INSTITUTO TECNOLÓGICO SUPERIOR

SUDAMERICANO

QUITO - ECUADOR

ESCUELA DE

SISTEMAS DE AUTOMATIZACIÓN

PROYECTO DE TITULACIÓN

TEMA:

Seguridad informática aplicada al Instituto Tecnológico Superior Sudamericano Quito

AUTOR: *Tulcanazo Valencia José Luis*

TUTOR: *MSc. ALDRIN MARCEL ESPÍN LEÓN*

San Francisco de Quito, Julio del 2018

AUTORÍA

Yo, Tulcanazo Valencia José Luis, portador de la cédula de ciudadanía No.172703181-5, declaro bajo juramento que el trabajo aquí descrito, es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional y que he consultado e investigado en base a las referencias bibliográficas que se incluyen en este documento. Esta investigación no contiene plagio alguno y es resultado de un trabajo serio desarrollado en su totalidad por mi persona.

_____

Tulcanazo Valencia José Luis

CERTIFICACIÓN

Una vez que se ha culminado la elaboración del Proyecto de Titulación cuyo tema es: **SEGURIDAD INFORMÁTICA APLICADA AL INSTITUTO TECNOLÓGICO SUPERIOR SUDAMERICANO QUITO**, certifico que el mismo se encuentra habilitado para su defensa pública.

_____

Msc. Fabrizio Vicente Villasís Chiriboga
Coordinador de la Escuela de Sistemas
de Automatización
Instituto Tecnológico Superior Sudamericano Quito

CERTIFICACIÓN

Por medio del presente certifico que el señor TULCANAZO VALENCIA JOSÉ LUIS, ha realizado y concluido su trabajo de titulación, cuyo tema es: **SEGURIDAD INFORMÁTICA APLICADA AL INSTITUTO TECNOLÓGICO SUPERIOR SUDAMERICANO QUITO**, para obtener el título de Tecnólogo en SISTEMAS DE AUTOMATIZACIÓN, bajo mi tutoría.

MSc. Aldrin Marcel Espín León
Director del Proyecto de Titulación

AGRADECIMIENTOS

Agradezco a Dios porque me dió el regalo más grande de mi vida que son mis padres, y gracias al amor, al apoyo y las bendiciones de ellos puedo cumplir este sueño profesional.

A mis hermanas, quienes son un ejemplo de lucha y fé para lograr las metas y éxitos en mi vida, porque además de ser mis hermanas son mis amigas y consejeras.

A mis compañeros y amigos, quienes hicieron de estos años una experiencia memorable, por sus consejos, lecciones, sabiduría, conversaciones y momentos compartidos.

A mi tutor MSc. Aldrin Espín, quien desde el primer momento que le solicité su guía no dudó en apoyarme, por ser mentor y contribuir con sus conocimientos, sugerencias y guía para la realización de este trabajo y terminar mis estudios con éxito.

A mis profesores quienes forman parte del Instituto Tecnológico Superior Sudamericano Quito, que son un ejemplo y siempre promueven el aprendizaje para mi conocimiento y formación.

Son muchas las personas que han formado parte de mi vida a las que me encantaría agradecerles su amistad, consejos, ánimo y compañía en los momentos más difíciles de mi vida, gracias por formar parte de mi vida, por todo lo que me han brindado y por todas sus bendiciones.

Para ellos: muchas gracias y que Dios los bendiga.

DEDICATORIA

Para obtener grandes resultados, hay que realizar grandes sacrificios. La concepción de este Proyecto está dedicada a mis padres, pilares fundamentales en mi vida, por su apoyo, sus consejos y sus valores que me ha permitido ser una persona de bien, pero más que nada por su amor.

A mis hermanas por su apoyo y la motivación constante que estudiando se puede conseguir varias metas profesionales y personales para ser feliz por cada objetivo alcanzado.

A mis maestros por sus enseñanzas impartidas y colaborar con mi formación de manera ejemplar.

RESUMEN

La información y los recursos informáticos son activos importantes y vitales del Instituto Tecnológico Superior Sudamericano, por lo que las máximas autoridades y los empleados en cualquier nivel jerárquico, tienen el deber de custodiarlos, preservarlos, utilizarlos y mejorarlos.

Esto implica que se deben tomar las acciones pertinentes para asegurar que la información y los sistemas informáticos estén apropiadamente protegidos contra muchas clases de amenazas y riesgos, sin importar los medios en los cuales la información se genera y/o guarde (en papel o en forma electrónica); como se procesa (computadoras personales, servidores, correo de voz, etc.) y cómo se transmite (en físico, correo electrónico, conversación telefónica, chat corporativo, etc.).

Ya no es suficiente con establecer controles en forma aislada, tampoco es suficiente actuar de modo meramente reactivo y defensivo, se requiere de un sistema de gestión de seguridad de la información (SGSI) y un accionar proactivo.

Las políticas de seguridad informática basadas en las normas ISO 27002: 2005 tienen como finalidad conocer las vulnerabilidades a las que están expuestos los recursos informáticos como son los software, hardware, diseño de red, enfocados desde el punto de vista técnico de seguridad.

El análisis en el Instituto Tecnológico Superior Sudamericano tiene como objetivo el estudio de la seguridad en los procesos críticos; a través de reuniones, consultas, observación, encuestas y ejecución de entrevistas al responsable de los laboratorios, para identificar los riesgos actuales a los que se exponen los datos tanto físicos, lógicos y sistemas de procesamiento de información.

Los resultados obtenidos darán a conocer que para minimizar los riesgos existentes es necesario implementar políticas de seguridad, lo cual ayudará a fortalecer tres aspectos importantes: la confidencialidad, integridad y disponibilidad de la información.

ABSTRACT

Information and computer resources are important and vital assets of the *Instituto Tecnologico Superior Sudamericano*, therefore, the highest authorities and employees at any hierarchical level have the duty to guard, preserve, use and improve them.

This implies that the pertinent actions must be taken to ensure that information and computer systems are properly protected against all kinds of threats and risks, regardless of the means in which the information is generated and / or stored (on paper or in electronic form); how it is processed (personal computers, servers, voicemail, etc.) and how it is transmitted (physical, email, telephone conversation, corporate chat, etc.).

It is no longer enough to establish controls on isolation, it is not enough to act in a merely reactive and defensive way; an information security management system (ISMS) and a proactive action are required.

The computer security policies based on the ISO 27002: 2005 standards are aimed at knowing the vulnerabilities to which computer resources are exposed, such as software, hardware, network design; everything focused from the technical safety point of view.

The objective of the analysis in the *Instituto Tecnologico Superior Sudamericano* is the study of safety in critical processes; through meetings, consultations, observations, surveys and the execution of interviews with the head of the laboratories, in order to identify the current risks to which the physical, logical data and information processing systems are exposed.

The results obtained will make show that in order to minimize existing risks it is necessary to implement security policies, which will help strengthen three important aspects: confidentiality, integrity and availability of information.

INDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

LISTA DE ANEXOS

1. ASPECTOS GENERALES

1.1 Introducción

La seguridad de la información no es un activo a comprar, ni un fin en sí mismo, tampoco un estado a alcanzar haciendo una determinada inversión; debe gestionarse, debe existir una meta concreta, criterios generales de evaluación y de decisión, y debe poder medirse.

Es un sistema dinámico en constante evolución que debe ser evaluado y monitoreado, con políticas establecidas que permitan comparar conscientemente y lo más objetivamente posibles escenarios diferentes y tomar decisiones con respecto a los riesgos que se afrontan y los recursos disponibles.

El Instituto Tecnológico Sudamericano identifica la información como un componente indispensable en la conducción y consecución de los objetivos, razón por la cual es necesario que el Instituto establezca políticas que aseguren que la información es protegida de una manera adecuada independientemente de la forma en la que ésta sea manejada, procesada, transportada o almacenada.

Este documento describe las políticas y para la elaboración del mismo, se toman como base las recomendaciones del estándar ISO 27002:2005[1]. Las políticas incluidas constituyen como parte fundamental del sistema de gestión de seguridad de la información del Instituto y se convierten en la base para la implantación de los controles, procedimientos y estándares definidos.

En nuestro país las empresas y unidades educativas como escuelas, colegios, institutos tecnológicos y universidades deciden realizar auditorías informáticas en el momento que detectan debilidades potenciales dentro de la unidad de tecnología de la información y muchas de las veces cuando sus indicadores dan muestra de desvío dentro de la planificación del Departamento.

[1] ISO 27002:2005, Es el estándar internacional que respalda la implementación de un Sistema de gestión de seguridad de la información, cubre a todo tipo de organizaciones (empresas comerciales, agencias, gubernamentales, organizaciones, instituciones sin ánimo de lucro) e independientemente de su tamaño (pequeña, mediana o gran empresa), tipo o naturaleza.

La falta de seguridades, tanto a nivel físico como lógico, no permiten salvaguardar la información de la empresa, siendo un riesgo que puede causar pérdidas económicas y el peligro de accesos no autorizados.

La seguridad informática es una necesidad presente dentro de una organización o compañía, los controles o procedimientos permitirán verificar los objetivos de continuidad de servicio, confidencialidad y seguridad de la información.

Actualmente el Instituto Tecnológico Superior Sudamericano Quito[2] no ha recibido una auditoría de seguridad informática lo que conlleva a plantear este Proyecto, ayudando a establecer políticas definidos en cada una de las funciones informáticas y cumplimiento de acuerdo al análisis elaborado.

1.2 Justificación

Es importante diseñar e implementar un sistema de seguridad informática, el principal riesgo es el robo de información sensible y confidencial, el cual puede ocasionar hasta el cierre de una institución.

La pérdida o mal uso de información confidencial genera daños y repercusiones relacionados con la integridad y disponibilidad de los archivos para el titular del documento.

Los elementos que forman parte del sistema de seguridad son denominados activos de una institución los cuales deben ser protegidos para evitar su pérdida, modificación o el uso inadecuado de su contenido.

Generalmente estos activos se dividen en tres grupos:

- ✓ Datos e Información
- ✓ Sistemas e Infraestructura: Son los componentes donde se mantienen o guardan los datos e informaciones

[2] El Instituto Tecnológico Superior Sudamericano Quito, es una institución de educación superior de derecho privado creado mediante Acuerdo Ministerial Nro. 2138 del 28 de junio de 1995, elevando a la categoría de Tecnológico mediante registro CONESUP conforme a lo dispuesto al Artículo 23 de la Ley de Educación Superior con Nro. 17-010 con fecha 13 de septiembre del 2000; con finalidad social y sin fines de lucro, con personería jurídica propia, con capacidad de autogestión administrativa y financiera para el cumplimiento de su misión y patrimonio propio.

- ✓ Personal: Son todos los individuos que manejan o tienen acceso a los datos e informaciones y son los activos más difíciles de proteger, porque son móviles, pueden cambiar su afiliación y son impredecibles.

No tener una política de seguridad de la información clara y definida, lleva inevitablemente al acceso no autorizado a una red informática o a los equipos que en ella se encuentran y puede ocasionar en la gran mayoría graves problemas.

El Instituto Tecnológico Sudamericano tiene el deber y la obligación de preservar los activos de información, utilizarlos y mejorarlos. Esto implica que para tomar las acciones apropiadas sobre la seguridad de la información deben ser basadas en la protección de muchas clases de amenazas y riesgos tales como fraude, sabotaje extorsión, violación de la privacidad, intrusos, hackers e interrupción del servicio.

1.3 Antecedentes

La evolución de los sistemas computacionales y aplicaciones, del Internet y de las comunicaciones en general han abierto una puerta para que las personas empiecen a descubrir el valor de la información y la facilidad de acceder a los datos.

En la institución académica se maneja información transcendental de estudiantes, dicha información debe ser protegida de ataques informáticos, lo mismos que pueden ocasionar serios problemas a sus bienes, servicios y operaciones.

La información es importante para todas las organizaciones y sin ella la empresa o entidades educativas como escuelas, colegios, Institutos Tecnológicos y Universidades dejarían de funcionar, es fundamental tener un plan o una estructura de seguridad de la información.

De acuerdo a una encuesta realizada al encargado del Área de Sistemas de la Institución, el mayor riesgo a la seguridad de la información está dado por el factor humano, específicamente errores, conductas inapropiadas y/o negligencia generadas internamente.

El desafío es entonces lograr una metodología que conduzca a una solución eficaz y eficiente, desde el punto de vista técnico y económico, que provea los niveles de seguridad requeridos y brinde la confianza al Instituto y a los usuarios.

1.3.1 Descripción general del Instituto Tecnológico Superior Sudamericano Quito

El Instituto cuenta con Carreras Tecnológicas como: Administración Turística, Sistemas de Automatización, Gestión Ambiental, Administración de Empresas y Gastronomía que son Carreras enfocadas en la matriz productiva del Ecuador.

Cuenta con la experiencia de docentes calificados para cada Carrera.

Historia

El Instituto Tecnológico Superior Sudamericano Quito funciona desde el año 1995, ubicado anteriormente en la dirección Av. Pérez Guerrero y Versalles (sector Santa Clara), como colegio e Instituto Tecnológico Superior. A partir del año 2012 cuenta con nueva infraestructura de acuerdo a las Carreras Tecnológicas refrendadas por la SENESCYT[3] en la dirección Av. 10 de Agosto N35-108 e Ignacio San María, con aulas amplias, laboratorios de computo, áreas dedicadas para cada carrera y tecnología para la enseñanza del alumnado.

Visión

Ser el mejor Instituto Tecnológico Superior del país, con una proyección internacional, para entregar a la sociedad hombres íntegros, profesionales excelentes, líderes en todos los campos, con espíritu emprendedor, con libertad de pensamiento y acción.

Misión

Formar gente de talento con calidad humana, académica, basada en principios y valores, cultivando pensamiento crítico, reflexivo e investigativo, para que comprendan que la vida es la búsqueda de un permanente aprendizaje.

Valores

- Libertad
- Responsabilidad
- Disciplina
- Constancia

[3] Senescyt.- es la entidad del gobierno ecuatoriano que ejerce la rectoría de la política pública en los ejes de su competencia. Tiene como misión coordinar acciones entre la Función Ejecutiva y las instituciones del Sistema de Educación Superior.

- Estudio

1.3.2 Organigrama del instituto

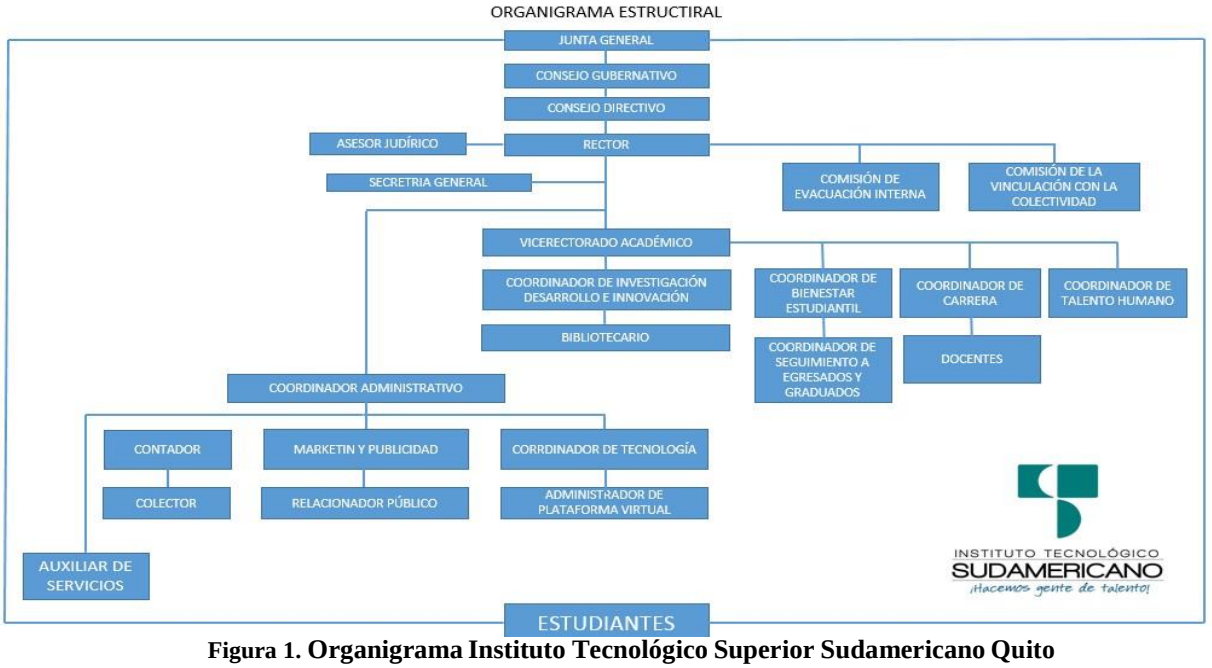

Figura 1. Organigrama Instituto Tecnológico Superior Sudamericano Quito
Fuente: el autor

1.3.3 Análisis de la situación actual

A continuación, se describirá la infraestructura actual del Instituto Tecnológico Sudamericano hasta el mes de marzo de 2018; los datos obtenidos son resultado de la información recogida en colaboración con el Administrador de Sistemas, inventario realizado y revisión de las instalaciones físicas.

Esta información permitirá realizar un análisis de la situación actual, en cuanto a seguridad, para determinar el punto de partida.

Con respecto a la disposición física del servidor del Instituto, este se encuentra ubicado en el laboratorio del cuarto y tercer piso, no cuenta con seguridad para su acceso, el tendido de cable UTP categoría 5e fue remodelado; de manera que la instalación sea independiente de la red eléctrica y evitar problemas de red.

1.3.4 Estructura de la red del Instituto

La red LAN del Instituto cuenta con tres servidores y 47 pc, 37 para uso de los estudiantes (laboratorio del tercer y cuarto piso) y 10 para el personal administrativo (piso 1). Existen dos redes una red LAN y otra red inalámbrica con routers en cada piso para la conexión móvil o portátil. Ver Anexo B

1.3.5 Datos del servidor

En el servidor principal está instalado el sistema operativo.
A continuación, las características del servidor principal

Aplicación:	**Internet**
Procesador:	Intel Xeon E3-1200 V3
Disco duro:	2 TB
Memoria RAM	8 GB
Dirección Ip WAN	WAN: 186.46.165.174
Dirección Ip LAN	LAN: 192.168.1.1
Sistema operativo.	clearOS

Tabla 1: Características del Servidor Principal del Instituto
Fuente: el autor

Figura 2. Fotografía del Servidor Principal del Instituto
Fuente: el autor

Características del Segundo Servidor

Aplicación:	**Internet**
Procesador:	Xeon 3040
Disco duro:	120 Gb
Memoria Ram	2 Gb
Dirección Ip WAN Y LAN	WAN: 192.168.1,200
	LAN: 192.168.1.2
Sistema operativo.	clare s7

Tabla 2: Características del Segundo Servidor del Instituto
Fuente: el autor

Figura 3. Fotografía del Segundo Servidor del Instituto
Fuente: el autor

Características del tercer servidor.

Aplicación:	**Internet**
Procesador:	Xeon 5000
Disco duro:	120 Gb
Memoria Ram	3 Gb
Dirección Ip WAN	WAN: no tiene
Dirección Ip LAN	LAN: 192.168.1.210
Sistema operativo.	WINDOWS 7

Tabla 3: Características del Tercer Servidor del Instituto
Fuente: el autor

1.3.6 Datos de las estaciones de trabajo del laboratorio

Las 37 estaciones de trabajo tienen instalado dos sistemas operativos Windows y Ubuntu.
Características equipos desktop

CPU	**Hp/ Dell y Clones**
Procesador	Intel Core 2 Duo
Disco duro	250 GB
Memoria	2 GB
Sistema operativo	Windows 10 / Ubuntu 12

Tabla 4: Características de Pc's de los laboratorios
Fuente: el autor

1.3.7 Estructura de la red WAN

El Instituto cuenta con un enlace a intranet de fibra óptica (simétrica) de un 20Mbps/20Mbps compartición 2 a 1, servicio contratado a la Corporación Nacional de Telecomunicaciones CNT EP.

Cuenta con una ONT AN550 Huawei y un router inalámbrico que son de propiedad del proveedor de servicio de internet. Este router se encuentra conectado al modem para proveer del servicio a toda la red, y se encuentra configurando con otro rango de IP para la red inalámbrica.

Figura 4. Fotografía Modem CNT EP GPON AN550
Fuente: el autor.

Figura 5. Fotografía Armario Rac de red de la Institución
Fuente: el autor

Figura 6. Fotografía Router TP-LINK
Fuente: el autor

1.3.8 Enlaces de comunicación

A continuación, la descripción del enlace:

Proveedor	**Corporación Nacional de Telecomunicaciones CNT EP.**
Teléfono	1800 100 100/ 1800 268 267
Contacto	Soporte Técnico
Ancho de banda	20Mbps/20Mbps
Direcciones IP reales	192.168.100.1
Descripción de enlace	Dedicado Exclusivamente para internet

Tabla 5: Descripción del Proveedor de Servicio de Internet de la Institución
Fuente: el autor

2. OBJETIVOS

2.1 Objetivo general

Establecer políticas de seguridad informática, mediante el diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO 27002 versión 2005, controlando el nivel de confiabilidad de información de datos en el Instituto Tecnológico Superior Sudamericano Quito.

2.2 Objetivos específicos

1. Analizar la situación actual y las posibles vulnerabilidades, posibles amenazas informáticas a las que se ve expuesta la información en el Instituto Tecnológico Superior Sudamericano Quito.

2. Determinar los parámetros y las políticas que se deben implementar en el sistema para mejorar la gestión, el manejo y proceso de información del Instituto Tecnológico Superior Sudamericano, con el fin de que el personal administrativo no realice modificaciones constantes.

3. Diseñar el Sistema de Gestión de la Seguridad Informática (SGSI) de acuerdo a los resultados obtenidos en los análisis de vulnerabilidades y amenazas, aplicado bajo las normas ISO 27002 versión 2005.

3. MARCO TEÓRICO

"Para el establecimiento de un sistema de gestión de seguridad de la información se utilizan los conceptos básicos referentes a seguridad y metodologías que se utilizan en la actualidad que proporcionan estándares de seguridad y protección, como lo son ISO/IEC 27002." (Larrondo, 2010)

3.1 Seguridad informática

La seguridad informática es la punta principal al iniciar desde un simple proyecto computacional ya sea software o hardware, hasta la implementación de aplicaciones, redes, o cualquier cosa que pueda ser escalón para atentar contra la seguridad (Gomez, 2011).

La seguridad informática tiene muchas ramas y métodos a nivel empresarial o de una organización, en la actualidad con el mundo de internet existen varias técnicas o software para vulnerar estos mecanismos de defensas al momento de proteger la información o activos sean físicos y lógicos.

"La seguridad informática es un proceso continuo, no un producto". Por lo tanto, es conjunto de sistemas procedimientos métodos y herramientas destinados a proteger la información." (Cocho, 2003).

Los requisitos que atribuyen cuando se habla de seguridad informática son complejos se debe tener en cuenta que se necesita proteger y clasificar la información según la importancia o el nivel de impacto si esa información o sistema es importante y cuáles serían la herramientas a utilizar "La informática es una herramienta que implica riesgos cada vez más crecientes, a veces mal conocidos y combatidos, por este motivo es preciso considerar el análisis de riesgo en las organizaciones, a fin de fortalecer la seguridad informática y garantizar la integridad, la confidencialidad y la disponibilidad de la información" (Ribagorda, 1995).

Para llevar a cabo la implementación de las mejores medidas de seguridad informática[4], se requiere un análisis de todo lo que se va a proteger.

[4] Seguridad Informática es un proceso y análisis de riesgos para garantizar la integridad, confidencialidad y disponibilidad de la información, conforme la tecnología evoluciona se implementa nuevos parámetros de seguridad y evaluación.

“El impacto social de las tecnologías de la información y de la sociedad informatizada es vulnerable” (Joyanes, 1998).

Tomando como referencia lo que sostiene Joyanes, se puede afirmar que la seguridad informática nace con la aparición de los ataques a la información y de los activos informáticos por parte de los intrusos interesados, en el contenido de esta. En este contexto, el objetivo de la seguridad de la información consiste en mantener la confidencialidad, la integridad y la disponibilidad.

3.1.1 Confidencialidad

La confidencialidad es la característica que hace que los componentes del sistema sean accesibles solo por los usuarios autorizados del mismo. Con esto se consigue que los datos e informaciones recogidas dentro de un sistema no puedan ser reveladas ni mostradas a ningún usuario o personal no autorizado que pudiera hacer un uso fraudulento o incorrecto de estos.

“Se establecen varios niveles de seguridad en base a los cuales se necesitara un grado de protección más alto atendiendo a la naturaleza de la información.” (Gomez, 2011)

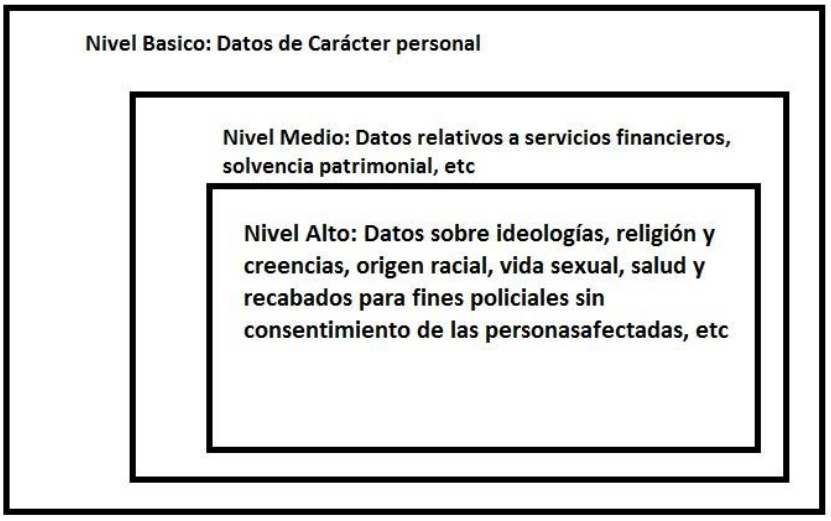

Figura 7. Niveles de seguridad según la naturaleza
Fuente: el autor

3.1.2 La integridad

La integridad es la característica que asegura que la información de que se dispone es completa y exacta en todo momento. Además, que la misma solo puede ser modificada o gestionada por los usuarios autorizados para ello, sin que ningún otro usuario externo a la misma pueda acceder a ella (en el caso que los datos sean modificados por personal no autorizado, esta modificación deberá ser registrada para posteriores controles y auditorías).

"Así la integridad de un sistema será un aspecto clave, puesto que se tendrá la confianza de que los datos que se están manejando tienen la fiabilidad necesaria y no han sido manipulados" (Gonzales, 2012)

3.1.3 La disponibilidad

No serviría de nada tener una información y unos datos almacenados de forma segura a la que no se pudiera acceder en el momento en que se necesiten, por ello esta característica asegura que los datos que están almacenados dentro del sistema sean accesibles por los usuarios autorizados para ello independientemente de la situación en la que estos se encuentren.

"En caso de que suceda algún fallo, error, pérdida o ataque en el sistema, este tiene que ver la capacidad y autonomía suficiente para poder recuperar el control lo antes posible, y así seguir ofreciendo las funcionalidades de las que dispone" (Fernández, Saiz, & Seoane, 2014).

3.1.4 La autenticidad

Una de las propiedades que abarca dentro de la seguridad informática en la actualidad se hace referencia a la autenticidad usada hoy en día por correos electrónicos, redes sociales o cualquier sitio web que permita él envío de información se segura, de donde procede y cuál es el destino final (suplantación de identidad).

"La autenticidad es la manera de asegurar el origen y el destino de la información, asegurando que la entidad no es falsa, ya sea utilizando la firma electrónica o digital, la validez del correo electrónico, mediante biometría, etc." (Fernández, Saiz, & Seoane, 2014)

3.1.5 Imposibilidad al rechazo

A través de esta imposibilidad de rechazo asegura que cualquier entidad o usuario que haya enviado o recibido información, niegue el haberlo hecho para eximirse de responsabilidades o con cualquier otro fin.

"cualquier usuario que haya enviado información nunca podrá negar ante otros que no lo hizo, puesto que sus acciones han sido registradas de forma que sin lugar a dudas pueda ser identificado como el causante de su acción. Al igual que sucede con el destinatario de esa información que tampoco podrá repudiar el hecho que la recibió" (Gonzales, 2012).

3.2 División de la seguridad

Dependiendo de la naturaleza de las amenazas, se puede dividir la seguridad física y seguridad lógica.

3.2.1 Seguridad física

Se utiliza para proteger el sistema informático utilizando barreras físicas y mecanismos de control. Se emplea para proteger físicamente el sistema informático.

Las amenazas físicas[5] pueden ser provocadas por el usuario, de forma accidental o voluntaria, o bien por factores naturales.

Dentro de las provocadas por el usuario, encontramos amenazas de tipo:

- Accidentales, como borrado de archivos accidentales, olvido de clave de cualquier sesión de red o software.
- Deliberadas, tales como robo de clave, borrado deliberado de la información, robo de datos confidenciales.

Dentro de las provocadas por factores naturales, podemos encontrar: incendios, sismos etc.

Los desastres que pueden suceder se pueden clasificar en

- Destrucción del centro de cómputo: completa o parcial

Amenazas Físicas[5].- Comprende al aspecto del hardware y la manipulación del mismo y el lugar en lo cual se va a instalar los equipos, a menudo se descuida la seguridad sobre el acceso, pero hay que tener en cuenta que cuando existe acceso físico a un recurso ya no existe seguridad alguna sobre el mismo, con el consiguiente riesgo: Un error típico de seguridad por acceso físico es el de tomas de conexión a la red informática no controladas, de acceso libre: un atacante con los suficientes conocimientos técnicos puede causar graves daños.

- Destrucción o mal funcionamiento de los equipos auxiliares del centro de cómputo
- Destrucción parcial o total de los equipos descentralizados.
- Pérdida de clave por parte del personal
- Huelga o problemas laborales
- Perdida de información, manuales o documentación esta puede ser parcial o completa.

Para estas medidas se debe realizar un plan de seguridad deberá contener todos los puntos, medidas de seguridad adaptadas a cada situación que dependerá del entorno en el que se localiza la organización. Este plan deberá distribuirse entre el personal responsable de la operación, y por precaución es recomendable tener una copia fuera de la dirección o área informática, si ocurre algún daño o vulnerabilidad posteriormente hay que cuantificar el daño o pérdida del equipos, archivos y documentos, para definir qué parte del plan debe ser activado: determinando el estado de todos los sistemas.

3.2.2 Seguridad lógica

La seguridad lógica[6] se encarga de asegurar la parte del software de un sistema informático, que se compone de todo lo que no es físico, es decir, los programas y los datos.

La seguridad lógica se encarga de controlar que el acceso al sistema informático, desde el punto de vista del software se realice correctamente y por usuarios autorizados, ya sea desde dentro del sistema informático, como fuera, es decir desde una red externa, usando una VPN[7] (protocolos PPTP[8] Protocolo de túnel punto a punto), la web (protocolos HTTP[9] Protocolo de

[6] Seguridad Lógica.- Son programas que pueden dañar el sistema: Virus y Malware, el punto más débil de un sistema informático son las personas relacionadas en mayor o menor medida con él, puede ser por falta de conocimiento o ataques intencionados propiamente, pero en cualquier escenario que se presente se busca prevenir.

[7] VPN.- (Virtual Private Network) es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet. Las empresas suelen utilizar estas redes para que sus empleados, desde sus casas, hoteles, etc., puedan acceder a recursos corporativos que, de otro modo, no podrían. Sin embargo, conectar la computadora de un empleado a los recursos corporativos es solo una función de una VPN.

[8] PPTP.- Tunelización de Punto a Punto El PPTP, que opera en el puerto TCP 1723, es uno de los protocolos VPN más antiguos en uso, en todas las versiones de Windows desde entonces.

transferencia de Hipertexto, HTTPS[10] protocolo de seguro de transferencia de hipertexto) , Transmisión de ficheros (FTP[11] Protocolo de transferencia de archivos), TELNET[12] (Telecommunication Network) (Gonzales, 2012)

Para mantener la seguridad de un sistema informático, se puede utilizar diferentes técnicas, como el uso de contraseñas, encriptación de la información, uso de programas antivirus, firewalls.

La seguridad lógica esta estandarizada de acuerdo a unos niveles determinados de seguridad. El estándar más utilizado internacionalmente es el que ofrece la TCSEC[13], los niveles describen diferentes tipos de seguridad de un sistema operativo y se enumera desde el mínimo grado de seguridad al máximo.

La clasificación de los sistemas de computación o informáticos ha sido ampliamente estudiada en el campo de la seguridad del sistema y son 4 niveles A, B, C y D. (Gomez, 2011)

> ***"Nivel D:*** *Sistemas que no cumplen con ninguna especificación de seguridad. No hay protección para el hardware, el sistema operativo es inestable y no hay autentificación.*
>
> ***Nivel C1: "****Protección discrecional. El acceso a distinta información se realiza mediante identificación de usuarios. Cada usuario maneja por tanto una información privada y distingue entre usuarios y el administrador del sistema, por lo tanto hay acceso de control discrecional e identificación y autenticación de usuarios."*

[9] HTTP.-es un protocolo de transferencia donde se utiliza un sistema mediante el cual se permite la transferencia de información entre diferentes servicios y los clientes que utilizan páginas web.
[10] HTTPS.-es un protocolo de comunicación de Internet que protege la integridad y la confidencialidad de los datos de los usuarios entre sus ordenadores y el sitio web.
[11] FTP.- es un protocolo de transferencia de archivos entre sistemas conectados a una red TCP basado en la arquitectura cliente-servidor.
[12] TELNET.- es el nombre de un protocolo de red que nos permite acceder a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella
[13] TCSEC.- Trusted Computer System Evaluation, desarrollado desde 1982 describe todos los niveles y diferentes tipos de seguridad en sistemas operativos.

Nivel C2: *Protección de acceso controlado. Se debe llevar auditoria de acceso e intentos fallidos de acceso a objetos. Tiene la capacidad de restricción para que los usuarios ejecuten cierto comando o tengan accesos a determinados archivos, también deniega o permite datos a usuarios en base no solo a los premisos sino también a los niveles de autorización. Requiere que se audite el sistema.*

Nivel B1: *Seguridad etiquetada. A cada objeto del sistema se le asigna una etiqueta con nivel de seguridad estipulado con respecto a una jerarquía (reservado, secreto, alto secreto, etc.) y con una categoría. Cada usuario que accede a un objeto debe poseer el permiso expreso para hacerlo (cada usuario tiene sus objetos asociados).*

Nivel B2: *Protección estructurada. Requiere que se etiquete cada objeto de nivel superior por ser padre de un objeto inferior. La protección estructurada es la primera que empieza a referirse al problema de un objeto a un nivel más elevado de seguridad y comunicación con otro objeto a un nivel inferior.”*

Nivel B3: *Dominios de seguridad. Refuerza a los dominios con la instalación de hardware, todas las estructuras de seguridad deben ser lo suficientemente pequeñas como para permitir análisis y comprobaciones ante posibles violaciones. Este nivel requiere que el usuario se conecte al sistema por medio de una conexión segura.*

Nivel A: *Protección verificada. Es el nivel más elevado, incluye un proceso de diseño, control y verificación, mediante métodos formales (matemáticos) para asegurar todos los procesos que realiza un usuario sobre el sistema*.”

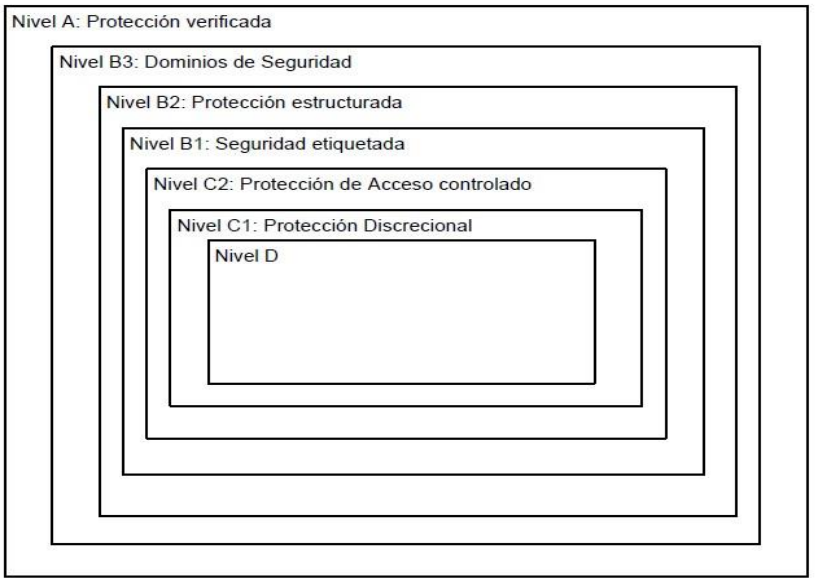

Figura 8. Niveles de seguridad Lógica
Fuente: Elaboración Propia

3.3 Aspectos fundamentales de la seguridad informática

La norma ISO/IEC 27002:2005[14] nos define los siguientes conceptos:

Entre los principales objetivos de la seguridad informática podríamos destacar lo siguiente:

- Minimizar y gestionar los riesgos de detectar los posibles problemas y amenazas a la seguridad.
- Garantizar la adecuada utilización de los recursos y de las aplicaciones del sistema.
- Limitar las pérdidas y conseguir la adecuada recuperación del sistema en caso de un incidente e seguridad.
- Cumplir con marco legal y con los requisitos impuestos por los clientes en sus contratos. (ISO, 2013)

"Una organización debe entender que la seguridad informática como un proceso y no como un producto que se pueda comprar o instalar. Se trata por lo tanto de un ciclo interactivo, en el que se incluye actividades como la valoración de riesgos, prevención, detección y respuesta ante incidentes de seguridad". (Gomez, 2011)

[14] ISO 27002:2005.- gestiona de forma adecuada la gestión de la seguridad de la información, que se adaptan a las necesidades del negocio u organización para dar los primeros pasos de un análisis profundo.

Figura 9. La Seguridad informática como proceso y no como producto
Fuente: Tomado (Gomez, 2011)

3.4 Políticas de la seguridad

Las ventajas que ofrece el plantear objetivos en la organización garantiza que la información manejada dentro y fuera del sistema central de la organización, cuente con los elementos necesarios para asegurar su protección contra alteración, divulgación o negación de acceso no autorizados, permitiendo la continuidad de las operaciones en las áreas de negocio principalmente o en áreas donde se maneja información secreta, confidencial o privada.

El principal objetivo informático de la organización es dar protección y seguridad a su información, para ello es necesario establecer las normas, políticas y estándares de seguridad para los sistemas distribuidos que procesan, almacenan y transmiten información, a fin de minimizar los riesgos en su integridad, confidencialidad y disponibilidad.

“La política de seguridad es un conjunto de leyes, reglas y prácticas que regulan la manera de dirigir, proteger y distribuir recursos en una organización para llevar a cabo los objetivos de seguridad informática dentro de la misma.” (López & Quezada, 2006)

La política define la seguridad informática para una organización, especificando tanto las propiedades del sistema como las responsabilidades de seguridad de las personas. En sí es un conjunto de leyes, reglas y prácticas que permiten salvaguardar los activos de una organización y brindar seguridad dentro de ésta. Las políticas sirven para cumplir los objetivos de seguridad dentro de una organización. (Fernández, Saiz, & Seoane, 2014).

3.4.1 ¿Cuándo escribir políticas de seguridad?

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

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

3.4.2 Modificar las políticas de seguridad

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

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

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

3.4.3 ¿Qué protege una política de seguridad?

Se protege lo que realmente tiene un valor para la empresa u organización, en la actualidad es necesaria y fundamental la implementación de las medidas de seguridad basadas en hardware, software y recursos humanos.

"Una política de seguridad está basada en varios mecanismos y procesos, la certificación y la norma ISO 27002 define una política de seguridad como un documento que ofrece instrucciones de administración y soporte para la seguridad de la información de acuerdo con los requisitos incluye 11 cláusulas." (ISO, 2013)

Para el desarrollo de este plan de estudio se realizó la entrevista con el responsable del área de sistemas del Instituto Tecnológico Superior Sudamericano Quito, se pudo comprobar que no se tiene normas de seguridad de la información, de lo cual se tomó el modelo con los estándares y normas de controles de la ISO 27002:2005. **Ver Anexo A**

3.5 Análisis de riesgos

Este procedimiento ayuda para implementar controles de seguridad en el Instituto Tecnológico Superior Sudamericano Quito, permitiendo calcular las vulnerabilidades y evalúa el efecto de las amenazas en cada área o a su nivel general, en la mayoría de los casos, el análisis de riesgos intenta mantener un balance económico entre el impacto de los riesgos y el costo de las soluciones de un programa efectivo de seguridad destinadas a manejarlos reduciendo la magnitud del daño[15].

"Un análisis de riesgos es el primer paso de una gestión de riesgo a nivel general, sirve para identificar las consecuencias probables o los riesgos asociados con las vulnerabilidades y así implementar controles que reduzcan los efectos a un nivel aceptable, Ya que no se puede contar con una seguridad total con el fin de valorar el su grado de riesgo." (Henríquez, 2011)

[15] Magnitud del Daño.- Existen varios métodos de como valorar un riesgo y al final, todos tienen los mismos retos las variables son difíciles de precisar y en su mayoría son estimaciones- y llegan casi a los mismos resultados y conclusiones,

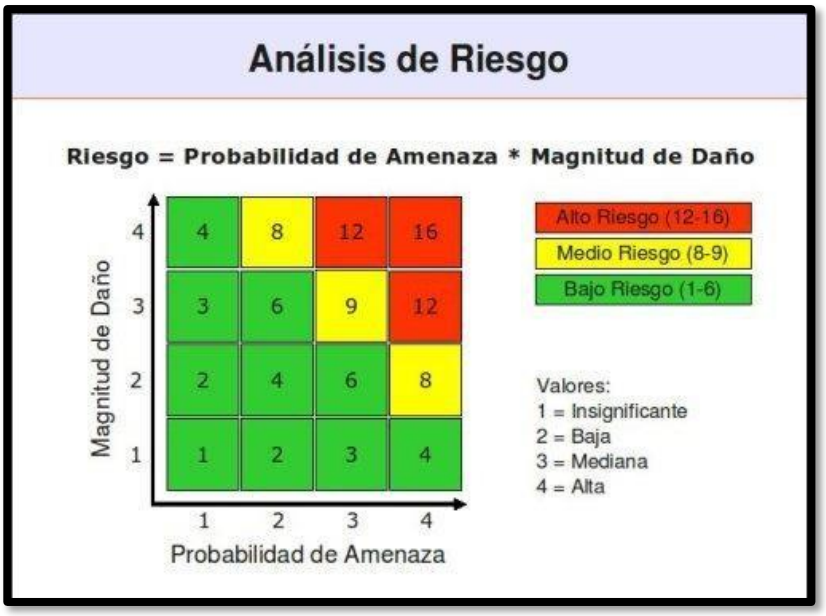

Figura 10. Análisis del Riesgo
Fuente: https://protejete.wordpress.com/gdr_principal/matriz_riesgo/

La Matriz para el Análisis de Riesgo, es punto clave en analizar y determinar los riesgos en el manejo de los datos e información de las organizaciones.

Hay que tomar en cuenta que el análisis de riesgo es un análisis detallado, extenso y consumidor de tiempo, porque requiere que se compruebe todos los posibles daños de cada recurso de una institución contra todas las posibles amenazas.

3.5.1 Clasificación del riesgo

El objetivo de la clasificación de riesgo es determinar hasta qué grado es factible combatir los riesgos encontrados. “La factibilidad normalmente depende de la voluntad y posibilidad económica de una institución, sino también del entorno donde nos ubicamos. Los riesgos que no queremos o podemos combatir se llaman riesgos restantes y no hay otra solución que aceptarlos.” (Piattini, 2011)

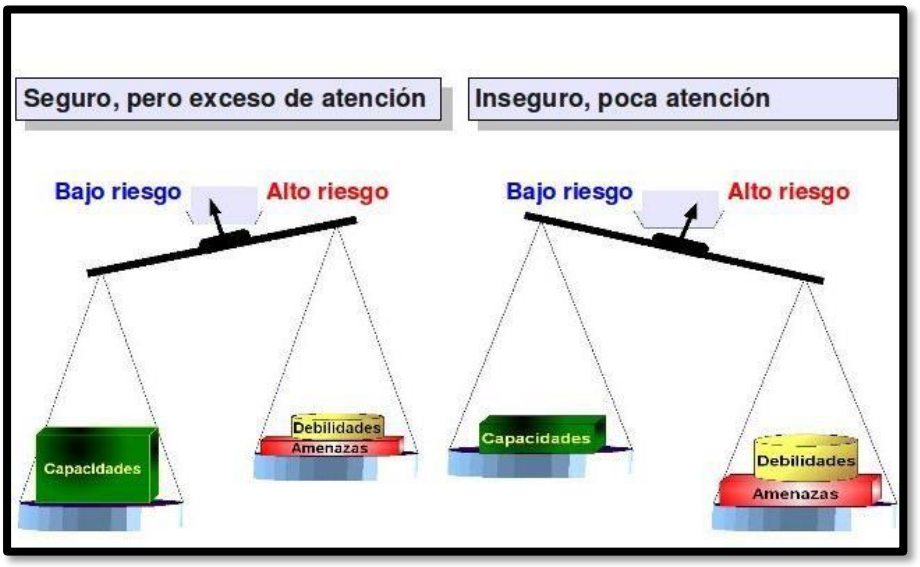

Figura 11. Clasificación del Riesgo
Fuente: https://protejete.wordpress.com/gdr_principal/clasificacion_riesgo/

Implementar medidas para la reducción de los riesgos significa realizar inversiones, en general económicas. El reto en definir las medidas de protección, entonces está en encontrar un buen equilibrio entre su funcionalidad (cumplir con su objetivo) y el esfuerzo económico que tenemos que hacer para la implementación y el manejo de estas.

De igual manera como debemos evitar la escasez de protección, porque nos deja en peligro que pueda causar daño, "El exceso de medidas y procesos de protección, pueden fácilmente paralizar los procesos operativos e impedir el cumplimiento de nuestra misión." (Gonzales, 2012)

El caso extremo respecto al exceso de medidas sería, cuando las inversiones para ellas, superen el valor del recurso que pretenden proteger.

3.5.2 Control de riesgo

El propósito del control de riesgo es analizar el funcionamiento, la efectividad y el cumplimiento de las medidas de protección, para determinar y ajustar sus deficiencias.

Las actividades del proceso, tienen que estar integradas en el plan operativo institucional, donde se define los momentos de las intervenciones y los responsables de ejecución.

Medir el cumplimiento y la efectividad de las medidas de protección requiere que levantemos constantemente registros sobre la ejecución de las actividades, los eventos de ataques y sus respectivos resultados. Estos tenemos que analizados frecuentemente. Dependiendo de la gravedad, el incumplimiento y el sobrepasar de las normas y reglas, requieren sanciones institucionales para los funcionarios.

"En el proceso continuo de la Gestión de riesgo, las conclusiones que salen como resultado del control de riesgo, nos sirven como fuente de información, cuando se entra otra vez en el proceso de la Análisis de riesgo." (Marquina, 2012)

3.6 Metodología

El Instituto no posee todavía ningún sistema de gestión de la seguridad de la información implantado. No tiene procesos, ni procedimientos de seguridad y se debe implementar siguiendo las normas básicas de actuación; por tanto, con esta situación el método a seguir será la de desarrollar el Plan Director de Seguridad que permita comenzar la implantación de un SGSI a fin de mejorar la seguridad de la información en toda la organización y adaptarla al estándar ISO 27002 integrando en todos sus procesos, procedimientos y normas adecuados para consolidar la seguridad de la información en el Instituto Tecnológico Sudamericano Quito.

Para el análisis de riesgos hay distintas metodologías, pero para el proyecto se aplicará la metodología MAGERIT.

3.6.1 Concepto

"Gracias a esta metodología creada por el Consejo Superior de Administración Electrónica es posible que las empresas puedan depender de la tecnología y sus avances para sus procesos administrativos obteniendo como resultado el cumplimiento de su razón misional y visional." (Marquina, 2012)

Su principal objetivo es el de observar y evaluar el uso de los activos informáticos dentro de una organización para corregir acciones que generen un riesgo contribuyendo así con la mitigación del mismo.

Con esta herramienta se permite a los analistas en seguridad de la información establecer acciones de mejora las cuales deben responder a una serie de controles que contribuyan a la mitigación del riesgo dentro del Instituto Tecnológico Superior Sudamericano Quito.

Los activos de información son todos aquellos elementos que utiliza la entidad para la elaboración, edición, transferencia y eliminación de su información, Magerit realiza la clasificación de los mismos de acuerdo a sus características particulares, similitudes o usos elementales lo que permitirá establecer de mejor manera el tratamiento del riesgo para mitigarlo
y hacer más segura la infraestructura informática.

Tipos de activos	Descripción
Activo de información	Archivos multimedia, documentación manuales de usuario, contratos, Normativas, oficios por entidades públicas de educación superior.
Software o aplicación	Sistemas de información, herramientas de desarrollo aplicativos desarrollados y en desarrollo, sistemas operativos, aplicaciones de servidores, etc.
Hardware	Equipos de oficina (PC, Infocus, Servidores, dispositivos móviles, etc.)
Red	Dispositivos de conectividad de redes, (router, swicth, etc.)
Equipamiento auxiliar	UPS
Instalación	Cableado estructurado, instalaciones eléctricas.
Servicios	Conectividad a internet, servicios de mantenimiento, etc.
Personal	Docentes, Personal Administrativo, personal de limpieza y organización etc.

Tabla 6: Clasificación de los Activos Metodología de MAGERIT
Fuente: Elaboración Propia

3.6.2 Objetivos

MAGERIT tiene como objetivos:

- Concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de atajarlos a tiempo.
- Ofrecer un método sistemático para analizar tales riesgos.
- Ayuda a describir y planificar las medidas oportunas para mantener los riesgos bajo control.
- Preparar a la organización para procesos de evaluación, auditoria, certificación o acreditación, según corresponda en cada caso.

"MAGERIT es el método más utilizado en la actualidad ya sea para empresas u organizaciones pequeñas y grandes, se puede utilizar en los tres modelos que son COBIT, ITIL E ISO 27002, para la implementación de las SGSI, el área correspondiente podrá hacer seguimientos de actualización de riegos o activos conforme al informe final obtenido por MAGERIT. " (Larrondo, 2010)

3.7 Auditoría informática

"Es un conjunto de conocimientos, normas, técnicas y prácticas dedicadas a la evolución y aseguramiento de la calidad, seguridad, razonabilidad, y disponibilidad de la información tratada y almacenada a través el computador y equipos a fines, como la eficacia, eficiencia y economía con que las administraciones de un ente están manejando dicha información y todos los recursos físicos y humanos asociados para su adquisición, captura, procesamiento, transmisión, distribución y uso." (Piattini, 2011)

3.7.1 Definición

La auditoría informática es un examen que se realiza con el fin de evaluar la eficiencia de una empresa al nivel de las TI.

"La informática hoy está integrada en la gestión de la empresa y por eso las normas y estándares propiamente informáticos deben estar sometidos a los generales de la misma." (Derrien, 2011)

La auditoría informática como una serie de exámenes que se realizan con carácter objetivo, crítico, sistemático y selectivo", con el fin de evaluar la eficacia y la eficiencia del uso adecuado de los recursos informáticos, de la gestión informática y si estas han brindado el soporte adecuado a los objetivos y a las metas de la empresa o institución.

"Es necesario definir el entorno y los límites donde se va a desarrollar la auditoría[16], es decir, el alcance. De igual forma se deben contemplar los objetivos de la misma.

En un centro de cómputo, es necesario conocer la importancia de realizar una auditoría informática." (Henríquez, 2011)

Las funciones adicionales de una auditoria es también "la revisión y la evaluación de los controles, sistemas, procedimientos de informática de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participa en el procesamiento de la información" (Lardent, 2001)

[16] La auditoría es una necesidad en las organizaciones, es de vital importancia para mantener el buen funcionamiento de los sistemas y la protección de los datos gestionados por esos sistemas. La auditoría se define principalmente por dos aspectos, la eficiencia y la eficacia.

3.7.2 Objetivos de la auditoría

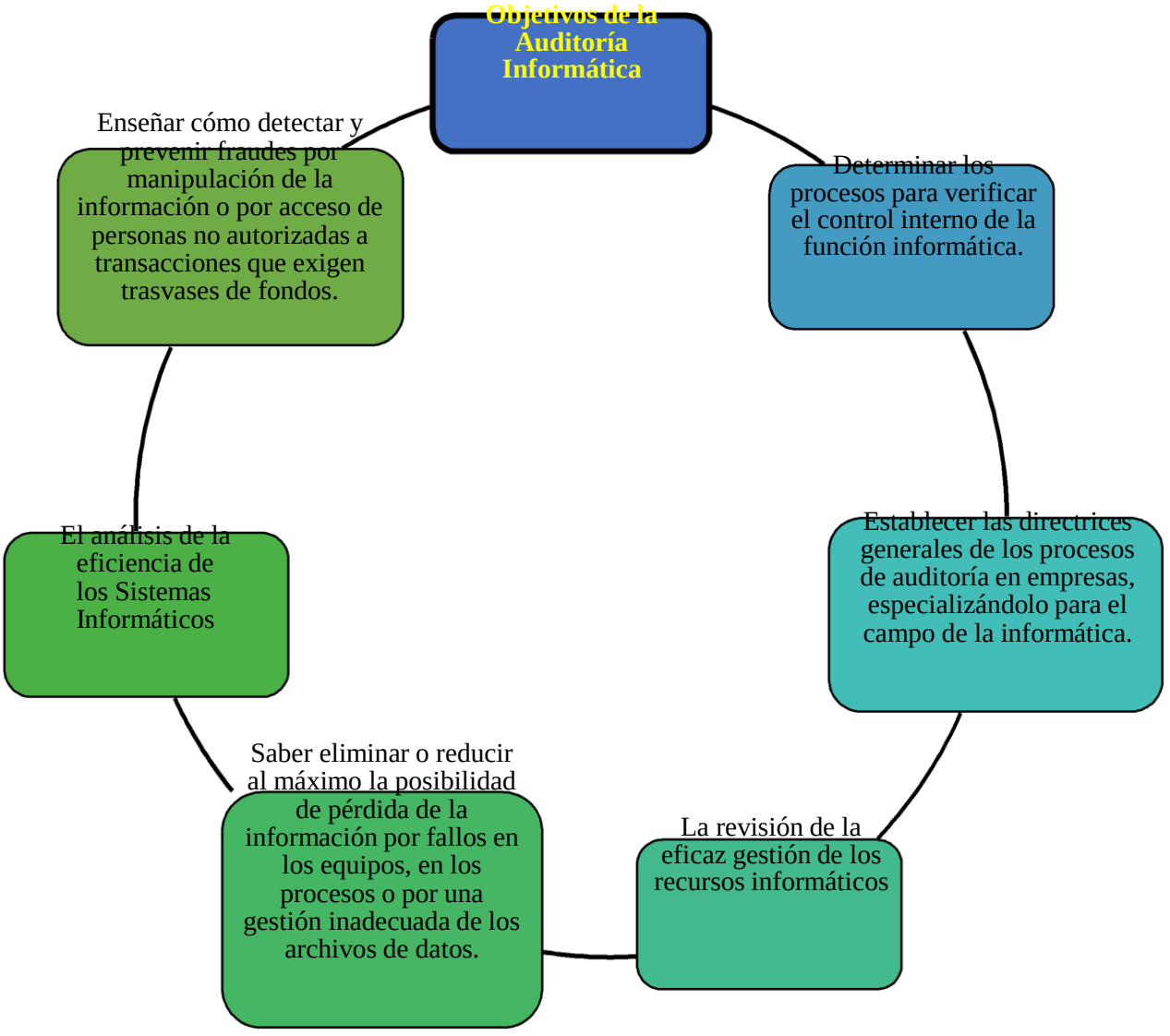

Figura 12. Objetivos de la Auditoría Informática
Fuente: el autor

3.7.3 Tipos de auditoría informática

Dentro de la auditoría informática destacan los siguientes tipos: (Piattini, 2011)

- **Auditoría de la gestión**: la contratación de bienes y servicios, documentación de los programas etc., al igual que la auditoría de sistemas[17] tiene como objetivo realizar un examen de evaluación de las actividades.

- **Auditoría de la base de datos:** Esta se encarga de monitorear, medir, asegurar y registrar los accesos a toda la información almacenada en las bases de datos.

Esta auditoría se encarga de manera fundamental en la seguridad de las bases de datos.

Entre sus objetivos se encuentran

- ✓ Evitar el acceso externo
- ✓ Imposibilitar el acceso interno a usuarios no autorizados
- ✓ Autorizar el acceso solo a los usuarios autorizados

- **Auditoría de la seguridad:** Referidos a datos e información verificando disponibilidad, integridad, confidencialidad, autenticación y no repudio.

Objetivos de una auditoría en seguridad:

- ✓ Evaluar la seguridad de los entornos
- ✓ Verificar el cumplimiento de políticas
- ✓ Identificar el compromiso de equipos por parte de intrusos o software malicioso.
- ✓ Elaboración de un informe para evaluar y de ser necesario modificar las políticas debe incluir recomendaciones y conclusiones.

- **Auditoría de la seguridad física**: referido a la ubicación de la organización, evitando ubicaciones de riesgo, y en algunos casos no revelando la situación física de esta.

También está referida a las protecciones externas (arcos de seguridad, circuito cerrado de televisión, vigilantes, etc.) y protecciones del entorno.

[17] Auditoría en Sistemas.- Establecer el grado de eficiencia, efectividad y economía de los sistemas informáticos en una organización y presentar conclusiones y recomendaciones encaminadas a corregir las deficiencias existentes y mejoradas tomadas.

- **Auditoría de la seguridad lógica**: comprende los métodos de autenticación de los sistemas de información.

- **Auditoría de redes:** Mecanismos que prueban una red informática, evaluando la seguridad y su desempeño, para lograr mayor eficiencia y aseguramiento de la información.

3.7.4 Fases de la auditoría de seguridad

Precisión de los objetivos y delimitación del alcance y profundidad de la auditoría, así como del período cubierto para el caso, por ejemplo, la revisión de accesos del último semestre; si no se especifica, los auditores deberán citar en el informe el período revisado, porque podría aparecer alguna anomalía anterior, incluso de hace mucho tiempo, y llegarse a considerar una debilidad de la auditoría.

- Análisis de posibles fuentes y recopilación de información, en el caso de los internos este proceso no puede existir.
- Determinación del plan de trabajo y en los recursos y plazos en caso necesario, si como de comunicación a la entidad.
- Adaptación de cuestionarios, y a veces consideración de herramientas o perfiles de especialistas necesarios, sobre todo en la auditoría externa.

3.7.5 Auditoría de la seguridad física

Se evaluará las protecciones físicas de los datos, programas, instalaciones, equipos, redes y soporte, y por supuesto habrá que considerar las medidas de evacuación para las personas como son: las alarmas, salidas alternativas, así como la exposición a riesgos superiores a lo considerado admisibles en la entidad e incluso en el sector.

“Existen diversas amenazas, pero para la seguridad física enfocado en una unidad educativa de nivel superior se puede presenciar accidentes naturales o de distinto tipo como: incendios, inundaciones, terremotos etc.” (Henríquez, 2011)

Algunos de los aspectos a considerar en la protección física:

- Ubicación del centro de procesos, de los servidores y en general de cualquier elemento a proteger.
- Estructura, diseño, construcción y distribución de los edificios y de sus pisos o plantas.
- Riesgos a los accesos físicos no controlados.
- Amenaza de fuego, problemas en el suministro eléctrico
- Evitar situaciones o sustracción de equipos, componentes, soportes magnéticos, documentación u otros activos.

3.7.6 Auditoría de la seguridad lógica

La seguridad lógica se refiere a la seguridad de uso de software, a la protección de los datos, procesos y programas, así como el acceso autorizado de los usuarios a la información.

"Es necesario verificar que cada usuario solo pueda acceder a los recursos que se autorice, y con las posibilidades que el propietario haya fijado: lectura, modificado, borrado y ejecución". (Piattini, 2011).

Aspectos a evaluar respecto a las contraseñas

- Quién asigna la contraseña inicial y sucesiva.
- Longitud mínima y composición de los caracteres.
- Vigencia, incluso puede haberlas de un solo uso o dependientes de una función.
- Número de intentos que se permiten al usuario.
- Controles existentes para evitar y detectar caballos de Troya[18]

[18] Caballo de Troya.- se denomina caballo de Troya, o troyano, a un software malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero que, al ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado

3.7.7 Auditoría de la seguridad y el desarrollo de aplicaciones

Cuando se busca evaluar la seguridad en la operación del software, se debe identificar las principales vulnerabilidades del software de la entidad, entre las cuales se menciona las siguientes:

- Errores de aplicaciones.
- Errores de sistemas operativos.
- Rutinas de acceso no autorizado.
- Servicios no autorizados.

3.7.8 Auditoría de la seguridad de datos

La protección de los datos puede tener varios enfoques respecto a las características de confidencialidad, disponibilidad e integridad. Puede haber datos críticos y de mayor importancia en cuanto a confidencialidad, como datos médicos, la contabilidad de una empresa, notas y sistemas de educación.

"Desde el origen del dato, que puede ser dentro o fuera de la entidad, y puede incluir preparación, autorización, incorporación al sistema: por el cliente, por empleados o usuarios, y debe revisarse como se verifican los errores." (Villalobos, 2008)

- ✓ **Proceso de los datos:** Controles de validación, integridad, almacenamiento: que existan copias suficientes, sincronizadas y protegidas.

- ✓ **Salida de resultados:** controles en transmisiones, en impresión, en distribución.

- ✓ **Retención de la información y protección en función de su clasificación:** destrucción de los diferentes soportes que la contengan cuando ya no sea necesaria.

- ✓ **Cliente-Servidor:** es necesario verificar los controles punto a punto, y no solo de una central como en otros sistemas, y la posibilidad de transferencia de ficheros o de captación y exportación de datos que pueden perder sus protecciones al pasar de una plataforma a otra. Los datos son la parte fundamental de los sistemas informáticos por tanto estos deben ser bien cuidados y manejados. La protección de la integridad,

disponibilidad y confidencialidad de los mismos debe ser el objetivo principal de todo sistema de seguridad informático.

Con esta auditoría se busca:

- Monitorear y mantener un registro del uso de los datos por los usuarios autorizados y no autorizados.
- Permitir investigación.
- Alertas en tiempo real.

Evaluar el estado de control existente

- Problemas por seguridad en instalaciones y el acceso físico[19]
- Riesgo relacionado a los accesos lógicos y privacidad de las bases de datos
- Relación entre sistema operativo[20]
- Riesgo relacionado a las aplicaciones y utilitarios utilizados por la organización.

3.7.9 Auditoría de la seguridad en comunicaciones y redes

En las políticas de la entidad debe reconocerse que los sistemas, redes y mensajes transmitidos y procesados son propiedad de la entidad y no deben usarse para otros fines no autorizados, por seguridad y productividad.

Los usuarios tendrán restricción de acceso según dominios, únicamente podrán cargar los programas autorizados, y solamente podrán variar las configuraciones y componentes los técnicos autorizados. (Lauces, 2016)

Internet e intranet: Separación de dominios e implementación de medidas especiales, como normas y cortafuegos (firewall)[21], y no solo en relación con la seguridad sino por accesos no justiciados a páginas donde permitan el ingreso de ciertos vínculos o link.

---

[19] Acceso Físico.- Problemas de seguridad en base de datos es fundamental tener una computadora de gran capacidad de almacenamiento con características avanzadas para que no haya errores y lentitud al momento de validar gran cantidad de información con múltiples registros.

[20] Sistema Operativo.- es el programa o software básico de un ordenador. Es una plataforma que facilita la interacción entre el usuario y los demás programas del ordenador y los dispositivos de hardware.

[21] Firewall.- Es un dispositivo que funciona como cortafuegos entre redes, permitiendo o denegando las transmisiones de una red a la otra. Un uso típico es situarlo entre una red local y la red Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial.

Correo electrónico: Tanto por privacidad, y por seguridad (PGP Pretty Good Privacy) [22] es muy utilizado actualmente, permite que el uso del correo sea adecuado y no utilizado para fines particulares.

Protección de programas: Para la prevención del uso no autorizado de programas propiedad de la entidad o de los que tengan licencia.

Control sobre las páginas Web[23]: Quien puede modificarla y desde donde, también los riesgos que pueden existir en el comercio electrónico

Vulnerabilidades de comunicaciones: inadecuados controles de acceso a la red e incorrectos mecanismos para prevenir fallas en comunicaciones.

3.7.10 Fuentes de la auditoría

Las fuentes estarán relacionadas con los objetivos, y entre ellas pueden estar:

- Políticas, estándares, normas y procedimientos.
- Planes de Seguridad.
- Documentación de Aplicaciones.
- Topología de redes.
- Planos de instalaciones.
- Archivos.
- Programas.
- Base de Datos.
- Documentos de planes de continuidad y sus pruebas.

3.7.11 Pruebas y herramientas para la auditoría informática

En la realización de una auditoría informática el auditor puede realizar las siguientes pruebas:

✓ **Pruebas sustantivas**: Verifican el grado de confiabilidad del Sistema de Información del organismo. Se suelen obtener mediante observación, cálculos, muestreos, entrevistas,

[22]PGP.-es un sistema de encriptación por llave pública escrito por Philip Zimmermann, y sirve para que nadie salvo uno mismo y el destinatario o destinatarios a los que vaya dirigido el mensaje puedan leerlo al ir los mensajes codificados

[23] Web.-página electrónica, página digital, o ciberpágina es un documento o información electrónica capaz de contener texto, sonido, vídeo, programas, enlaces, imágenes y muchas otras cosas, adaptada para la llamada World Wide Web (WWW)

técnicas de examen analítico, revisiones y conciliaciones. Verifican asimismo la exactitud, integridad y validez de la información. (Derrien, 2011)

✓ **Pruebas de cumplimiento**: verifican el grado de cumplimiento de lo revelado mediante el análisis de la muestra. Proporciona evidencias de que los controles claves existen y que son aplicables efectiva y uniformemente.

Las principales herramientas de las que dispone un auditor informático son:

- Observación
- Realización de cuestionarios
- Entrevistas a auditados y no auditados.
- Muestreo estadístico
- Flujogramas
- Lista de chequeos
- Mapas conceptuales

3.8 Normas y/o Estándares Internacionales

3.8.1 COBIT

Los controles COBIT son un modelo autoritario internacional para el uso diario en esquemas de control y auditoría. Es el modelo actualmente utilizando por los miembros del ISACA[24] a nivel mundial desde 1992.

COBIT fue desarrollado como un estándar generalmente aplicable y aceptado para la práctica del control de la Tecnología Informática (TI)[25].

[24] ISACA.- fue fundada en el año 1967 cuando un grupo de auditores en sistemas informáticos percibieron la necesidad de centralizar la fuente de información y metodología para el área de operación, es una asociación internacional que apoya y patrocina el desarrollo de metodologías y certificaciones para la realización de actividades de auditoría y control en sistemas de información.

[25] TI.- Asociación de la Tecnología Informática de América (ITAA), es: el estudio, diseño, desarrollo, innovación puesta en práctica, ayuda o gerencia de los sistemas informáticos computarizados, particularmente usos del software y hardware». En general, del uso de computadoras y del software electrónico, así como de convertir, almacenar, proteger, procesar, transmitir y de recuperar la información.

Está basado en los objetivos de control existentes de la ISACA mejorados con los estándares internacionales existentes y emergentes técnicos, profesionales, reguladores y específicos de la industria o empresas ayudando a reducir sus perfiles de riego a través de la adecuada administración de la seguridad. La información específica y las tecnologías relacionadas son cada vez más esenciales para las organizaciones, pero la seguridad de la información es esencial para la confianza de las mismas empresas, organizaciones y usuario final. (ISACA & Bernabe, COBIT 5: PROCESOS CATALIZADORES, 2012).

Las organizaciones deben cumplir con requerimientos de calidad, de seguridad tanto para su información, como para sus activos. La administración deberá obtener un balance adecuado en el empleo de recursos disponibles, los cuales incluyen: personal, instalaciones, tecnología, sistemas de aplicación y datos.

Para cumplir con lo anteriormente expuesto, así como para alcanzar las expectativas, la administración deberá establecer un sistema adecuado de control interno.

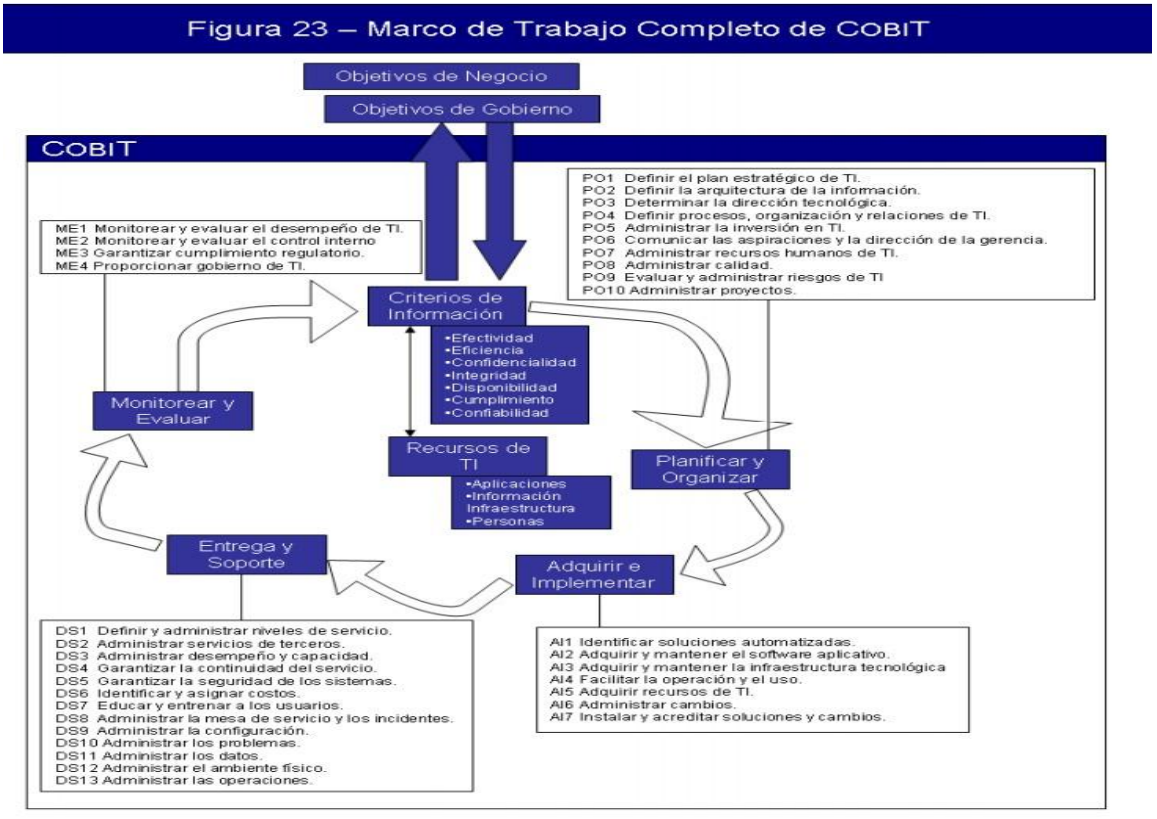

Figura 13. Marco de trabajo completo de COBIT
Fuente: Guía Gobernanza IT COBIT

Por lo tanto, este sistema de control deberá existir para proporcionar soporte a los procesos de negocio y debe ser preciso en la forma en la que cada actividad individual de control satisface los requerimientos de información y puede impactar en los recursos de TI.

El impacto de los recursos de TI es resaltado en el marco referencial de COBIT conjuntamente a los requerimientos de información del negocio que deben ser alcanzados: Efectividad, Eficiencia, Confidencialidad, Integridad, Disponibilidad, Cumplimiento y confiabilidad.

El control, que incluye estructuras, prácticas, políticas y procedimientos organizacionales, es responsabilidad de la administración.

COBIT presenta los siguientes beneficios

- Incrementar los niveles de confianza
- Beneficiarse de recomendaciones basadas en mejores prácticas a través de auditorías.
- Identificar riesgos.
- Administración correcta de los recursos.
- Medir el desempeño.
- Llegar al cumplimiento de metas.

3.8.1.1 Dominios de control de nivel

COBIT, posee 34 objetivos de control de alto nivel, uno para cada uno de los procesos de TI, agrupados en 4 dominios que son:

Planeación y organización: este dominio cubre las estrategias y las tácticas, se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos del negocio. Además, la consecución de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, se deberá establecer una organización y una infraestructura tecnológica apropiada. (ISACA, COBIT 4.1, 2008)

Adquisición e implementación: "Para llevar a cabo la estrategia de TI, las soluciones de TI deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además este dominio cubre los cambios y el mantenimiento realizado a sistemas existentes."

Entrega o soporte: "En este dominio se hace referencia a la entrega o distribución de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por la seguridad en los sistemas y la continuidad de las operaciones así como aspectos sobre entrenamiento. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios."

Monitoreo: "este dominio incluye el procesamiento de los datos el cual ejecutado por los sistemas de aplicación, frecuentemente clasificados como controles de aplicación."

Todos los procesos necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control.

"Es importante tener en cuenta que estos procesos de TI pueden ser aplicados en diferentes niveles de organización, unos pueden ser aplicados al nivel de la empresa, otros a nivel de la función de TI, otros al nivel del propietario de los procesos de negocio, etc"

3.8.2 ISO 27002

La ISO 27002 es para la seguridad de la información lo mismo que la ISO 27000: es una norma redactada por los mejores especialistas del mundo en el campo de seguridad de la información y su objetivo es proporcionar una metodología para la implementación de la seguridad de la información en una organización.

También permite que una organización sea certificada, lo cual significa que la entidad de certificación independiente ha confirmado que la seguridad de la información se ha implementado en esa organización de la mejor forma posible.

"La norma ISO define como organizar la seguridad de la información en cualquier tipo de organización, con o sin fines lucros, privada o pública, pequeña o grande. Es posible afirmar que esta norma constituye la base para la gestión de la seguridad de la información". (ISO, 2013)

A raíz de la importancia de la norma ISO 27002, muchas legislaturas han tomado esta norma como base para confeccionar las diferentes normativas en el campo de protección de datos personales, protección de información confidencial, protección de sistemas de información, gestión de riesgos operativos en instituciones financieras, educativas, públicas etc.

Figura 14. Dominio de la norma ISO 27002:2005
Fuente: Tomada del sitio Web oficial https://www.iso.org/

"La norma ISO 27002 determina como gestionar la seguridad de la información a través de un sistema de gestión de seguridad de la información. Un sistema de gestión de este tipo, igual que las normas ISO 27000 y la versión 14001, está formado por cuatro fases que se deben implementar en forma constante para reducir al mínimo los riesgos sobre confidencialidad,

integridad y disponibilidad de la información.” (ISACA & Cerezo, Soportando y Auditando La Gestion De La Continuidad Del Negocio Por Normas ISO, 2013)

3.8.2.1 Dominios y estándar de seguridad según la ISO

El estándar ISO 27002:2005 propone una serie de controles de seguridad para un sistema de gestión de la información (SGSI). Está diseñado para satisfacer los requerimientos identificados, mediante un análisis de riesgos.

Incluye 11 cláusulas de control de seguridad o secciones diseñadas para ser implantados y que satisfagan los requerimientos de seguridad identificados por una gestión de riesgos. Cada categoría incluye un objetivo de control y uno o varios controles aplicables para lograrlo.
Las cláusulas que define el estándar son las siguientes:

1) **Política de seguridad (1 categoría, 2 controles).**

Brinda un lineamiento de implementación del documento de la política de seguridad, así como la revisión del mismo.

2) **Organización de la seguridad de la información (2 categorías, 11 controles).**

Fija un marco referencial para el manejo de la seguridad, tanto una organización interna, como hacia terceros.

3) **Gestión de activos (2 categorías, 5 controles).**

Establece responsabilidades sobre los activos, así como su clasificación.

4) **Seguridad de recursos humanos (3 categorías, 9 controles).**

Brinda una serie de controles a implantar antes, durante y en el cese o cambio de personal.

5) **Seguridad física y ambiental (2 categorías, 13 controles).**

Indica medidas para establecer áreas seguras y la protección de equipo.

6) **Gestión de comunicaciones y operaciones (10 categorías, 32 controles).**

Garantiza una apropiada operación de los medios de procesamiento de la información, como protección contra código malicioso, copias de seguridad, seguridad en redes, entre otros.

7) Control de acceso (7 categorías, 25 controles).

Gestiona el control de acceso de usuarios, a la red, al sistema operativo, aplicaciones y equipo fuera de sitio.

8) Adquisición, desarrollo y mantenimiento de sistemas de información (6 categorías, 16 controles).

Brinda los requisitos de seguridad necesarios para los sistemas de información.

9) Gestión de incidentes de seguridad de la información (2 categorías, 5 controles).

Indica controles a implantar en el caso de eventos relacionados con la seguridad.

10) Gestión de la continuidad del negocio (1 categoría, 5 controles).

Establece controles a aplicar en caso de una suspensión de las actividades comerciales, así como su protección. También brinda lineamientos para la implementación de planes de continuidad.

11) Conformidad (3 categorías de seguridad, 10 controles).

Para el cumplimiento de requerimientos legales, de políticas y normas. También establece ciertas consideraciones para realizar auditorías a los sistemas de información.

3.8.2.2 Fases o etapas de la Norma ISO

Para elaborar un plan de seguridad o políticas se debe inicializar por el ciclo PDCA[26], ciclo de Deming o ciclo de mejora continua es uno de los temas que con más frecuencia aparece en el mundo moderno de TI, tanto así que se ha ido incorporando a la definición de estándares y mejores prácticas como ISO-27002:2005, las siguientes fases son: (ISO, 2013)

[26] PDCA.- Se trata de una estrategia de mejora continua difundida por Edwards Deming en la década de 1950, con base en las definiciones hechas por Walter A. Shewart en los años 30, y que describe cuatro pasos básicos para lograr la mejora: Plan, Do, Check y Act.

La fase de planificación: "esta fase sirve para planificar la organización básica y establecer los objetivos de la seguridad de la información y para escoger los controles adecuados de seguridad (la norma contiene un catálogo de 133 posibles controles)."

La Fase de implementación: "esta fase implica la realización de todo lo planificado en la fase anterior[27]"

La fase de revisión: "el objetivo de esta fase es monitorear el funcionamiento del SGSI[28] mediante diversos canales y verificar si los resultados cumplen los objetivos establecidos."

La fase de mantenimiento y mejora: "el objetivo de esta fase es mejorar todos los incumplimientos detectados en la fase anterior.

El ciclo de las cuatro fases nunca termina, todas las actividades deben ser implementadas clínicamente para mantener la eficacia del SGSI."

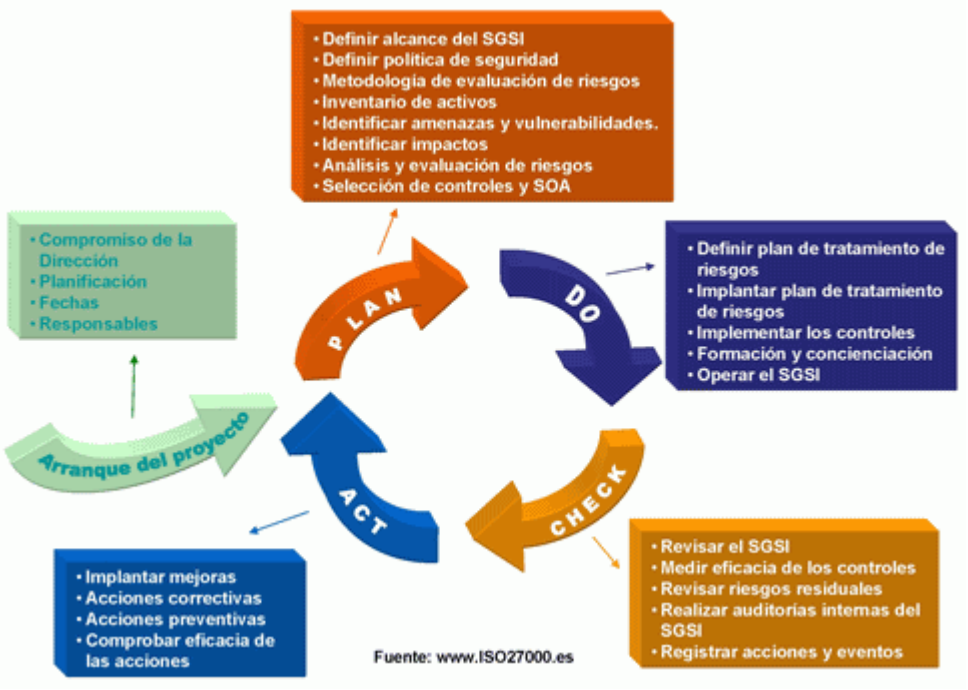

Figura 15. Ciclo de Deming ISO 27001/27002
Fuente: Tomado de la página oficial https://www.iso.org/

[27] Se realiza un estudio de todo el negocio u organización, para la implementación de mejora continua o establecer los primeros mecanismos de seguridad.

[28] SISG.- (Sistema de Gestión de Seguridad de la Información) es el concepto central sobre el que se construye ISO 27001. La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización, Este proceso es el que constituye un SGSI, que podría considerarse, por analogía con una norma tan conocida como ISO 9001, como el sistema de calidad para la seguridad de la información.

3.8.3 ITIL (Biblioteca de Infraestructuras de Tecnologías de Información)

Es un conjunto de conceptos y prácticas para la gestión de servicios y el desarrollo de tecnologías de la información y las operaciones relacionadas con la misma en general. ITIL da descripciones detalladas de un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI.

"Estos procedimientos son independientes de proveedor y han sido desarrollados para servir como guía que abarque toda infraestructura, desarrollo y operaciones de TI". (Medina & Rico, 2012)

Esta metodología es la más aceptada para la gestión de servicios de tecnologías de información en todo el mundo, ya que es una recopilación de las mejores prácticas tanto del sector público como del sector privado. Estas mejores prácticas se dan en base a toda la experiencia adquirida con el tiempo en determinar actividad, y son soportadas bajo esquemas organizacionales complejos; pero a su vez bien definidos y que se apoyan en herramientas de evaluación e implementación.

"ITIL como metodología propone el establecimiento de estándares que ayudan al control, operación y administración de los recursos (ya sean propios o de los clientes). Plantea hacer una revisión y restructuración de los procesos existentes en caso de que estos lo necesiten (si el nivel de eficiencia es bajo o que haya una forma más eficiente de hacer las cosas), lo que nos lleva a una mejora continua." (Van & Kolthof, 2008)

Figura 16. Mapa de Proceso de ITIL
Fuente: ITIL V3, p.12

3.8.3.1 Áreas a las que se dirige ITIL

ITIL, ofrece guías para la administración de los procesos de TI relacionado a:

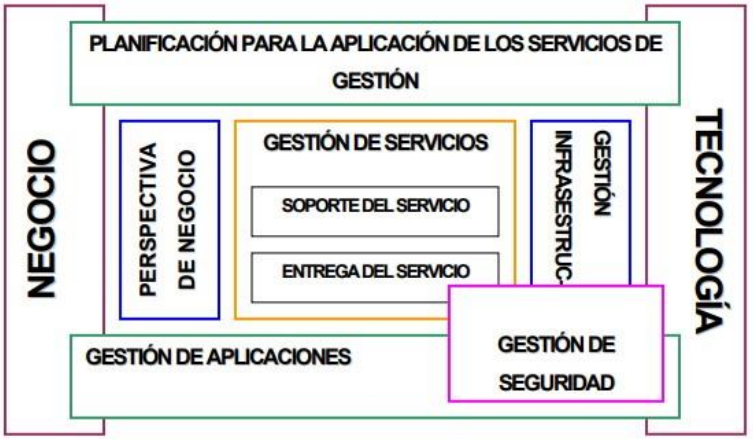

Figura 17. Área general de ITIL en TI
Fuente: Tomado, Pía Ramírez. P.12 2008

3.8.3.2 Ciclo de vida de útil

El ITIL posee una serie de conceptos y herramientas de gestión de prestación de servicios, principalmente de tecnologías de la información, y las operaciones relacionadas con ellas. Esta forma de afrontar la gestión no es un manual que se ha de seguir al pie de la letra, ITIL no es rígido en cuanto en su implementación, por lo que se pueden adoptar los aspectos o funcionalidades que se adapten mejor a nuestro tipo de proyectos y permita optimizar su gestión.

El ciclo de vida de ITIL[29] se puede desglosar en las siguientes fases:

Estrategia: propone un enfoque de la gestión como una capa estratégica de la compañía, que deja de ser simplemente una burocracia de cumplimentar o acatar. (Van & Kolthof, 2008)

Diseño: cubre los principios y métodos necesarios para transformar los objetivos estratégicos en portafolios de servicios y activos. (Van & Kolthof, 2008)

[29] Ciclo de Vida ITIL.- la implantación del modelo de gestión persigue una mejora en los ciclos de gestión dentro de la compañía, A través de las mejores prácticas de ITIL se orienta hacia el servicio Normalmente en el ámbito de TI se genera una jerarquía concreta, se vuelve más eficaz, y se focaliza en los objetivos de la organización.

Transición: se trata del proceso de transición para la implementación de nuevos servicios o de su mejora. (Van & Kolthof, 2008)

Operación: cubre las mejores prácticas para la gestión rutinaria. (Van & Kolthof, 2008)

Mejora Continua: corresponde a un procedimiento mediante el cual se crea y mantiene del valor ofrecido a los clientes a través de un diseño, transición y operación del servicio optimizado. (Van & Kolthof, 2008)

3.8.3.3 ITIL Modelo Integral

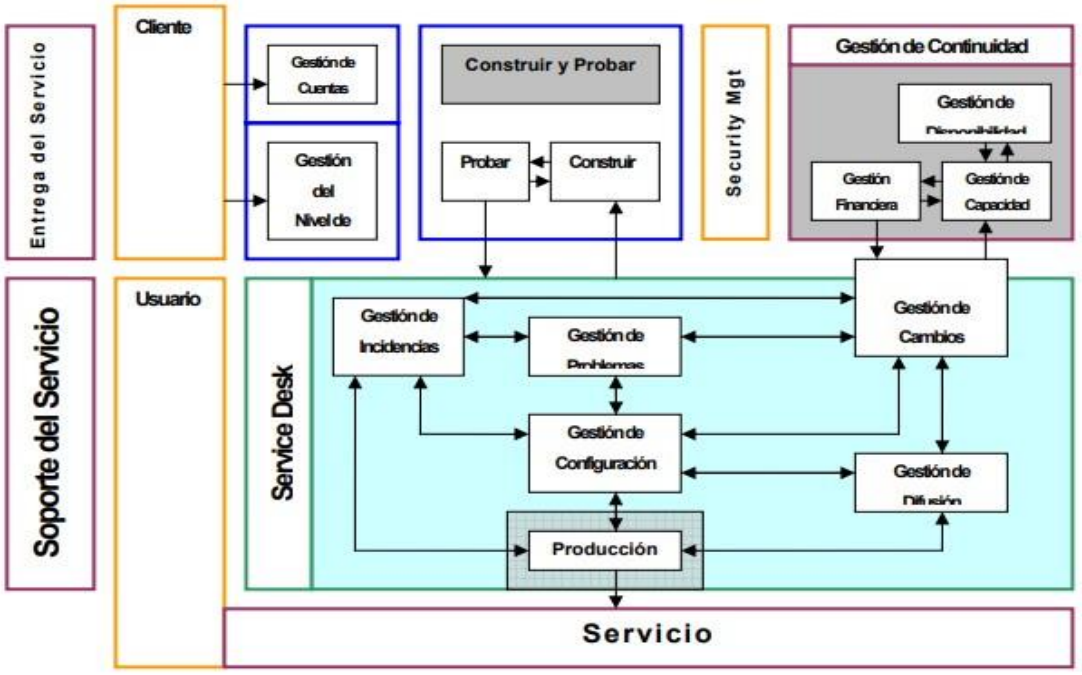

Figura 18. Modelo Integral dentro del proceso de Service Desk ITIL
Fuente: Tomado, Pía Ramírez. P.41 2008

Es importante darse cuenta de que la organización o compañía puede aplicar cualquiera de estos procesos, independientemente de todos los otros. Aunque ellos tengan múltiples interrelaciones y estas no estén invertidas, cada proceso trae beneficios por sí mismo por ejemplo, como un punto de partida, la organización puede verse beneficiada de aplicar solamente el proceso de la gestión del cambio (Van & Kolthof, 2008).

3.9 Comparativo de las Normas y/o Estándares Internacionales

A continuación se realizará un comparativo de los modelos COBIT, ITIL e ISO-IEC 27002 basado en las funciones, las áreas de cobertura, la organización que creo el modelo, para que se implementa y quienes los orientan (evaluadores)[30].

Es importante concluir que un modelo no será mejor que otro, debido a que inicialmente hay que evaluar la pertinencia, la cobertura (áreas) y ante todo que cada organización cada empresa tiene su particularidad, por ende lo importante será adoptar un modelo pertinente, tomar los elementos que sean aplicables y adaptar el modelo de referencia para generar un modelo propio de la empresa.

ÁREA	COBIT	ITIL	ISO-IEC 27002
Funciones	Mapeo de procesos IT	Mapeo de la gestión de niveles de Servicio	Marco de referencia de la seguridad de la información
Áreas Creador	4 Procesos y 34 Dominios ISACA	9 Procesos OGS	10 Dominios ISO International Organization for Standardization
¿Para qué se Implementa?	Auditoria de Sistemas de Información	Gestión de Niveles de Servicio	Cumplimiento de estándar de seguridad
¿Quiénes lo Evalúan?	Compañías de Contabilidad Compañías de consultoría en IT	Compañías de Consultoría en IT	Compañías de Consultoría en IT, Empresas de Seguridad Consultores de Seguridad en redes

Tabla 7: Tabla de Comparación de modelos de Normas y SGSI
Fuente: Elaboración Propia

[30] Evaluadores se los conoce también como auditores informáticos estos pueden ser internos o externos donde hacen un estudio y planificación para la agilización del proceso y verificar fallas.

4. DESARROLLO DEL PROYECTO

4.1 Análisis de la situación actual del Instituto Tecnológico Superior Sudamericano Quito

Para realizar el diseño de las políticas de seguridad basado en la norma ISO/IEC 27002:2005 se analizó en que porcentajes y que estándares de seguridad se debe implementar, la versión 2005 nos guía al control de las buenas prácticas, a continuación se muestra la tabla de la situación inicial.

1. POLÍTICAS DE SEGURIDAD	**RESPUESTA**	**PORCENTAJE**
1.1 Existen documentos de políticas de seguridad de sistemas de información	NO	0%
1.2 Existe normativa relativa a la seguridad de los Sistemas de Información	NO	0%
1.3 Existen procedimientos relativos a la seguridad de Sistemas de Información	NO	0%
1.4 Existe un responsable de las políticas, normas y procedimientos	NO	0%
1.5 Existen controles regulares para verificar la efectividad de las políticas	NO	0%
2. ORGANIZACIÓN DE LA SEGURIDAD	**RESPUESTA**	**PORCENTAJE**
2.1 Existen roles de responsabilidades definidos para las personas implicadas en la seguridad	NO	0%
2.2 Existe un responsable encargado de evaluar la adquisición y cambios de sistemas de información	NO	0%
2.3 Existen programas de formación en seguridad para los empleados, clientes y terceros	NO	0%
2.4 existe un acuerdo de confidencialidad de la información que se accede	NO	0%
2.5 se revisa la organización de la seguridad periódicamente por empresa externa	NO	0%
3. ADMINISTRACIÓN DE ACTIVOS	**RESPUESTA**	**PORCENTAJE**
3.1 Existen inventario de activos actualizados	SI	20%
3.2 El inventario contiene activos de datos, software, equipos y servicios	SI	20%
3.3 Se dispone de una clasificación de la información según la criticidad de la misma	NO	0%
3.4 Existe un responsable de los activos	SI	20%
3.5 Existen procedimientos para clasificar la información	NO	0%

1. SEGURIDAD DE LOS RRHH	RESPUESTA	PORCENTAJE
4.1 Se tienen definidas responsabilidades y roles de seguridad	NO	0%
4.2 Se tiene en cuenta la seguridad en la selección y baja de personal	NO	0%
4.3 Se plasma las condiciones de confidencialidad y responsabilidades en los contratos	NO	0%
4.4 Se imparte la información adecuada de seguridad y tratamientos de activos	NO	0%
4.5 Se recogen los datos de los incidentes de forma detallada	SI	20%
5. SEGURIDAD FÍSICA Y DEL AMBIENTE	**RESPUESTA**	**PORCENTAJE**
5.1 Existe perímetros de seguridad física (una pared, Puerta con llave).	SI	20%
5.2 Existe controles de entrada para protegerse frente a acceso de personal no autorizado	SI	20%
5.8 Existe seguridad en el cableado frente a daños e intercepciones	SI	20%
5.9 Se asegura la disponibilidad e integridad de todos los equipos	NO	0%
5.10 Existe algún tipo de seguridad para los equipos retirados o ubicados exteriormente	NO	0%
6. GESTIÓN DE COMUNICACIONES Y OPERACIONES	**RESPUESTA**	**PORCENTAJE**
6.1 Todos los procedimientos operativos identificados en la política de seguridad han de estar documentados	NO	0%
6.2 Existe algún método para reducir el mal uso accidental o deliberado de los sistemas	NO	0%
6.3 Realizar copias de Backup de la información esencial para el negocio	SI	20%
6.4 Existen rastro de auditoria	NO	0%
6.5 Existen medidas de seguridad en el comercio electrónico (Web)	NO	0%
7. CONTROL DE ACCESOS	**RESPUESTA**	**PORCENTAJE**
7.1 Existe un procedimiento formal de registro y baja de acceso	NO	0%
7.2 Existe una gestión de los password de usuario	SI	20%
7.3 Se protege el acceso de los equipos desatendidos	SI	20%
7.4 Existen políticas de limpieza en el puesto de trabajo	NO	0%
7.5 Existe una política de uso de los servicios y conexión de red	NO	0%
8. ADMINISTRACIÓN DE INCIDENTES	**RESPUESTA**	**PORCENTAJE**
8.1 Se comunica los eventos de seguridad	NO	0%
8.2 Se comunica las debilidades de seguridad	NO	0%
8.3 Existe la gestión de incidentes	NO	0%
9. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	**RESPUESTA**	**PORCENTAJE**
9.1 Existe un Plan de Continuidad del Negocio y Análisis del Riesgo	NO	0%
10. CUMPLIMIENTO	**RESPUESTA**	**PORCENTAJE**
10.1 Se tiene control sobre plataformas tecnológicas para la organización	NO	0%

10.2 Existe un área encargada que valide el nivel de cumplimiento de las políticas	NO	0%
11.3 Existe Auditorias físicas o digitales para el control y cumplimiento	NO	0%

Tabla 8: Situación actual del Instituto Tecnológico Sudamericano Quito.
Fuente: el autor

4.2 Ataques de red

En el instituto no disponen de herramientas destinadas exclusivamente para prevenir los ataques de red, en principio debido a que no se han presentado hasta el momento, problemas en este sentido. No hay herramientas para detección de intrusos. **Ver Documento de Políticas de Seguridad.**

4.3 Contraseñas

El manejo de contraseñas de todos los equipos está a cargo del Administrador del Área de Sistemas. **Ver Documento de Políticas de Seguridad.**

4.4 Seguridad de base de datos

El instituto no cuenta con un sistema de base datos, por el momento está en desarrollo para el registro y el almacenamiento de calificaciones o información académica de los estudiantes y docentes, es fundamental y necesario ya que es una herramienta principal.

Una vez implementado se sugiere aplicarlo en un servidor Ubuntu o cualquier sistema operativo Linux, mediante el panel de control webmin[31] todo depende de la organización y estructuración del planteamiento del Director o encargado del Área de Sistemas .

La única persona que pueda tener acceso a los archivos de la base de datos debe ser el Administrador de Sistemas o encargado del Instituto, una vez implementada se necesita una auditoría para evitar problemas de entrada y salida de información, problemas en guardar registros, confidencialidad y determinar usuarios que van a acceder a la base de datos. **Ver Documento de Políticas de Seguridad.**

[31] Webmin.-es una interfaz web escrita en Perl para administrar un servidor. Con esta herramienta se pueden configurar los permisos para Usuarios y Grupos o configurar el funcionamiento de nuestro Mysql Server, cuotas de espacio, servicios, archivos de configuración, apagado del equipo, etc.

Webmin tiene una estructura por módulos para administrar una amplia variedad de herramientas como Apache, PHP, MySQL, DNS, Samba, DHCP, etc, además de ser completamente configurables y de poder crear nuevos.

4.5 Control de aplicaciones en PC'S

Actualmente ningún estudiante o usuario puede instalar aplicaciones en las pc de los laboratorios del instituto, en caso de requerir instalar una nueva aplicación se debe dar a conocer la necesidad de la misma y luego solicitar al Encargado de Sistemas o Administrador la instalación respectiva.

No hay estándares definidos, procedimientos a seguir y no existe documentación respecto a la instalación y actualización de la configuración de las estaciones de trabajo, la actualización del software es al finalizar cada semestre. **Ver Documento de Políticas de Seguridad.**

4.6 Control de acceso físico al centro de cómputo

El servidor se encuentra ubicado en los laboratorios del 3ro y 4to piso, el único servidor que cuenta es el servidor Gateway que encuentra en el 4to piso de la Institución para su ingreso cuenta con una puerta de seguridad que está bajo llave, ninguna persona puede insertar cualquier dispositivo, flash memory para alterar su funcionamiento. **Ver Documento de Políticas de Seguridad.**

4.7 Control de acceso a los equipos

Dispositivos con entradas a lectoras de memorias micro SD, USB, y lectoras de CD están habilitadas y no hay ningún control sobre ellos, no se hacen controles automáticos de virus ni se prohíbe el booteo desde estos dispositivos, en los laboratorios se encuentra permitido hacia los estudiantes de la Escuela de Sistemas de Automatización para las prácticas de la Institución.

En la parte administrativa se recomienda tomar medidas sobre estos puntos detallados, ya que es el área donde más vulnerabilidades de archivos pueden presentar, se recomienda la adquisición o compra de un router exclusivo para mayor seguridad y no exista el robo o manipulación de información interna o externamente.

Se realizan controles sobre los dispositivos de hardware instalados al finalizar cada ciclo académico es decir cada clase es responsabilidad de cada docente que utiliza los laboratorios la revisión de los periféricos estén completos y que las PC no se abran. **Ver Documento de Políticas de Seguridad.**

4.8 Estructura del edificio

El Instituto funciona actualmente en un edificio de 5 pisos tomando en cuenta el subsuelo, donde el primer piso corresponde a la parte administrativa los 3 pisos restantes corresponden a laboratorios y aulas. No se tomó en cuenta el diseño e infraestructura de la red y no se tomó en cuenta las condiciones de seguridad. **Ver Documento de Políticas de Seguridad.**

4.9 Dispositivos de soporte

En el Instituto no disponen del equipamiento informático adecuado, por ejemplo, aire acondicionado, UPS, instalaciones eléctricas con descarga a tierra. **Ver Documento de Políticas de Seguridad.**

4.10 Cableado estructurado

El instituto cuenta con sus respectivas canaletas en toda la infraestructura del edificio, tanto como una buena distribución del cable de red hacia los ordenadores.

Cuando hay caídas se repara una vez detectado para cumplir las normas se necesita una área de IT, personal encargado solo al monitoreo de la red, políticas y vulnerabilidades que se puedan presentar o mejorar. **Ver Documento de Políticas de Seguridad.**

4.11 Mantenimiento

Solicitud de mantenimiento: cada vez que los usuarios necesitan asesoramiento o servicios del área de tecnologías, se comunican verbalmente con el encargado de sistemas explicando la situación. Cada requerimiento no se registra en ningún documento físico o digital.

Mantenimiento preventivo: si existe planificación para realizar mantenimiento preventivo y correctivo de los equipos informáticos, a nivel general del instituto este proceso se realiza al finalizar cada semestre pero no existe una bitácora de registro de incidentes o fallos si se presentara en algún computador a nivel general. **Ver Documento de Políticas de Seguridad.**

4.12 Instaladores

Los instaladores de las aplicaciones que utiliza el instituto se encuentran en sus respectivos CD' s y Memorias USB o formato ISO. **Ver Documento de Políticas de Seguridad.**

4.13 Licencias

Actualmente el instituto no cuenta con licencias del software de antivirus, el resto tanto de sistemas operativos como ofimática es ilegal en Windows, la mayoría en licencias libres son en distribución Linux. **Ver Documento de Políticas de Seguridad.**

4.14 Back up

Cuando se hace un cambio de la configuración del servidor, no se guardan copias de las configuraciones anteriores y posteriores al cambio, ni se documentan los cambios que se realizan ni la fecha de estas modificaciones.

No hay ningún procedimiento formal para la realización ni la recuperación del back ups.

EL proceso de back ups es manual no automático y lo realiza el encargado de sistemas, cada semestre los datos almacenados en las estaciones de trabajo. **Ver Documento de Políticas de Seguridad.**

4.15 Documentación

No existe documentación de licencias de software, direcciones ip's, diagramas físicos de los equipos y red. **Ver Documento de Políticas de Seguridad.**

5. CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- Se estableció políticas de seguridad como una guía para trabajar y minimizar los riesgos asociados a los activos, reduciendo impactos y pérdida de información originado por la falta de políticas de seguridad informática.

- Se analizó los activos de información y la situación actual del Instituto con respecto a la seguridad de la información, refleja índices de riesgos, los cuales exponen a la información a daños y modificaciones que pueden causar un impacto negativo dentro de las actividades.

- Se determinó y proyectó que la Institución tome acciones que permitan prevenir y detectar oportunamente vulnerabilidades a las que están expuestas la información; por lo tanto, se identificaron y clasificaron los activos aplicando la metodología de MAGERIT, y su implementación bajo la norma ISO 27002:2005 que permite mejorar la confidencialidad, integridad y disponibilidad de la información.

- Se diseñó la presente investigación e implementación están destinadas se destinó a la mejora continua de la SGSI, por tanto, la seguridad total nunca concluye, pero gestionar controles de seguridad en el proceso y manejo de la información se vuelve un complemento esencial, pues permite asegurar información valiosa no solo de la Institución sino también de los estudiantes.

5.2 Recomendaciones

- Se recomienda realizar campañas o inducciones de concientización sobre la importancia de la seguridad de la información, esta campaña será dirigida a todo el personal administrativo y docente del Instituto Tecnológico Superior Sudamericano Quito.

- Se recomienda contratar personal técnico cuya función sea administrar, revisar, monitorear y dar seguimiento periódico a los controles, se debe mantener un control estricto de acceso a los programas, para evitar copia, modificación o divulgación de la información.

- Es necesario controlar la implementación de software en los sistemas operativos para minimizar el riesgo de corrupción y fuga de información. Los estudiantes deberán tener acceso únicamente a la información que necesiten, todo cambio debe tener una aprobación previa.

- Es importante que se realice pruebas piloto para verificar si no tiene fugas o pérdida de información en la base de datos o sistema de registro académico que se implementará en el Instituto Tecnológico Superior Sudamericano Quito.

- Se recomienda que todo el personal administrativo y docente se maneje con correos electrónicos como Microsoft Outlook para la privacidad y confidencialidad de la información y no por correos como Gmail, Yahoo, etc.

REFERENCIAS

Cocho, J. (2003). *Riesgo y Seguridad de los sistemas de información.* España: Universidad Politécnica de Valencia.

Derrien, Y. (2011). *Tecnicas de la Auditoria Informatica Segundo tomo.* Italia: Marcombo.

Fernández, E., Saiz, A., & Seoane, C. (2014). *Seguridad Informática.* Buenos Aires: Edigrafos.

Gomez, A. (2011). *Seguridad Informatica Basica.* Mexico: STARBOOK EDITORIAL.

Gonzales, A. (2012). *Seguridad Informatica en la Educacion Superior.* España: Academia Española.

Henríquez, E. (2011). *Auditoría en informática.* Colombia: Cesca.

Hernandez, R. (2010). *Seguridad en las redes e Internet.* Obtenido de http://www.segu-info.com.ar/firewall/firewall.htm

Imbaquingo, D., & Jácome, J. (2017). *Fundamentos de Auditoría informática Basada en Riesgos.* Ibarra: Editorial Universidad Técnica del Norte.

ISACA. (2008). *COBIT 4.1.* EE.UU: ISACA.

ISACA, & Bernabe, M. (2012). *COBIT 5: PROCESOS CATALIZADORES.* EEUU: ISACA.

ISACA, & Cerezo, A. (2013). *Soportando y Auditando La Gestion De La Continuidad Del Negocio Por Normas ISO.* Monterrey: ISACA.

ISO, N. (2013). *ISO27001.* Obtenido de http://www.iso27000.es/download/doc_sgsi_all.pdf

Joyanes, L. (1998). *Cibersociedad: los retos sociales ante un nuevo mundo.* Madrid: McGraw-Hill Interamericana.

Lardent, A. (2001). *Sistemas de información para la gestión empresarial-procedimientos, seguridad y auditoría.* Buenos Aires: Pearson Educatión.

Larrondo, A. (2010). *Uso de la norma ISO/IEC 27002 para SGSI.* Madrid, España.

Lauces, J. (2016). *Seguridad en redes inalambricas de area local (WLAN).* España: Investigación.

López, M. J., & Quezada, C. (2006). *Fundamementos de Seguridad y Políticas de Seguridad.* Mexico: UNAM.

Marquina, E. G. (2012). *Análisis y Gestión de Riesgo Implementando MAGERIT.* España: Acádemica Española.

Medina, Y., & Rico, D. (2012). *Modelo ITIL Gestión de Servicios en Sistemas de Información.* España: Académica Española.

Mendoza, L. (2014). *SISTEMAS DE INFORMACIÓN III.* QUITO.

Pérez, J. (2012). *La Base de Datos, Su seguridad y Auditoria.* Madrid: Trabajo Academico.

Piattini, M. (2011). *Auditoria Informática, Un enfoque práctico.* Argentina: Alfaomega.

Ribagorda, A. (1995). *Seguridad y protección de la información.* España: Universitaria Ramón Areces.

Van, J., & Kolthof, A. (2008). *Gestion de Servicios TI, Basado en ITIL.* Canada: ITSM Library.

Villalobos, J. (2008). *AUDITANDO EN LA BASE DE DATOS.* Costa Rica: Uniciencia.

Vivas, P. (2011). *Seguridad De La Información Para Empresas.* Quito-Ecuador .

ANEXOS

Anexo A. Entrevista para el Administrador del Área de Sistemas del Instituto Tecnológico Superior Sudamericano Quito, con estándares de la Norma ISO 27002.

Políticas de seguridad de la información

- **¿Se cuenta con políticas de seguridad de la información?**

SI ( ) NO (X)

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

SI ( ) NO(X)

ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD

- **¿El instituto Tecnológico Superior Sudamericano Quito, cuenta con un área para labores exclusivas de seguridad de la información?**

SI ( ) NO (X)

- **¿El instituto Tecnológico Superior Sudamericano Quito, ha contratado un asesoramiento en materia de seguridad de la información?**

SI ( ) NO (X)

CON RELACIÓN A LA CLASIFICACIÓN Y CONTROL DE ACTIVOS INFORMÁTICOS

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

SI (X) NO ( )

- **¿Este inventario esta automatizado?**

SI (X) NO ( )

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

SI (X) NO ( )

POLÍTICAS DEL PERSONAL RESPECTO A LA SEGURIDAD INFORMÁTICA

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

SI (X) NO ( )

- **¿El Instituto Tecnológico Superior Sudamericano Quito cuenta con convenios de confidencialidad de la información?**

SI ( ) NO (X)

SEGURIDAD FÍSICA Y AMBIENTAL DE LOS SISTEMAS DE INFORMACIÓN

- **¿Todas las áreas esta identificadas?**

SI (X) NO ( )

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

SI ( ) NO (X)

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

SI (X) NO ( )

- **¿Se realiza mantenimiento periódico del hardware y software en el Instituto Tecnológico Superior Quito?**

SI (X) NO ( )

CON RELACIÓN A LA GESTIÓN DE LAS COMUNICACIONES DE DATOS Y OPERACIONES DE LOS SISTEMAS INFORMÁTICOS

- **¿El Instituto Tecnológico Superior Sudamericano Quito, cuenta con controles contra software malicioso (antivirus, antispyware, etc.)?**

SI (X) NO ( )

- **¿El Instituto Tecnológico Superior Sudamericano Quito, cuenta con registro de accesos y uso de los aplicativos y servicios de la red de los colaboradores?**

SI ( ) NO (X)

- **¿Se cuenta con controles de seguridad de los medios de almacenamiento?**

SI (X) NO ( )

- **¿El Instituto Tecnológico Superior Sudamericano Quito, cuenta con compromisos de responsabilidad del uso de los recursos de la Institución?**

SI ( ) NO (X)

CONTROL DE ACCESO

Nota: en los estándares de la norma ISO 27002, el control de acceso se rige a aplicativos creados y de dominio propio como almacenamiento de información privada en sitios web, aplicativos móviles etc., de lo cual en esta norma no se cumple dentro del parámetro.

DESARROLLO Y MANTENIMIENTO DE SISTEMAS INFORMÁTICOS

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

SI ( ) NO (X)

- **¿Se valida los códigos fuente desarrollados por personal externo antes de la puesta en producción?**

SI ( ) NO (X)

GESTIÓN DE INCIDENTES DE SISTEMAS INFORMÁTICOS

- **¿El Instituto Tecnológico Superior Sudamericano Quito, cuenta con un procedimiento formal para reportes de incidentes?**

SI ( ) NO (X)

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

SI ( ) NO (X)

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

SI ( ) NO (X)

Administración de la continuidad de los sistemas informáticos

- **¿El Instituto Tecnológico Superior Sudamericano Quito cuenta con planes de continuidad de operaciones?**

SI ( ) NO (X)

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

SI ( ) NO (X)

CUMPLIMIENTO LEGAL REFERIDO A LOS SISTEMAS INFORMÁTICOS

- **¿El Instituto Tecnológico Superior Sudamericano Quito, cuenta con políticas de datos y privacidad de la información de los colaboradores?**

SI ( ) NO (X)

- **¿Cuentan con controles del uso inadecuado de los recursos del Instituto Tecnológico Superior Sudamericano Quito?**

SI ( ) NO (X)

- **¿El Instituto Tecnológico Superior Sudamericano Quito, cuenta con controles del cumplimiento de las políticas de la seguridad de la información?**

SI ( ) NO (X)

- **¿Realizan Auditorias a los sistemas informáticos de la Institución?**

SI (X) NO ( )

Anexo B Red del Instituto Tecnológico Superior Sudamericano Quito