remotamente, este será descargado diariamente y puesto a prueba en un servidor virtual en el datacenter de la UCACUE.

- La Universidad adquirirá y mantendrá software o herramientas de backups de máquinas virtuales con el propósito de proteger los servicios que se despliegan desde el datacenter local.

7. Registros de actividad y supervisión:
   - El área de desarrollo y actualización de soluciones tecnológicas se encargará de implementar controles en el desarrollo que permitan registrar todos los eventos más relevantes dependiendo de la criticidad del sistema podría ser necesario registrar todos los eventos para futuros análisis o auditorías.

5.5.6.8. Política de seguridad en las telecomunicaciones

Objetivo:

El objetivo es establecer los controles necesarios para proteger las comunicaciones externas desde y hacia la UCACUE como las comunicaciones internas o sea las de la intranet.

1. Controles de red:
    - El área de infraestructura y redes y soporte será la responsable de la gestión de las redes y soporte en comunicaciones internas, será la única área autorizada a realizar cambios, en esquemas, topologías o asignación de direccionamiento ip privado o público.
    - La dirección de TIC será autorizará el acceso físico o remoto a los servicios tecnológicos dentro y fuera de la Institución.
    - El área de Infraestructura generará y actualizará las topologías de redes de toda la Universidad, Sedes y Extensiones.

2. Seguridad en los servicios de red:
    - El área de infraestructura monitoreará los servicios contratados con proveedores con el propósito de asegurar el cumplimiento del contrato, y si se presentara cualquier evento, este deberá ser notificado formalmente al proveedor y con copia al representante del área o Unidad Académica afectada.

5.5.6.9. Política de desarrollo y mantenimiento de sistemas de información.

Objetivo:

El objetivo es como incorporar controles de seguridad durante la adquisición de aplicaciones o sistemas de información, así como agregar una capa de seguridad durante todo su ciclo de vida en el caso de desarrollos propio y contratados.

1. Requisitos de seguridad de los sistemas de información:
    - Las adquisiciones de software nuevo, desarrollos nuevos y actualizaciones de sistemas internos de la

Universidad, se someterán a los controles de la presente política.

- Las contrataciones con desarrollos de terceros, deberán someterse, formalmente, a la presente política de seguridad y deberán firmar un acuerdo para este efecto con la Universidad.

2. Aseguramiento del proceso de desarrollo y soporte
    - Control de desarrollo seguro de aplicaciones: Los nuevos desarrollos propios o contratados, así como las actualizaciones de los sistemas, deberán cumplir con los siguientes controles de seguridad:
        - Validación de datos de entrada: Desde la etapa de diseño se implementarán controles con el propósito de validar los datos y requisitos ingresados; para este efecto deberán considerarse los siguientes controles:
            - Controles de orden y codificación por cada desarrollo.
            - Controles de acceso por el rol del usuario.

- Controles de los valores posibles que previamente deberán ser validados de acuerdo los requerimientos del sistema.
- Controles de autorización de accesos, para este fin se dispone que la única persona que podrá autorizar el acceso y los niveles del mismo, será el líder del área de desarrollo.

- Integridad de mensajes: Las aplicaciones o sistemas que se diseñen para enviar mensajes que incluyan información personal, privada o con ciertos niveles de criticidad, para cumplir con los criterios de la Integridad, Disponibilidad y Confidencialidad, deberán someterse a los controles especificados en la presente política en la sección de “Controles Criptográficos”.
- Validación de datos de salida: Se exigirá formalmente a los desarrolladores internos o externos, la validación de los datos de salida con el propósito de garantizar el correcto funcionamiento y ejecución de la aplicación o sistema, los datos de salida deberán estar de acuerdo con los requerimientos funcionales

estimados en el inicio de cada proyecto de desarrollo, actualización o mantenimiento de sistemas de información.

- Administración de claves: Todas las claves serán protegidas contra copia, modificación, destrucción y divulgación no autorizadas a través de algún método de almacenamiento cifrado en las bases de datos.

3. Protección de los datos de prueba: Las pruebas de los sistemas, serán realizadas con datos extraídos del ambiente productivo de los sistemas. Para su protección se deberán cumplir con los siguientes controles:
   - El líder del área de desarrollo será quien, formalmente, autorizará el despliegue una copia de la base de datos de producción en el ambiente de pruebas.
   - El líder del área de producción designará, formalmente, una persona responsable de la extracción y despliegue de la base de datos de producción en el ambiente de pruebas.

- La base de datos de producción podrá estar presente durante el tiempo que dure la fase de pruebas.
- Cuando la fase de pruebas haya concluido a satisfacción, la base de datos utilizada (copia de la base de datos de producción) deberá ser eliminada inmediata y formalmente del ambiente de pruebas.

4. Control de acceso a los códigos fuente: Con el propósito de controlar riesgos relacionados a los códigos fuentes, se deberá cumplir con los siguientes controles:
   - El líder del área de desarrollo será el responsable de la custodia y autorización a los códigos fuentes de los sistemas de información.
   - El líder del área de desarrollo entregará el acceso, formalmente, de los sistemas de información a los desarrolladores.
   - Todos los códigos fuentes de los sistemas de información serán registrados mediante un método formal usando una codificación que contendrá los siguientes campos: nombre de programa, numeración de versión, fecha de última modificación,

hora de última compilación, estado (En desarrollo, en certificación o en producción).

- El líder del área solicitará formalmente la elaboración de copias de seguridad de los códigos fuentes al área de infraestructura.
- El líder del área de desarrollo designará formalmente un delegado para la revisión de los respaldos de los sistemas, el cual se encargará de poner a prueba y validar la integridad y funcionalidad de los respaldos.

5. Procedimiento de control de cambios: Con el propósito de minimizar los riesgos de modificación no autorizada de los sistemas de información, se contemplarán los siguientes controles durante el proceso de realización de cambios:
    - Toda solicitud de cambio será regida al proceso establecido por la dirección de TIC.
    - La solicitud de cambio será procesada solo si ha sido solicitado a través de un mecanismo formal.
    - Previa aceptación del cambio se deberá verificar que la solicitud no se contraponga a la presente política en ninguno de sus controles.

- Todo cambio será registrado formalmente e implementado manteniendo un control de versiones.

6. Restricciones en los cambios de los sistemas de información entregados por terceros: Si surgiere la necesidad de la modificación o personalización del código fuente suministrados por proveedores, se deberán regir a los siguientes controles:
   - Se revisarán los términos y condiciones de la contratación de desarrollo o adquisición del sistema con el fin de determinar si la modificación está contemplada en el contrato.
   - El único responsable de la autorización del cambio en los sistemas contratados a proveedores será el Director de TIC.
   - El cambio se podrá realizar si y solo si, no se contrapone con ninguna de los controles de la presente política.
   - El cambio se deberá efectuar llevando un control de versiones formal.

7. Desarrollo externo de sistemas de información: El desarrollo contratado con proveedores deberá estar sometido a los siguientes controles:
    - Se contratará anexando los acuerdos de propiedad intelectual, garantías, licencias, calidad y propiedad del código fuente y confidencialidad.
    - El área de desarrollo en conjunto con el o las áreas solicitantes serán quienes determinen los requisitos y términos de referencia de la contratación.
    - El líder del área de desarrollo determinará una comisión que podrá ser interna o contratada para auditar el sistema, previo a la puesta en producción con el objetivo de verificar que el código cumpla con los requerimientos de: seguridad de los sistemas establecidos en la presente política, la calidad del código, uso de buenas prácticas de desarrollo, estabilidad del sistema, y otros que puedan surgir por tipo de desarrollo.

5.5.6.10. Política de gestión de incidentes de seguridad de la información

Objetivo:

El objetivo del presente dominio entregar un sistema formal de notificación de eventos de seguridad, con el propósito de que se pueda brindar un tratamiento coherente, eficaz y oportuno.

1. Responsabilidades y procedimientos:
    - Es responsabilidad de todos los funcionarios Todos los funcionarios internos o contratistas, son responsables de reportar eventos y debilidades de seguridad de la información que se hayan detectado de manera formal dirigido a la Dirección de TIC, o a través del centro de soporte de incidentes tecnológicos (https://soporte.ucacue.edu.ec).
    - Es responsabilidad de la Dirección de TIC el capacitar constantemente a todos los funcionarios, contratistas y todos quienes formen parte del tratamiento de la información, el enfoque de las capacitaciones debe estar dirigido hacia reconocer y

reportar un incidente y vulnerabilidades en el tratamiento de la información.

2. Evaluación de los eventos e incidentes de la seguridad de la información: Es necesario identificar y evaluar los eventos de seguridad de la información tomando en cuenta los siguientes parámetros:

   - Acceso no autorizado a la información.
   - Divulgación de información sensible.
   - Denegación de servicio.
   - Ataques externos o internos.
   - Ataques dirigidos y al azar.
   - Pérdida o robo de la información.
   - Modificación no autorizada.
   - Información no actualizada.
   - Uso indebido de software.
   - Uso indebido de credenciales de usuario.
   - Suplantación de identidad.
   - Ataques de ingeniería social.

   De la misma manera deberá hacer el análisis de los siguientes parámetros:

   - Daño potencial de recursos a causa del incidente.

- Necesidad de preservación de la evidencia.
- Tiempo y recursos necesarios para poner en práctica la estrategia.
- Efectividad de la estrategia.
- Duración de las medidas a tomar.
- Criticidad de los sistemas afectados.
- Características de los posibles atacantes.
- Si el incidente es de conocimiento público.
- Pérdida económica.
- Posibles implicaciones Legales.

3. Respuesta a los incidentes de seguridad: El designada por la Dirección de TIC, encargada de gestionar los incidentes de seguridad, deberán tener en cuenta los siguientes factores para mitigación:
   - Tiempo y Recursos necesarios para poner en práctica la estrategia de recuperación.
   - Análisis de la efectividad esperada de la Estrategia planteada.
   - Posibles implicaciones legales.
   - Relación costo-beneficio de la estrategia.
   - Relación y análisis con experiencias anteriores.

- Identificación de los Procedimientos de cada sistema comprometido.
- Identificación de usuarios o servicios comprometidos para aplicar la estrategia de mitigación.

4. Aprendizaje Obtenido de los incidentes de seguridad: El área designada por la dirección de TIC encargada de la seguridad de la información garantizará el correcto manejo a la información obtenida de los incidentes de seguridad que haya sufrido la institución, y registrarla en una base de conocimientos que a la postre será una base de datos donde estará alojadas los tipos de incidentes de seguridad, así como las soluciones a los mismos.

CAPÍTULO 6

PLAN DE IMPLEMENTACIÓN DE LA POLÍTICA DE SEGURIDAD

6.1 ACTIVIDADES DEL PLAN DE IMPLEMENTACIÓN

Se han determinado las siguientes actividades específicas para el plan de implementación de la política de seguridad:

FIGURA 6. 1 Actividades del Plan de Implementación del SGSI.

6.2 CRONOGRAMA DE GENERACIÓN E IMPLEMENTACIÓN DEL SGSI

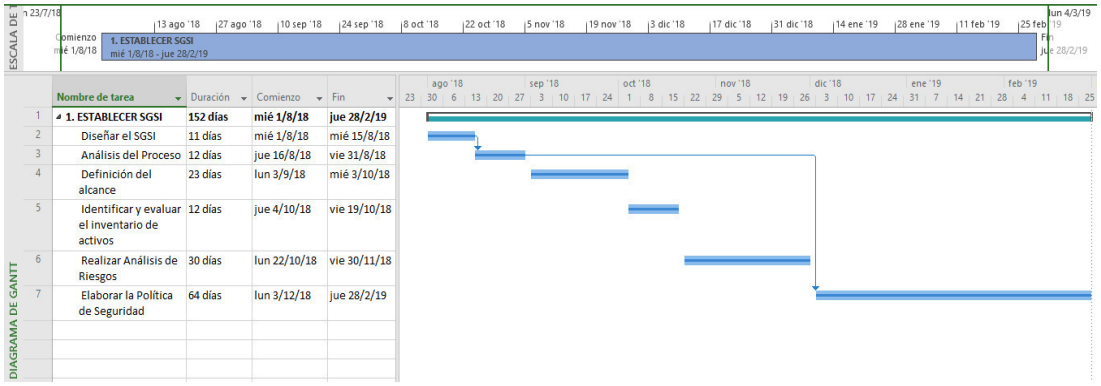

FIGURA 6. 2 Cronograma Actividad Establecer SGSI.

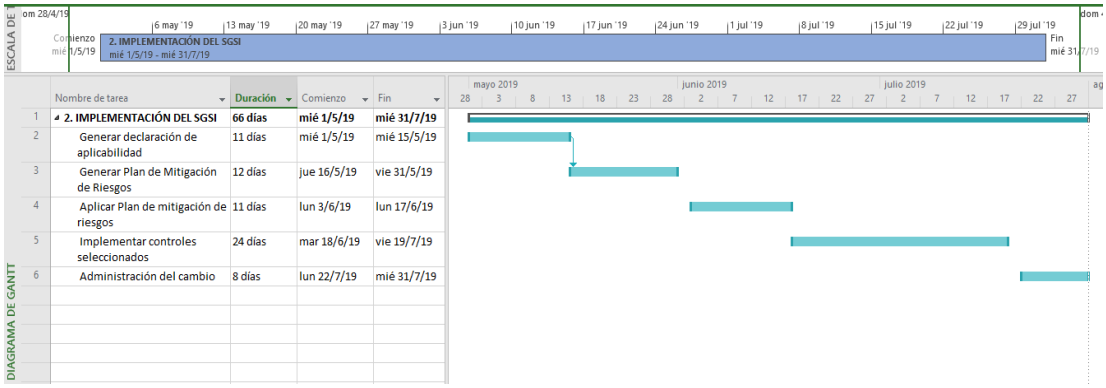

FIGURA 6. 3 Cronograma Implementación del SGSI.

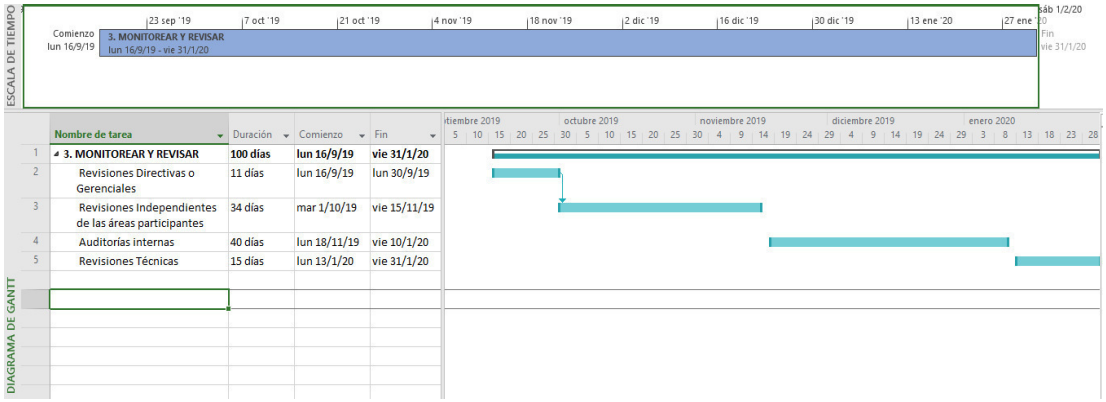

FIGURA 6. 4 Cronograma - Monitorear y Revisar.

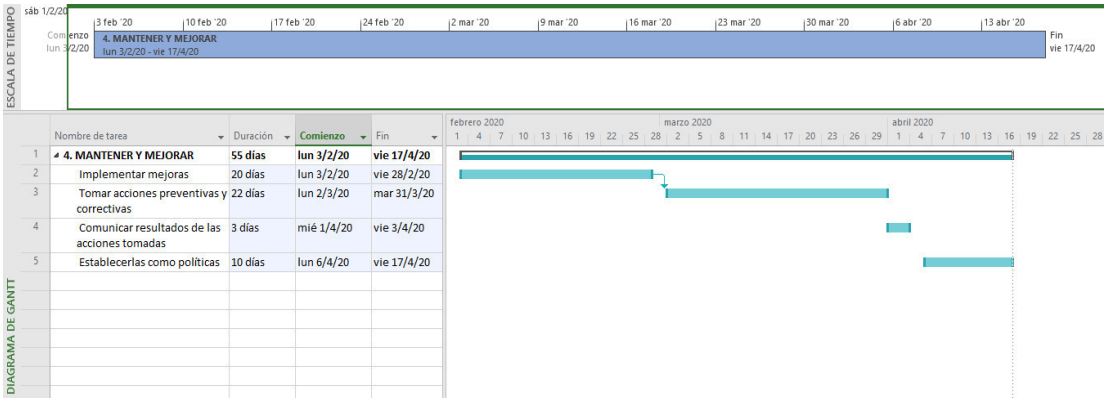

FIGURA 6. 5 Cronograma – Mantener y Mejorar.

6.3 PLAN DE IMPLEMENTACIÓN DEL SGSI

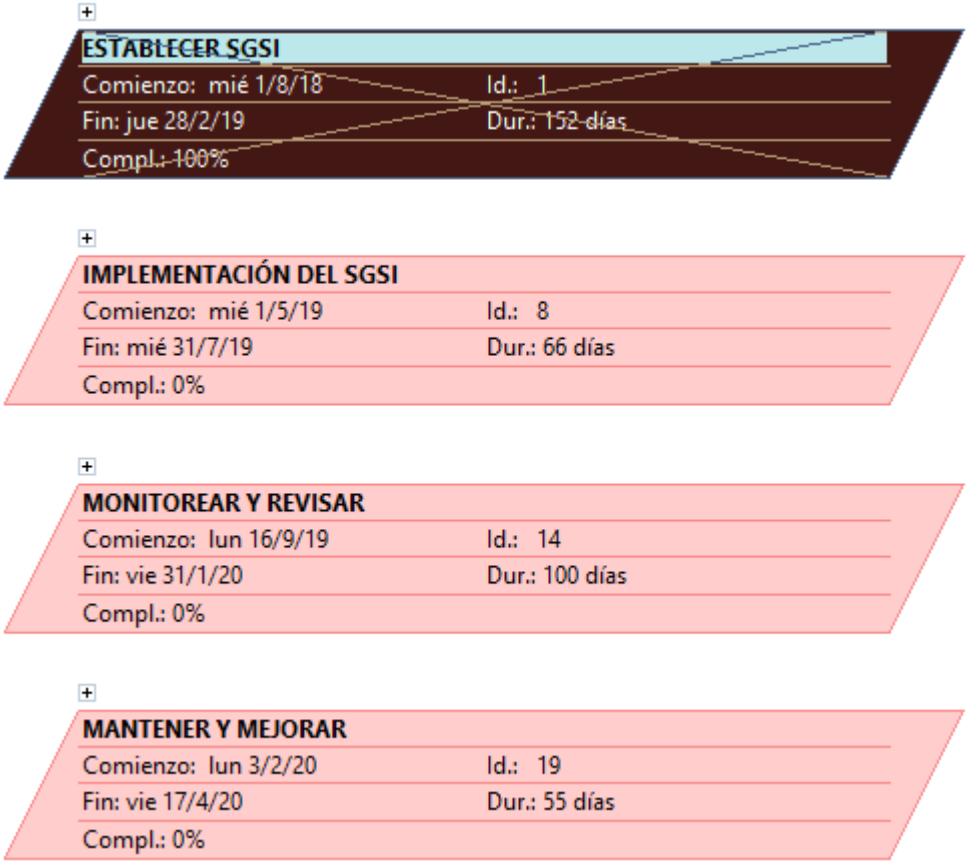

FIGURA 6. 6 Plan de Implementación.

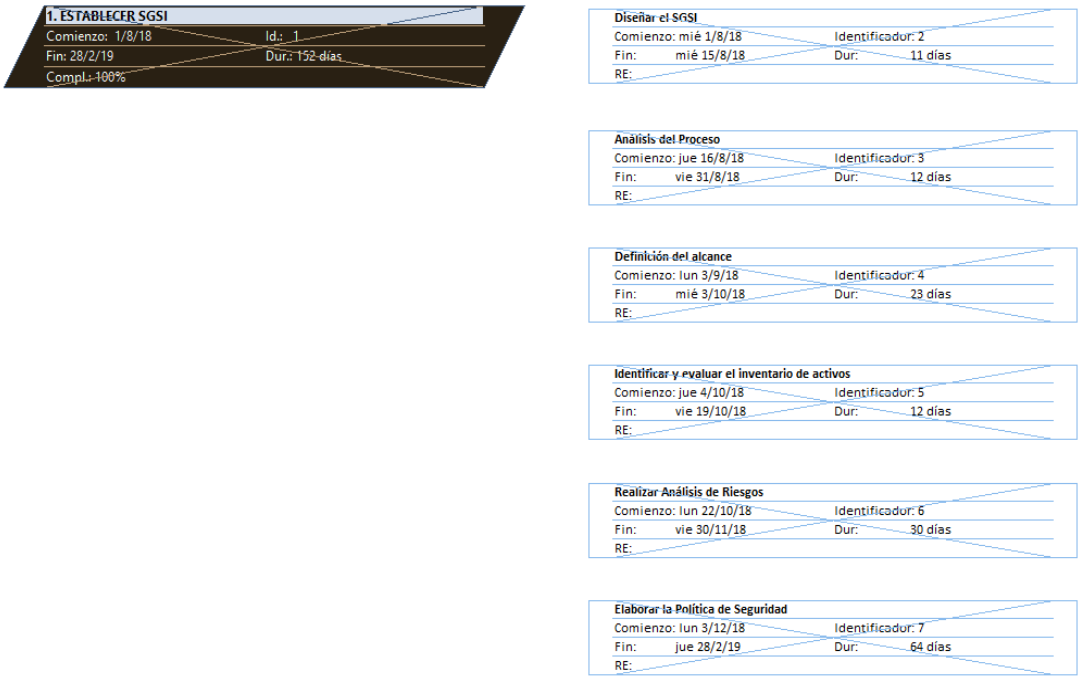

FIGURA 6. 7 Subtareas del proceso Establecer SGSI.

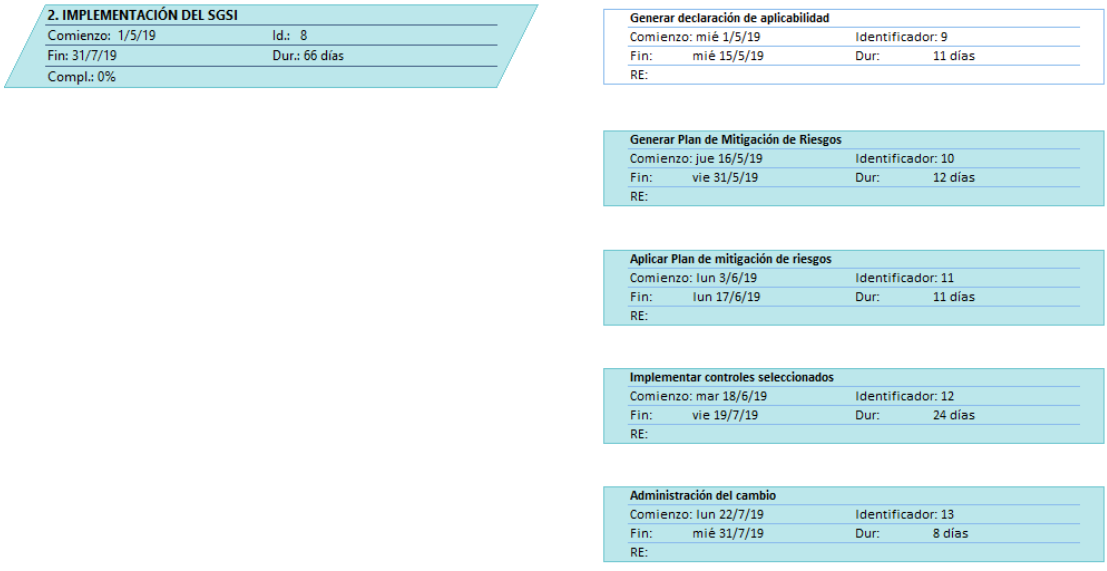

FIGURA 6. 8 Subtareas del proceso Implementación del SGSI.

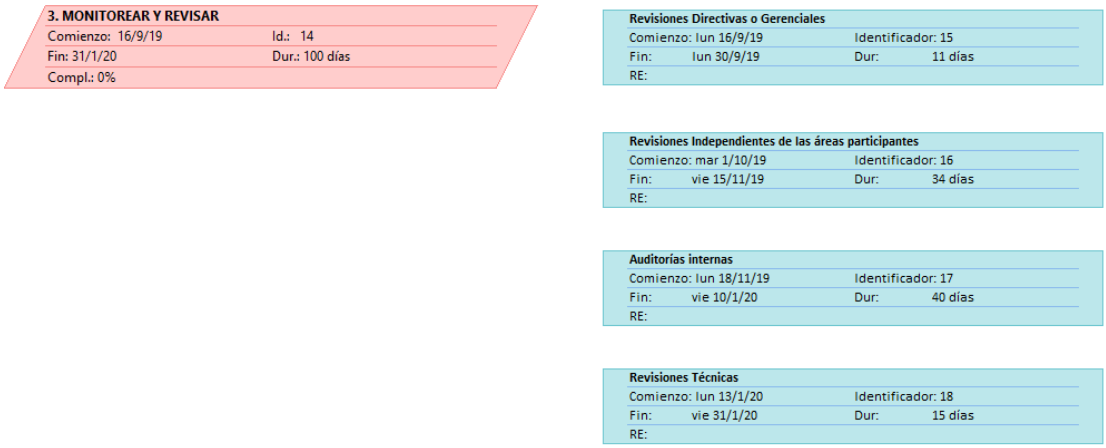

FIGURA 6. 9 Subtareas del proceso Monitorear y Revisar.

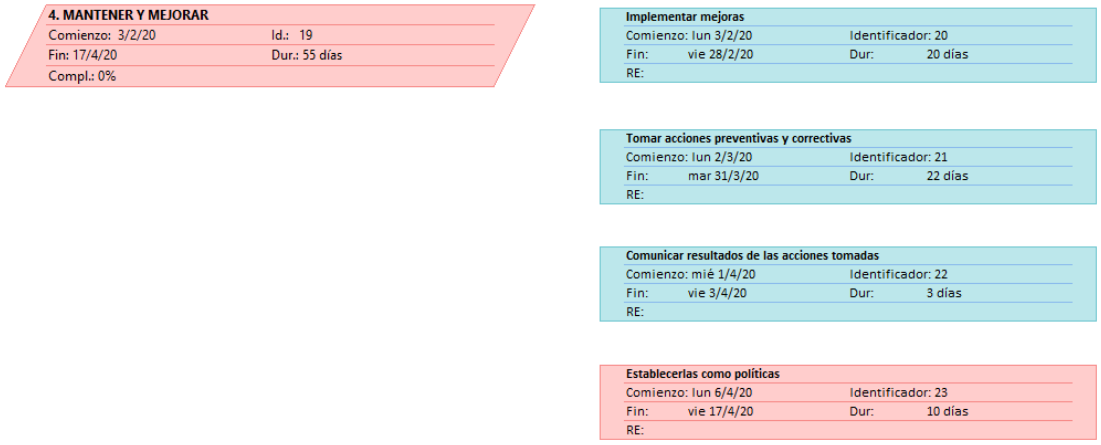

FIGURA 6. 10 Subtareas del proceso Mantener y Mejorar.

6.4 IMPACTO ESPERADO DEL PROYECTO

Tabla 12 Impacto esperado después de la implementación del SGSI. Fuente: Autor

No. Dominio	DOMINIO DE LA NORMA	Cumplimiento Actual	Cumplimiento Esperado
5	Políticas de seguridad.	15%	100%
6	Aspectos organizativos de la seguridad de la información.	36%	75%
7	Seguridad ligada a los recursos humanos.	20%	95%
8	Gestión de activos.	44%	85%
9	Control de accesos.	35%	90%
10	Cifrado.	20%	85%
11	Seguridad física y ambiental.	24%	70%
12	Seguridad en la operativa.	36%	95%
13	Seguridad en las telecomunicaciones.	23%	85%
14	Adquisición, desarrollo y mantenimiento de los sistemas de información.	25%	95%
15	Relaciones con suministradores.	NO APLICA	NO APLICA

No. Dominio	DOMINIO DE LA NORMA	Cumplimiento Actual	Cumplimiento Esperado
16	Gestión de incidentes en la seguridad de la información.	23%	95%
17	Aspectos de seguridad de la informacion en la gestión de la continuidad del negocio.	25%	85%
18	Cumplimiento.	15%	90%

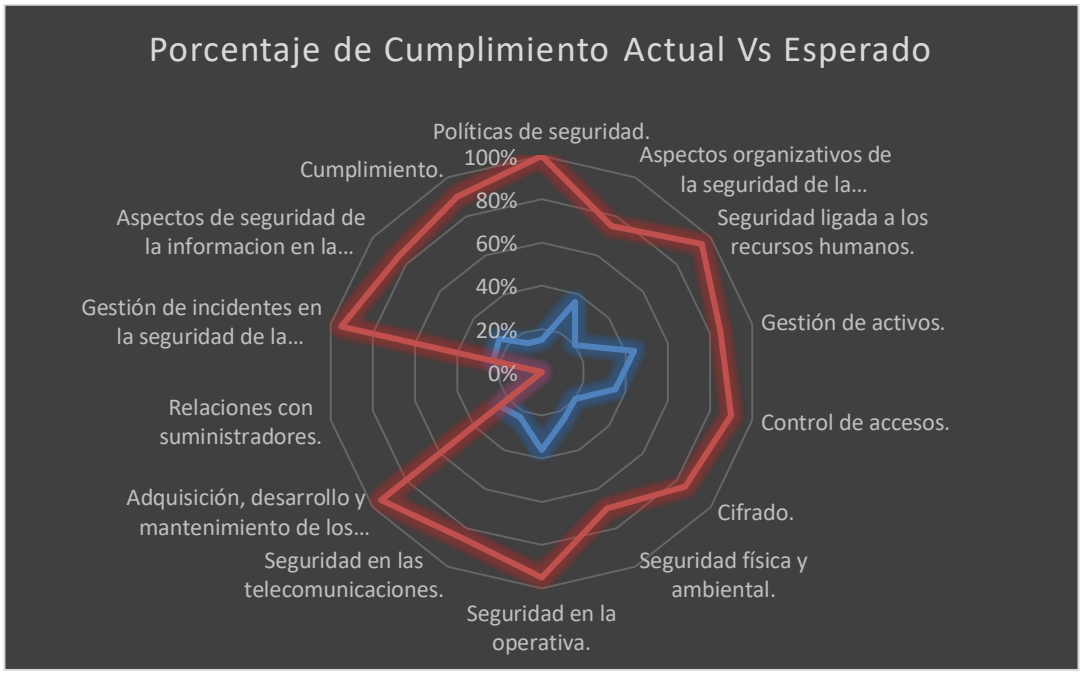

FIGURA 6. 11 Mapa de calor de Situación Actual Vs Cumplimiento esperado.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. Como parte del presente proyecto, los activos de información relacionados con el proceso de actualización y desarrollo de soluciones informáticas y gestión de bases de datos, fueron identificados y clasificados en función de su nivel de criticidad, pues, antes del mismo, solo existía un inventario de los activos físicos.

2. Se realizó la identificación de las amenazas potenciales, así como las vulnerabilidades y por consecuencia el análisis de los riesgos informáticos a los que están sometidos los activos más críticos de información,

relacionados con el proceso de desarrollo y actualización de soluciones informáticas y gestión de bases de datos.

3. Para la mitigación de los riesgos a los que se encuentran expuestos los activos de información relacionados con el proceso de desarrollo y actualización de soluciones informáticas y gestión de bases de datos, se diseñó un esquema de seguridad basado en la aplicación de los controles de la norma IEC/ISO 27002.

4. En el presente proyecto, se diseñó además, un plan de implementación del esquema de seguridad con su respectivo cronograma, el mismo que está basado en 4 etapas: Establecer el SGSI, Implementar el SGSI, Monitoreo y Revisión del SGSI y por último el Mantenimiento y Mejoramiento del SGSI; de la misma forma se hizo un análisis del impacto que se pretende obtener con la implementación del presente esquema de seguridad al proceso de desarrollo y actualización de soluciones informáticas y gestión de bases de datos.

RECOMENDACIONES

1. Implementar la política de seguridad de la información que en este documento se sugiere para una de las áreas más críticas, como es la de desarrollo y actualización de soluciones informáticas y gestión de base de datos, y hacer respetar los controles en ella expuestos, normando bajo una reglamentación jurídica las faltas a la misma.

2. Definir una comisión que podría ser temporal, pero de preferencia debería ser permanente para la clasificación e inventariado de los activos físicos y lógicos de información, asignando niveles de criticidad a cada activo.

3. Capacitar a todos los funcionarios en relación a sus roles sobre el uso correcto de los sistemas, manejo de claves, manipulación de equipos de cómputo, acceso a la información en la nube, apertura de correos electrónicos, uso de soluciones antivirus, entre otros, basado en buenas prácticas de seguridad de la información, así como de mecanismos formales de notificación de eventos de seguridad de información.

4. Solicitar a la Alta Dirección de la Universidad, el involucramiento directo en los aspectos relacionados con la seguridad de la información, mediante la creación de un área o departamento específico para este propósito, la cual dependa y reporte directamente a rectorado.

BIBLIOGRAFÍA

[1] Almoguera, P. , *ABC.es ,* http://www.abc.es/20120328/espana/abci-detenidos-universitarios-hackers-201203281634.html , 2012.

[2] Araya, J. , *Semanario Universidad ,* https://semanariouniversidad.com/pais/universidad-y-otros-medios-vctimas-de-ataques-informticos/ , 2014

[3] Cano, J. J. , Inseguridad Informática: Un concepto dual en seguridad informática , *Revista de Ingeniería - Universidad de los Andes* , 2004.

[4] International Telecommunication Union , *Global Cybersecurity Index 2017,* Ginebra: ITU-D , 2017.

[5] ISO/IEC. , *Estándar Internacional ISO /IEC 17799 ,* https://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf , 2005.

[6] JHUÉZ, J. , *METODOLOGÍAS PARA LA GESTIÓN DE RIESGOS ,* https://capacitacioncgr.jovenclub.cu/wp-content/uploads/2018/05/Metodologia-para-la-Gestion-del-Riesgo.pdf , 2015.

[7] López, P. A. , *Seguridad Informática ,* Editex , 2010.

[8] Medina, F. , *El comercio.com* , http://www.elcomercio.com/actualidad/bandas-hackers-titulos-licencias-falsas.html , 18 de 1 de 2016.

[9] NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE FORT GEORGE G MEADE MD. , *National Information Systems Security (INFOSEC) Glossary* , https://apps.dtic.mil/docs/citations/ADA433929 , 2000.

[10] Obando, V. , *El Espectador* , http://www.elespectador.com/noticias/judicial/universidades-victimas-de-hackers-articulo-560884 , 2015.

[11] Sánchez, L. E. , *future.inese.es ,* http://future.inese.es/la-informacion-es-el-activo-mas-valioso-para-muchas-empresas-sin-embargo-no-la-tienen-asegurada/ , 2013.

[12] Silva Coehlo, F. E., Segadas de Araujo, L. G., & Kowask Bezerra, E. , *Gestión de la Seguridad de la Información.* Bogotá: Fundación CEDIA , 2014.

[13] Universidad Católica de Cuenca , https://www.ucacue.edu.ec/la-universidad/mision-y-vision/ , fecha de consulta octubre de 2018.

[14] Mesquida, A. L. , Sistema de Gestión Integrado según las normas ISO 9001, ISO/IEC 20000 e ISO/IEC 27001 , *Revista Española de Innovación, Calidad e Ingeniería del Software*, 28 Ed, 2010

[15] Disterer, G. , *ISO/IEC 27000, 27001 and 27002 for Information ,* http://dx.doi.org/10.4236/jis.2013.42011 , Journal of Information Security. Vol 4 , 2013

[16] Pineda, J. , Informe de resultados de la “1° encuesta de seguridad de la información en universidades ecuatorianas miembros de CEDIA” , https://csirt.cedia.org.ec/wp-content/uploads/2014/05/Informe-de-Resultados-2014.pdf, 2014