UNIVERSIDAD INTERNACIONAL SEK

FACULTAD DE ARQUITECTURA E INGENIERÍAS

Trabajo de fin de carrera titulado:

"DISEÑO DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA EL ÁREA DE TICS DEL INSTITUTO TECNOLÓGICO SUPERIOR CENTRAL TÉCNICO, BASADO EN LA NORMA DE SEGURIDAD ISO/IEC 27002:2013"

Realizado por:

Ing. Hilda Yecenia Cevallos Jarro

Director del proyecto:

Ing. Verónica Elizabeth Rodríguez Arboleda, MBA

Como requisito para la obtención del título de

MASTER EN TECNOLOGÍAS DE LA INFORMACIÓN CON MENCIÓN EN SEGURIDAD EN REDES Y COMUNICACIÓN

DECLARACION JURAMENTADA

Yo, HILDA YECENIA CEVALLOS JARRO, con cedula de identidad 1104224108, declaro bajo juramento que el trabajo aquí desarrollado es de mi autoría, que no ha sido previamente presentado para ningún grado a calificación profesional; y, que ha consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración, cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la UNIVERSIDAD INTERNACIONAL SEK, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente

_____

HILDA YECENIA CEVALLOS JARRO

C.C.: 1104224108

DECLARATORIA

El presente trabajo de investigación titulado:

"DISEÑO DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA EL ÁREA DE TICS DEL INSTITUTO TECNOLÓGICO SUPERIOR CENTRAL TÉCNICO, BASADO EN LA NORMA DE SEGURIDAD ISO/IEC 27002:2013"

Realizado por:

HIDA YECENIA CEVALLOS JARRO

Como requisito para la Obtención del Título de:

MASTER EN TECNOLOGÍAS DE LA INFORMACIÓN CON MENCIÓN EN SEGUIRDAD EN REDES Y COMUNICACIÓN

Ha sido dirigido por el profesor

Ing. Verónica Elizabeth Rodríguez Arboleda, MBA.

Quien considera que constituye un trabajo original de su autor

_____

Ing. Verónica Elizabeth Rodríguez Arboleda, MBA.

DIRECTORA

LOS PROFESORES INFORMANTES

Los profesores informantes:

Walter Edison Estrella Mogollon

Christian David Pazmiño Flores

Después de revisar el trabajo presentado lo han calificado como apto para su defensa oral ante el tribunal examinador

_____ _____

Walter Edison Estrella Mogollon Christian David Pazmiño Flores

Quito, marzo de 2019

DEDICATORIA

Este proyecto de tesis lo dedico a:

Dios, por bendecirme con salud y trabajo para alcanzar un objetivo más en mi vida profesional.

Mi papá Wilson Cevallos, por brindarme su apoyado incondicional.

Mi mamita Hilda Jarro, que siempre la tengo presente y sé que desde el cielo me cuidas y me guías.

Mis hermanos y sobrinos, por estar conmigo y apoyarme siempre, son el motivo y mi pilar fundamental de mi crecimiento personal y vean en mí un ejemplo a seguir, los quiero mucho.

Finalmente a mis maestros, aquellos que guiaron mi camino académico, y a mi tutora de tesis que me ayudó despejando dudas presentadas en el desarrollo de este proyecto de tesis.

AGRADECIMIENTO

Agradezco infinitamente a:

Dios, por su infinita bondad y amor y ser la luz que guía mi camino.

Mi papá por su confianza depositada en mí y su gran apoyo.

Mis hermanos y sobrinos por su apoyo incondicional.

Al Instituto Tecnológico Superior Central Técnico, por brindarme las facilidades de estudio respectivo para el desarrollo del mismo.

Mi directora de Tesis, Ing. Verónica Rodríguez por su valiosa dirección en el desarrollo de este proyecto de tesis y llegar a la conclusión de la misma.

RESUMEN

En el presente proyecto de tesis se propone medidas para que el personal del área de TICS del Instituto Tecnológico Superior Central Técnico (ITSCT) pueda controlar las amenazas que puedan afectar la integridad, confidencialidad y disponibilidad de su información. Inicialmente se realizó una matriz de riesgos mediante la metodología Magerit, para identificar y valorar las amenazas y vulnerabilidades a las que está expuesta la información de la Institución. Se analizó la norma ISO/IEC 27002:2013 que es una guía de buenas prácticas para la gestión de la seguridad de la información para a todo tipo de organizaciones independientemente del tamaño, tipo o naturaleza adaptándose correctamente al área de TICS, en base a los riesgos identificados en el área de TICS se seleccionó los controles de la Norma que permitirían mitigar los riesgos encontrados en la Institución. Los controles seleccionados fueron plasmados en una propuesta de protocolo de seguridad de la información y se recomienda implementar en el Instituto Tecnológico Superior Central Técnico, ya que servirá como guía para el buen uso y manejo de los activos del área de TICS.

Palabra Clave: Política de seguridad, Metodología Magerit, Noma ISO/IEC 27002

ABSTRACT

The current thesis project proposes procedures for TICS area personnel of the Instituto Tecnológico Superior Central Técnico (ITSCT) can control threats that could affect the integrity, confidentiality and availability of their information. Firstly, a risk matrix was created using the Magerit methodology to identify and assess threats and vulnerabilities to which the Institution's information is exposed. The ISO / IEC 27002: 2013 standard was analyzed, which is a guide to good practices for the management of information security for all types of organizations, regardless of size, type or nature, which adapts correctly to TICs area. Based on the risks identified in TICs area, controls were selected from the ISO standard, which allow to mitigate found risks found in the Institution. The selected controls were described in a proposal of information security protocol. The proposal is recommended to be implemented in the Instituto Tecnológico Superior Central Técnico (ITSCT) since it will be used as a guide for proper use and management of TICS area assets.

Key: Security Politic**,** Magerit methodology, ISO 27002 Standard.

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO I

INTRODUCCIÓN

1.1. Problema de investigación

1.1.1. Planteamiento del problema.

1.1.1.1. Diagnóstico.

El Instituto Tecnológico Superior Central Técnico (ITSCT), es una entidad de educación superior, que tiene procesos críticos como: registro de información personal de administrativos, docentes y estudiante, servicios de matrícula, titulación, vinculación con la comunidad, Formación Dual, pasantías y/o prácticas pre- profesionales, registro de asistencia, ingreso de notas, evaluación docente, portafolio docente, reportes estadísticos, base de datos de entidades con las que mantiene convenios para los procesos de Practicas pre-profesionales y Vinculación con la comunidad por parte de los estudiantes. Los servicios antes mencionados recopilan información valiosa y confidencial y son administrados mediante un software académico que es desarrollado por el área de TICS, ésta área se encarga además de la Administración de los laboratorios Informáticos.

Mediante la observación directa y una entrevista realizada al coordinador del área de TICS, se identificó los siguientes inconvenientes:

- No existe documentación y asignación de responsabilidades de los procedimientos que se ejecutan en el área de TICS, son creados subjetivamente y llevados a cabo por experiencia de los integrantes del equipo de TICS.
- Algunos usuarios no hacen uso de bloqueo de pantalla a los equipos de cómputo que les ha sido asignada, por lo que cualquier persona puede acceder a ellos.
- Algunos usuarios realizan cambios de claves de acceso a sus equipos de cómputo a criterio personal, sin una periodicidad y/o bitácora definida.
- Lo equipos de cómputo no poseen antivirus, por lo que son vulnerables a infectarse.
- No existe control en los periféricos que permiten el acceso a flash memory, lo que desencadena que se puedan infectar de virus malware.
- Los usuarios no hacen uso de los correos electrónicos institucionales asignados.
- No existe un acuerdo de confidencialidad y de no divulgación de la información que garantice la confidencialidad, integridad, disponibilidad, reserva y protección de los datos e información.
- No existe la documentación correspondiente del software académico, como son: análisis de requisitos, manual del programador y manual del usuario.
- Cuando se presenta algún tipo de error de ejecución en el software académico, las correcciones a realizar dependen solamente del o los desarrolladores del software.
- El área de TICS no cuenta con una normativa de uso y manejo de la información que garantice su integridad, confidencialidad y disponibilidad.

1.1.1.2. Pronóstico.

Con el crecimiento de la población estudiantil detallada en la Tabla 1, la creación del Centro de Idiomas y de nuevas carreras como: Tecnología Superior en Diseño e Impresión

OFFSET, Desarrollo Infantil Integral, Mecánica Automotriz, Mecánica Industrial, Electrónica y Electricidad, la información crece significativamente y, no se ha considerado la importancia de protegerla por lo cual podría ser víctima de delitos informáticos (modificación y/o robo de información, intrusiones, suplantación de identidad, falsificación documental, etc.) que dificulten el normal funcionamiento de los procesos del ITSCT.

Tabla 1 *Población estudiantil*

	Años	
Tipo de carrera	**2017**	**2018**
Tradicional	1252	719
Dual	292	270
Rediseñada	652	1519
Dual Rediseñada	84	161
Instituto de Idiomas	0	1206
Total estudiantes	**2280**	**3875**

Fuente: Área de TICS del ITSCT

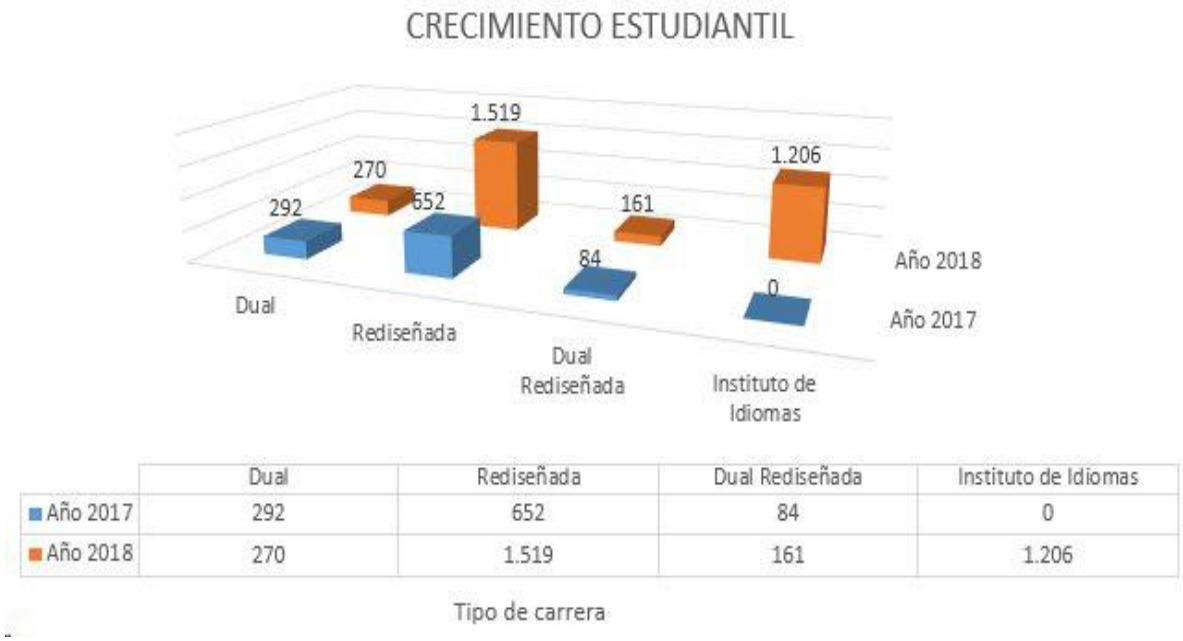

Figura 1 Crecimiento estudiantil ITSCT
Fuente: Elaborado por la autora de la investigación

1.1.1.3. Control del Pronóstico.

Para contrarrestar los efectos que pudiesen ser generados por delitos informáticos en el área de TICS, se consideró la elaboración de controles de seguridad de la información basado en la norma ISO 27002:2013, esta norma provee buenas prácticas de seguridad de la información que ayudará al área de TICS a gestionar y proteger sus activos de información.

1.1.1.4. Formulación del problema.

En el área de TICS del Instituto Tecnológico Superior Central Técnico, se concentran procesos críticos que manejan información valiosa y se han generado inconvenientes en cuanto al uso y manejo de la misma, comprometiendo su integridad, confidencialidad y disponibilidad.

1.2. Objetivos

1.2.1. Objetivo General

Diseñar una política de seguridad de la información para el área del TICS del Instituto Tecnológico Superior Central Técnico (ITSCT), basado en la norma de seguridad ISO/IEC 27002:2013, que servirá como guía de acción para que las autoridades y docentes hagan buen uso y manejo de la información garantizando su confidencialidad, integridad y disponibilidad.

1.2.2. Objetivos específicos

- Analizar la situación actual de los procesos que lleva a cabo el área de TICS del Instituto Tecnológico Superior Central Técnico (ITSCT) mediante la elaboración de una matriz de riesgos, que permita la identificación de vulnerabilidades, amenazas y riesgos de seguridad en el manejo de la información.
- Analizar la norma ISO/IEC 27002:2013 en base a la matriz de riesgos elaborada, para seleccionar los controles que se ajusten a las necesidades de seguridad de la información del área de TICS del Instituto Tecnológico Superior Central Técnico (ITSCT).
- Diseñar los controles de la política de seguridad de la información, basado en la norma de seguridad ISO/IEC 27002:2013, para minimizar la probabilidad de ocurrencia e impacto de los riesgos asociados con las vulnerabilidades y amenazas de seguridad de la información existentes en el área de TICS del Instituto Tecnológico Superior Central Técnico (ITSCT).

1.3. Justificación

Hoy en día el Instituto Tecnológico Superior Central Técnico (ITSCT) tiene una infraestructura tecnológica en crecimiento de la cual dependen muchos procesos administrativos, académicos que requieren que la información que maneja esté siempre disponible, sin alteración y sea confiable.

En el área de TICS se desarrolla software y se gestiona de la mayor parte de la información institucional; en esta se evidenció que no posee procesos documentados con los respectivos responsables, no existen controles que permitan el adecuado tratamiento

de la información, situación por la cual el servidor era manipulado por los usuarios del área, quienes modificaban la información a petición o conveniencia de los docentes sin autorización de los directivos de la institución, violando así la integridad de los datos.

Con el objetivo de proporcionar reglas para que los docentes utilicen apropiadamente los equipos y la información, contribuir con la calidad y eficacia en los servicios críticos en el ITSCT y las autoridades puedan tomar acciones preventivas y correctivas dentro de la institución, se ha desarrollado un protocolo de seguridad.

Para cumplir con los objetivos propuestos en este trabajo de tesis, se realizó una identificación de riesgos en el área de TICS utilizando la metodología Magerit, la cual permitió identificar las vulnerabilidades y amenazas existentes en el uso y manejo de los activos de información. Para la selección de controles de acuerdo a los riegos identificados, se utilizó como base la norma de seguridad ISO/IEC 27002:2013, que es una guía de buenas prácticas que describe los objetivos de control y controles recomendables a seguir dentro del marco de la seguridad de la información, aplicables a entidades grandes y pequeñas y se ajusta a las necesidades institucionales. Este estándar de calidad de seguridad de la información ayuda a minimizar los riesgos de daño, robo o fuga de la información, alteración o repudio, manteniendo así la integridad, confidencialidad, disponibilidad de la información.

1.4. Estado del arte

El área de TICS del Instituto Tecnológico Superior Central Técnico (ITSCT), maneja información valiosa que ayudan al cumplimiento de los objetivos institucionales, situación por la cual debe ser protegida adecuadamente siguiendo una serie de normas de seguridad de

la información considerando sus dimensiones de integridad, confidencialidad y disponibilidad.

Ochoa (2015) afirma. "ISO proporciona un mejor desempeño de Seguridad de la Información" (p.17); y según Posso (2009), la norma ISO 27002 establece directrices y principios generales para iniciar, implementar mantener y mejorar la gestión de la seguridad de la información en una organización y que sirve como guía para el desarrollo de normas de seguridad para las prácticas eficaces de gestión de la seguridad, así como para crear confianza en las actividades entre las organizaciones. (p.3)

"Los controles definidos en la norma ISO 27002 como políticas y procedimientos servirán de base para el diseño, implementación e implantación de un futuro SGSI" (Solarte, Rosero y Benavides, 2015).

En el Desarrollo de políticas de seguridad informática e implementación de cuatro dominios en base a la Norma 27002 para el área de hardware en la empresa Uniplex Systems S.A. en Guayaquil realizado por Posso (2009), menciona que: Lo primordial es centrarse en los procesos principales de la organización donde se concentra la mayor parte de actividades relacionadas con la gestión de la información, que suele coincidir con las áreas de sistemas de información donde la seguridad de la información que se gestiona es crítico para el desarrollo de las actividades del negocio. (p.8)

En el trabajo *Implementation of security controls according to ISO/IEC 27002 in a small organization* (Implementación de los controles de seguridad según ISO/EC 27002 en una pequeña organización) realizado por Horváth & Jakub (2009), menciona que: En organizaciones pequeñas debe aplicarse requisitos de ISO / IEC 27001, teniendo en cuenta las posibilidades de dichas organizaciones, como también no es necesario implementar todos los controles de seguridad de ISO/EC 27002, por la sencilla razón de que la organización no utiliza Tecnología o procesos.

Guato, Fernando, Muenala y Geovanna (2016) autores del trabajo de tesis de pregrado Aplicación de las normas técnicas ISO/IEC 27001 e ISO/IEC 27002 para el cumplimiento del esquema gubernamental de seguridad de la información (EGSI) en la infraestructura del Sistema Nacional de Nivelación y Admisión (SNNA), y Ledezma (2015) autora de Desarrollo de políticas de seguridad de la información basadas en las Normas ISO 27002 para una Coordinación Zonal del INEC, sustentan la aplicación de la norma ISO 27002 en referencia al cumplimiento a los requerimientos del acuerdo ministerial No. 166 del Registro Oficial del Ecuador emitido por la secretaria Nacional de Administración pública, donde se especifica el esquema gubernamental de seguridad de la información.

> El 19 de septiembre de 2013 se emitió el Acuerdo Ministerial No. 166, publicado mediante Registro Oficial No. 88 del 25 de septiembre de 2013, que dispone que las entidades de la Administración Pública Central, Institucional y Dependiente de la Función Ejecutiva (APCID), la implementación del Esquema Gubernamental de Seguridad de la Información EGSI, Norma Técnica Ecuatoriana INEN ISO/IEC 27002 "Código de Buenas Prácticas para la Gestión de la Seguridad de la Información". En concordancia con el Plan Nacional de Gobierno Electrónico 2014-2017 del Ecuador, reforzando el principio de garantizar seguridad y confianza y como parte del Plan Estratégico de Seguridad y Protección de Datos, el EGSI es un instrumento de vital importancia para todos los actores del Plan Nacional: ciudadanos, servidores, empresas, y gobierno y otros actores del estado. (Secretaria Nacional de Administración Pública, 2013)

En el proyecto Aplicación de las normas técnicas ISO/IEC 27001 e ISO/IEC 27002 para el cumplimiento del esquema gubernamental de seguridad de la información (EGSI) en la infraestructura del Sistema Nacional de Nivelación y Admisión (SNNA) desarrollado por Guato et al. (2016), realizan una comparación entre metodologías para el análisis de riesgos y llegan a la conclusión de utilizar la metodología MAGERIT por las siguientes razones:

- Ofrece una visión más amplia con pasos específicos a realizar, se basa en objetivos de seguridad de la información obteniendo como resultado un estado del riesgo junto con un plan de seguridad.
- Puede ser utilizada en cualquier tipo de institución, organización o empresa.
- Es la única metodología que cumple con ciertos estándares de la familia ISO 27000, estos sirven de guía para establecer e implementar un SGSI.
- Posee un nivel de madurez, ha evolucionado hasta la versión 3, y se basa en el proceso de gestión de riesgos de acuerdo a la NORMA ISO/IEC 31000.

Una vez analizado los artículos citados, se concluye que: la metodología MAGERIT, es la opción más efectiva y completa para el análisis de riesgos en el área de TICS del ITSCT, ya permite la valoración de activos en base a su integridad, disponibilidad y confidencialidad, como también la identificación de amenazas y vulnerabilidades que pueden impactar los activos, facilitando la selección de medidas de seguridad que garanticen el éxito de los procesos; y, para la selección y elaboración de las medidas de seguridad para el área de TICS, se tomará como referencia la Norma ISO/IEC 27002, ya que “puede ser implementada en empresas pequeñas como en grandes organizaciones” (Posso, 2009, p.9), públicas o privadas garantizando la confidencialidad, integridad y disponibilidad de la información.

CAPÍTULO II

MARCO TEÓRICO

1.1. Seguridad informática

Velasco (2008) refiere que la trascendencia de la seguridad de la información en las organizaciones públicas o privadas radica en que: (i) el volumen de información crece día a día; (ii) la información es un intangible con un valor bastante apreciable en la economía actual; (iii) la información es una ventaja estratégica en el mercado, que la convierte en algo atractivo para la competencia, como elemento generador de riqueza, (iv) la frecuencia de los ataques a los activos de una organización es cada vez mayor, cualquiera que sea el medio al que se acuda, y (v) no existe una cultura de seguridad en los usuarios de la información, lo que conduce a que las organizaciones empiecen a incorporar prácticas seguras de protección de la información, advirtiendo que este proceso habrá de impactar la cultura de la organización; aspecto que requiere de tiempo y compromiso, empezando por la dirección de la misma.

En la XVII jornada internacional de seguridad informática, IX informe de encuesta latinoamericana de seguridad de la información, Junio 2017 se destaca el porcentaje de los obstáculos para lograr la seguridad de la información:

Tabla 2 *IX informe de encuesta latinoamericana de seguridad dela información*

Obstáculos para lograr la seguridad de la información	**2015**	**2016**	**2017**
Ausencia o falta de una cultura en seguridad de la información		38.7%	59.1%
Falta de colaboración entre áreas/departamentos	45.7%	30.5%	42.6%
Poco entendimiento de la seguridad de la información	33.5%	32.0%	33.5%
Falta de apoyo directivo	41.6%	32.3%	30.7%

Fuente: Cano, María y Meza (2017)

Ante tantas eventualidades presentadas en lo referente a la seguridad del activo más valioso, en las organizaciones se podría pensar en que una de las formas de minimizar los riesgos sería la evaluación a nivel interno de algunos ítems: administrativos, profesionales interdisciplinarios, tecnologías, aplicación de políticas, disponibilidad de recursos, capacitación, entre otros. (Electrónica, 2017)

La seguridad requiere una inversión debido a la necesidad de implantar hardware, adquirir licencias de software, los costes de sus mantenimientos y de formar a administradores y a usuarios. Si se conciencia a los usuarios de las políticas y procedimientos de seguridad que hay implantados, se reduce algunas necesidades de inversión e incluso, permite optimizarlas porque serán los propios usuarios quienes nos retroalimentarán con la información más directa. Además, los usuarios prefieren comprender el porqué de las cosas a que les sea impuesto, ya que puede producir una sensación de resistencia y de rechazo. (Forum, Council, Security y Management, 2013)

1.2. Amenaza informática

Forum et al. (2013) menciona que una amenaza es la causa potencial de un incidente no deseado, el cual puede causar daño a un sistema o a la organización. Los principales tipos de amenazas se describen a continuación:

1.2.1. Amenaza lógica

Es aquella que afecta a la información almacenada en los activos. A su vez hay dos casos especialmente importantes:

- Amenaza estructurada: Producida por alguien que posee una metodología formal, un posible patrocinador y sobre todo, un objetivo definido. Un buen ejemplo de ellos son los famosos espionajes industriales. Esta amenaza busca comprometer un sistema a largo plazo, y por lo tanto tratan de evitar dejar cualquier rastro de ataque.
- Amenaza no estructurada: el atacante no posee una metodología formal, tampoco tiene patrocinador y no tiene un objetivo. Suelen ser intrusos "ociosos", efectos del malware o empleados descontentos. A esta amenaza, le es indiferente dejar rastro y lo que busca es notoriedad. Por ejemplo, modificar el contenido de una web pública.

1.2.2. Amenaza física

Un atacante tiene diferentes tipos de acceso físico a la organización y puede ocasionar problemas. Ejemplos hay de una persona buscando información confidencial en la papelera o seguir a un empleado y entrar con él por la puerta como su fuera un compañero.

1.3. Riesgos informáticos

Fugas de información, fraude y robo de datos, vulnerabilidades, falta de un plan de continuidad, etc., son riegos potenciales que pueden afectar a los sistemas de información.

Los riesgos informáticos son problemas potenciales, que pueden afectar a los sistemas de información o a los equipos de cómputo. Si no se tienen las medidas adecuadas

> para salvaguardar los datos y la información, dichos riesgos se pueden presentar por las vulnerabilidades y amenazas en cualquier momento. (Solarte et al., 2015)

Según Escrivá, Romero y Ramada (2013) mencionan que ante un determinado riesgo, una organización puede optar por tres alternativas distintas:

- **Asumirlo sin hacer nada.** Esto solamente resulta lógico cuando el perjuicio esperado no tiene valor alguno o cuando el coste de aplicación de medidas superaría al de la reparación del daño.
- **Aplicar medidas** para disminuirlo o anularlo.
- **Transferirlo** (por ejemplo, contratando un seguro).

Es preferible hablar de riesgos que de seguridad, ya que al conocer el riesgo se puede establecer una contramedida que lo mitigue o erradique.

Mediante los controles de seguridad de la norma ISO/IEC 27002:2013 se establecen mecanismos adecuados para mitigar riesgos que se pueden presentar en el uso de los sistemas de información.

Antes de describir la norma ISO/IEC 27002:2013, es importante definir las normas ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27004 e ISO/IEC 27005.

1.4. Norma ISO/IEC 27000

ISO/IEC 27000 es un conjunto de estándares desarrollados o en fase de desarrollo por la ISO (*International Organization for Standardization*) e IEC (*International Electrotechnical Commission*), que brindan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización de tipo público o privada, grande o pequeña. (Orrego, 2013, p.22)

Grupa (2015) menciona que la serie 27000 se completa con una gama de estándares y documentos individuales, los cuales son:

1.4.1. Norma ISO/IEC 27001

Se puede emplear en todo tipo de organizaciones (privadas, públicas, entidades sin ánimo de lucro, etc.), sin importar el tamaño o la actividad.

Esta norma define los requisitos para la creación, implementación, funcionamiento, supervisión, revisión, mantenimiento de un sistema de gestión de seguridad de la información (SGSI) documentado en base a las necesidades de la organización o de partes de la misma, pero no aclara mediante que procedimientos se ponen en práctica (Andrés y Gómez, 2009).

1.4.2. Norma ISO/IEC 27002

Según Andrés y Gómez (2009), esta norma "Establece directrices y principios generales para el comienzo, implementación, mantenimiento y la mejora de la gestión de la seguridad de la información en una organización".

Es una guía de buenas prácticas, que describe los objetivos de control y controles recomendables a seguir dentro del marco de la seguridad de la información.

Los controles de esta norma sirven de guía para desarrollar las pautas de seguridad interna y prácticas efectivas de seguridad. Para la correcta selección de controles se realiza un análisis de riesgos previo, y el grado de implementación de los controles dependerá de los requisitos de seguridad y de los recursos disponibles de la organización. La última edición de esta norma es la del 2013, que ha sido actualizada a 14 Dominios. 35 Objetivos de control y 114 controles.

A continuación, se detalla de forma general los 14 dominios dela norma ISO/IEC 27002:2013.

1.4.2.1. Políticas de seguridad.

Este dominio hace referencia a la creación de un documento sobre la política de seguridad de la información de la organización. Este documento debe ser aprobado por la gerencia y luego publicado y socializado a todos los empleados de la organización.

La política de seguridad debe ser revisada y actualizada cada cierto tiempo planificado o cuando se produzcan cambios significativos con el fin de que estas mantengan su competencia, adecuación y eficacia.

1.4.2.2. Aspectos organizativos de la seguridad de la información.

En este apartado se tiene como objetivo manejar la seguridad de la información dentro de la organización.

Las actividades de seguridad de la información deben ser coordinadas por representantes de la organización, que deben tener responsabilidades bien definidas, para reducir la posibilidad de que se produzcan modificaciones no autorizadas o usos indebidos de los activos de la organización.

1.4.2.3. Seguridad ligada a los recursos humanos.

Antes de la vinculación a la organización de un empleado es importante que sea debidamente analizado. La organización debe brindar capacitaciones periódicas a sus

empleados, para crear conciencia y procesos disciplinarios en cuanto a la seguridad de la información. Los empleados deben conocer las posibles amenazas relativas a la seguridad de la información, y ser conscientes de sus responsabilidades y obligaciones en los roles que son contratados.

1.4.2.4. Gestión de activos.

Los activos de información comprenden la infraestructura, cableado de red, equipos de cómputo, servidores, sistemas operativos, software de aplicación, bases de datos, copias de información, etc. Estos activos deben ser clasificados para mantener un inventario actualizado con los respectivos custodios.

1.4.2.5. Control de accesos.

El acceso a los activos de información debe ser controlado en base a los requisitos del negocio. Debe garantizarse el acceso a usuarios autorizados con el fin de evitar daños a los mismos.

1.4.2.6. Cifrado.

Es muy importante utilizar algoritmos criptográficos para proteger y garantizar la autenticidad, confidencialidad e integridad de la información.

1.4.2.7. Seguridad física y ambiental.

La seguridad física y ambiental hace referencia a un perímetro de seguridad física que cuente con controles físicos de entrada, extintores, puertas con llave, cámaras de seguridad, bitácoras de acceso, etc., controlar la temperatura adecuada para los equipos, seguridad en el cableado, mantenimiento de equipos, para proteger de amenazas externas y ambientales las áreas que contienen activos de información.

1.4.2.8. Seguridad en la operativa.

Es importante que estén definidos, documentados y autorizados por la gerencia los procedimientos y responsabilidades de operación de los recursos de procesamiento de la información.

1.4.2.9. Seguridad en las telecomunicaciones.

Se debe establecer normas de intercambio formales para proteger el intercambio de información a través del uso de medios de comunicación sean estos físicos o digitales.

1.4.2.10. Adquisición, desarrollo y mantenimiento de los sistemas de información.

Se debe contemplar aspectos de seguridad al adquirir sistemas o al desarrollarlos. Los requisitos de seguridad de los sistemas de información deben ser identificados y acordados durante todo el ciclo de vida del sistema (software).

1.4.2.11. Relaciones con suministradores.

Asegurar la protección de los activos de información de la organización que sean accesibles a los proveedores.

1.4.2.12. Gestión de incidentes en la seguridad de la información.

Se debe trabajar con reportes formales de los eventos y debilidades de la seguridad de la información, asegurando una comunicación tal que permita que se realice una acción correctiva oportuna. Los eventos de seguridad de información deben ser evaluados y respondidos de acuerdo con los procedimientos documentados.

1.4.2.13. Aspectos de seguridad de la información en la gestión de la continuidad del negocio.

Los planes de continuidad del negocio deben ser desarrollados documentados e implementados, con el fin de impedir la interrupción de las actividades del negocio y asegurar que las operaciones esenciales sean rápidamente recuperadas.

Los planes de continuidad del negocio deben ser actualizados y sometidos a pruebas, mantenimiento y evaluación.

1.4.2.14. Cumplimiento.

“Es necesario implementar los procedimientos apropiados para asegurar el cumplimiento de los requerimientos legislativos, reguladores y contractuales sobre el uso del material con

respecto a los cuales puedan existir derechos de propiedad intelectual y sobre el uso de productos de software patentado" (Inen, 2017).

La elección de controles se lo realiza después de un análisis de riesgos y la implementación de dichos controles depende de los requisitos de seguridad identificados y de los recursos disponibles en la organización.

1.4.3. Norma ISO/IEC 27003

Según Grupa (2015).

Esta norma fue publicada el 01 de febrero de 2010 y actualizada el 12 de Abril de 2017. No certificable, ayuda y orientación sobre la implementación de un SGSI de acuerdo con la ISO/IEC 27001.

Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo ISO/IEC 27001. Describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la dirección para implementar un SGSI. Tiene su origen en el anexo B de la norma BS 7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.

1.4.4. Norma ISO/IEC 27004

Publicada el 15 de diciembre de 2009 y revisada en Diciembre de 2016. No certificable. Es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para

determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001 (Grupa, 2015).

1.4.5. Norma ISO/IEC 27005

Publicada la tercera edición en Julio de 2018 con actualizaciones respecto a requisitos de norma ISO/IEC 27001:2013. La segunda edición es de 1 de junio de 2011 y la primera edición del 15 de Junio de 2008. No certificable. Proporciona directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. Su primera publicación revisó y retiró las normas ISO/IEC TR 13335-3:1998 e ISO/IEC TR 13335-4:2000. (Grupa, 2015)

1.5. Políticas de seguridad

El éxito o fracaso de una organización, depende de la calidad del servicio que ésta proporciona, pero sin embargo éste no podría funcionar sin la información requerida para los diversos fines que persiguen las empresas. Es por ello que éstas deben implementar políticas y medidas estratégicas que aseguren la calidad de sus datos, además de planificar una fase de identificación y evaluación del riesgo al cual es susceptible de sufrir, en cuanto a diversos tipos de ataques, que lleven a la pérdida de registros, tiempo y trabajo. (Aceves, n.d.)

Gomez Vieites (2014) afirma. “Una política de seguridad es una declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que

proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran".

Según Dussan Clavijo (2006), Una política de seguridad son un conjunto de directrices, normas, procedimientos instrucciones que guía las instrucciones de trabajo y definen los criterios de seguridad para que sean adoptados a nivel local o institucional, con el objetivo de establecer, estandarizar y normalizar la seguridad tanto en el ámbito humano como tecnológico. (p.89)

Mendez-Vilas, Gonzalez, González y Bote (2003) indican que, para el desarrollo del documento de políticas de seguridad se debe considerar las siguientes características:

- Enfocar la política hacia la problemática particular de la organización.
- Contar con un documento con una estructura bien definida.
- Definición clara y precisa de los enunciados.
- Que exponga de manera explícita el ámbito de aplicación.
- Que se establezcan obligaciones y derechos tanto para los administradores como para los usuarios.
- Que se defina claramente las sanciones a las que estará sujeto quien no se apegue a las políticas de seguridad institucionales.
- Que el documento cuente con vigencia y flexibilidad para su actualización.

Las políticas de seguridad, así como las leyes que se generan, por si mismas no resuelven los problemas a menos que realmente se apliquen, y se realice una vigilancia sobre su aplicación. Por otro lado, la seguridad no es un problema donde solo una persona intervenga, sino es algo donde cada individuo que pertenece a una organización debe participar y hacer conciencia de los efectos en caso de cumplir las políticas establecidas. (Mendez-Vilas et al., 2003)

> La implementación de Políticas de Seguridad de la Información es un proceso técnico y administrativo que debe abarcar a toda la organización, por ende, debe estar avalado y contar con un fuerte apoyo de la dirección y/o máxima gerencia, ya que sin este apoyo, su implementación será más compleja e incluso puede fracasar. (Burgos y Campos, 2008, p.241)

Para el diseño de una política de seguridad para el área de TICS del Instituto Tecnológico Superior Central Técnico (ITSCT), se toma como referencia la Norma ISO/IEC 27002:2013 que es una guía de buenas prácticas, que describe los objetivos de control y controles recomendables a seguir dentro del marco de la seguridad de la información.

1.6. Metodología MAGERIT

MAGERIT fue creada con el fin de cumplir con objetivos como conocer el estado de seguridad de los sistemas de información y la implementación de medidas de seguridad, garantizar que no haya elementos que queden fuera del análisis para que haya una profundidad adecuada en el mismo, mitigar las vulnerabilidades y asegurar el desarrollo del sistema en todas las fases de desarrollo. Estos objetivos han posicionado a MAGERIT como una de las metodologías más utilizadas en el ámbito empresarial ya que les permite prepararse para procesos de auditorías, certificaciones y acreditaciones. (Abril, Pulido y Bohada, 2013, p.43)

Según el Consejo Superior de Administración Electrónica (2012), MAGERIT persigue los siguientes objetivos:

Directos:

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.

- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnología de la información y comunicación (TIC)
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.

Indirectos

- Preparar a la organización para procesos de evaluación, auditoria, certificación o acreditación, según corresponda cada caso.

Consejo Superior de Administración Electrónica (2012), indica que la metodología MAGERIT tiene los siguientes pasos:

1.6.1. Determinar los activos relevantes para la organización.

Este primer paso está compuesto por las siguientes actividades:

a) Identificar y definir los activos más relevantes.

b) Clasificar por el tipo de activo.

Los activos se clasifican de la siguiente manera:

- **Datos** que materializan la información.
- **Servicios** auxiliares que se necesitan para poder organizar el sistema.
- **Las aplicaciones informáticas** (Software) que permiten manejar los datos.
- **Los equipos informáticos** (Hardware) y que permiten hospedar datos, aplicaciones y servicios.
- **Los soportes de información** que son dispositivos de almacenamiento de datos.
- **El equipamiento auxiliar** que complementa el material informático.
- **Las redes de comunicaciones** que permiten intercambiar datos.
- **Las instalaciones** que acogen equipos informáticos y de comunicaciones.

- **Las personas** que explotan u operan todos los elementos anteriormente citados.

c) Identificar relaciones existentes con otros activos.

Los activos forman árboles o grafos de dependencias donde la seguridad de los activos que se encuentran más arriba en la estructura o 'superiores' depende de los activos que se encuentran más abajo o 'inferiores'. Estas estructuras reflejan de arriba hacia abajo las dependencias, mientas que de abajo hacia arriba la propagación del daño caso de materializarse las amenazas.

- Activos esenciales.
  - Información que se maneja.
  - Servicios prestados.
- Servicios internos.
  - Que estructuran ordenadamente el sistema de información
  - El equipamiento informático
  - Aplicaciones (software)

d) Determinar las dimensiones de seguridad por activo.

- Su **confidencialidad**: ¿Qué daño causaría que lo conociera quien no debe? Esta valoración es típica de datos.
- Su **integridad**: ¿Qué perjuicio causaría que estuviera dañado o corrupto? Esta valoración es típica de los datos, que pueden estar manipulados, ser total o parcialmente falsos o incluso faltar datos.
- Su **disponibilidad**: ¿Qué perjuicio causaría no tenerlo o no poder utilizarlo? Esta valoración es típica de los servicios.

e) Valoración de los activos desde la perspectiva de la necesidad de proteger.

Una vez determinadas que dimensiones de seguridad interesan de un activo, hay que proceder a valorarlo. La valoración se puede ver desde la perspectiva de la "necesidad de

proteger", pues cuanto más valioso es un activo, mayor nivel de protección requeriremos en la dimensión (o dimensiones) de seguridad que sean pertinentes, considerando que no se hace referencia a lo que cuestan las cosas, sino de lo que valen. Si algo no vale para nada, prescíndase de ello. Si no puede prescindir impunemente de un activo de un activo, es algo que vale; eso es lo que hay que averiguar pues eso es lo que hay que proteger.

La valoración puede ser cuantitativa (con una cantidad numérica) o cualitativa (en alguna escala de niveles). Los criterios más importantes a respetar son:

- La **homogeneidad**: se refiere a la comparación de valores aunque sean de diferentes dimensiones (confidencialidad, disponibilidad e integridad) a fin de poder combinar valores propios y valores acumulados, así como poder determinar si es más grave el daño de una dimensión o en otra.
- La **relatividad**: es importante para poder relativizar el valor de un activo en comparación con otros activos.

1.6.2. Determinar a qué amenazas están expuestos los activos.

Una amenaza es un perjuicio potencial provocado por un incidente deseado o no deseado, hacia todos los activos de una organización empresarial. Si se llegara a ejecutar la amenaza puede poner en peligro la integridad, confidencialidad, autenticidad y disponibilidad de un activo. (Gaona Vásquez, 2013)

Según el (Consejo Superior de Administración Electrónica, 2012a), en este paso se lleva a cabo las siguientes actividades:

1.6.2.1. Identificación de amenazas.

En la identificación de amenazas, se detallan las principales amenazas sobre cada uno de los activos y se debe tener en cuenta el tipo de amenaza que se describe a continuación:

a) De origen natural: terremotos, inundaciones, etc.

b) De origen industrial: hace referencia a desastres industriales (contaminación, fallos eléctricos)

c) Defectos de las aplicaciones: hay aplicaciones que nacen directamente en el equipamiento propio por defectos en su diseño o en su implementación, con consecuencias potencialmente negativas sobre el sistema.

d) Causadas por las personas de forma accidental: Las personas con acceso al sistema de información pueden ser causa de problemas no intencionados, típicamente por error o por omisión.

e) Causadas por las personas de forma deliberada: Las personas con acceso al sistema de información pueden ser causa de problemas intencionados: ataques deliberados; bien con ánimo de beneficiarse indebidamente, bien con ánimo de causar daños y perjuicios a los legítimos propietarios.

No todas las amenazas afectan a todos los activos, sino que hay una cierta relación entre el tipo de activo y lo que podría ocurrir. Cuando un activo es víctima de una amenaza, no se ve afectado en todas sus dimensiones (confidencialidad, disponibilidad e integridad), ni en la misma cuantía.

1.6.2.2. Valoración de las amenazas

Una vez determinado que una amenaza puede perjudicar a un activo, hay que valorar su influencia en el valor del activo. Para hacer una valoración más exacta es necesario estimar la frecuencia de ocurrencia y el porcentaje de degradación.

- **Probabilidad de ocurrencia**: cuán probable o improbable es que se materialice la amenaza. La probabilidad de ocurrencia se evalúa de acuerdo a los siguientes valores:

Tabla 3 *Probabilidad de ocurrencia*

MA	100	Muy frecuente	A diario
A	10	Frecuente	Mensualmente
M	1	Normal	Una vez al año
B	1/10	Poco frecuente	Cada varios años
MB	1/100	Muy poco frecuente	Siglos

Fuente: Consejo Superior de Administración Electrónica, 2012a, p.28 Magerit Libro I

- **Degradación**: mide el daño causado por un incidente en el supuesto que ocurriera. La degradación del valor se lo evalúa en base a los siguientes valores:

Tabla 4 *Degradación del valor*

MA	Muy alta	Casi seguro	Fácil
A	Alta	Muy alto	Medio
M	Media	Possible	Difícil
B	Baja	Poco probable	Muy dificil
MB	Muy baja	Muy raro	Extremadamente difícil

Fuente: Consejo Superior de Administración Electrónica, 2012a, p.28 Magerit Libro I

1.6.3. Estimar el impacto

Definido como el daño sobre el activo derivado de la materialización de la amenaza.

Se puede calcular el impacto en base a tablas sencillas de doble entrada como se muestra en la siguiente figura:

- **MB**: muy bajo
- **B**: bajo
- **M**: medio
- **A**: alto
- **MA**: muy alto

impacto		*degradación*		
		1%	10%	100%
valor	MA	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

Figura 2 Estimar el impacto
Fuente: Consejo Superior de Administración Electrónica, 2012b, p.6
Libro Magerit III

1.6.4. Estimar el riesgo.

Definido como el impacto ponderado con la tasa de ocurrencia de la amenaza.

"Se denomina riesgo a la medida del daño probable sobre un sistema" (Consejo Superior de Administración Electrónica, 2012).

Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia en base a los siguientes valores:

Para calcular el riesgo, se considera los siguientes valores:

escalas		
impacto	probabilidad	riesgo
MA: muy alto	**MA**: prácticamente seguro	**MA**: crítico
A: alto	**A**: probable	**A**: importante
M: medio	**M**: posible	**M**: apreciable
B: bajo	**B**: poco probable	**B**: bajo
MB: muy bajo	**MB**: muy raro	**MB**: despreciable

riesgo		*probabilidad*				
		MB	B	M	A	MA
impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Figura 3 Estimación del riesgo - escala cualitativa
Fuente: Consejo Superior de Administración Electrónica, 2012b, p.7
MAGERIT libro III Versión 3

1.6.5. Determinar que salvaguardas hay dispuestas frente al riesgo.

Se definen las salvaguardas o contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo.

Para la selección de las salvaguardas se debe considerar:

- El tipo de activo a proteger.
- Amenaza a la que está expuesta.
- Dimensión o dimensiones de seguridad que requieren protección.
- Si existen salvaguardas alternativas.

Para excluir una salvaguarda se debe analizar:

- No aplica – se dice cuando una salvaguarda no es de aplicación porque técnicamente no es adecuada al tipo de activos a proteger, no protege la dimensión necesaria o no protege frente a la amenaza en consideración.
- No se justifica – se dice cuando la salvaguarda aplica, pero es desproporcionada al riesgo que tenemos que proteger.

CAPÍTULO III

ANÁLISIS SITUACIONAL

3.1. Instituto Tecnológico Superior Central Técnico

El Instituto Tecnológico Superior Central Técnico (ITSCT), es una institución pública de educación superior creada por el gobierno de DR. Gabriel García Moreno. En octubre del año 2000 mediante el registro institucional Nro. 17-028 otorgado por el Consejo Nacional de Educación Superior (CONESUP), se crea las especialidades de: Electricidad, Electrónica, Mecánica Industrial y Mecánica Automotriz. Actualmente el ITSCT forma parte del Sistema de Educación Superior conforme lo estable el artículo 352 de la Carta Suprema del Estado y el artículo 14 literal b) de la Ley Orgánica de Educación Superior LOES. (ITSCT, n.d.-a)

A partir del 2013 la Secretaría de Educación Superior, Ciencia, Tecnología e Innovación (SENESCYT), realizó las gestiones pertinentes para que el ITSCT no dependa administrativamente del nivel medio. Finalmente, en junio del 2016, el ITSCT se traslada a las instalaciones del SECAP ubicado en la avenida Isaac Albéniz y el Morlán, perteneciente a la parroquia Chaupicruz, cantón Quito y provincia Pichincha.(ITSCT, n.d.-a)

3.2. Misión

"El ITSCT es una Institución de Educación Superior Pública que aporta a la sociedad con talento humano competente, ético y emprendedor para impulsar el sector productivo,

económico y social del país en el marco del Plan Nacional de Desarrollo mediante la investigación, Desarrollo e Innovación (I.D.I).” (ITSCT, n.d.-b).

3.3. Visión

“El ITSCT será reconocido como pionero en la educación tecnológica por su excelencia académica e investigativa, profesionalización del talento humano y la vinculación con la sociedad a nivel nacional e internacional.” (ITSCT, n.d.-b).

3.4. Área de TICS del Instituto Tecnológico Superior Central Técnico

En el área de TICS, se concentra la información personal de docentes, administrativos, como también la información personal y académica de estudiantes en la plataforma académica GIA (Gestión Integral Académica).

El área de TICS no cuenta con estándares o metodologías de seguridad de la información, por tal motivo se desarrollará una política de seguridad de la información basado en la norma ISO/IEC 27002:2013, para esto es necesario analizar, identificar vulnerabilidades y amenazas a la que está expuesta la información mediante una matriz de riesgos para evaluar los riesgos, con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información.

Para este análisis de riesgos, se lleva a cabo la metodología MAGERIT.

3.5. Aplicación de la metodología Magerit para el análisis y valoración del riesgo

3.5.1. Determinar los activos relevantes para la organización

Un activo es un: "Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización" (Consejo Superior de Administración Electrónica, 2012, p.22).

Los activos necesitan protección para asegurar las operaciones del negocio y continuidad de la organización.

Con la autorización (ANEXO 1) del Ing. José Luis Flores Flores, Rector del Instituto Tecnológico Superior Central Técnico (ITSCT), se procedió a recolectar información, para ello se aplicó técnicas de observación directa a las actividades que se realizan en el área de TICS ya que no poseen de procesos documentados, también se realizó una entrevista de seguridad de la información al Ing. Juan Carlos Viera Velasco, coordinador del área de TICS del Instituto Tecnológico Superior Central Técnico (ITSCT), del mismo modo se consideran las inspecciones físicas.

Las actividades realizadas por el área de TICS son:

- Desarrollo del sistema académico de Gestión Integral Académica (GIA), del cual se encuentra ya en producción los módulos de matrículas, registro de asistencia, registro de distributivos, homologaciones, administración de paralelos, cambio de jornada y paralelo, estadísticas y auditoría, agregar/eliminar créditos.
- Del sistema académico de Gestión Integral Académica (GIA), se encuentran desarrollando los módulos de titulación, vinculación con la comunidad, prácticas pre-profesionales, Formación Dual y portafolio digital, registro de convenios del sistema académico de Gestión Integral Académica (GIA), para los procesos de Prácticas pre-

profesionales, Vinculación con la comunidad y Formación Dual por parte de los estudiantes.

- Desarrollo del sistema académico de Gestión Integral Académica (GIA), para el instituto de idiomas del Instituto Tecnológico Superior Central Técnico, del cual ya se encuentra en producción el módulo de matrículas, cambio de jornada y paralelo; se encuentra en desarrollo el módulo de registro de notas.
- Mantenimiento preventivo y correctivo de equipos informáticos de laboratorios.
- Administración de laboratorios informáticos.
- Administración del aula virtual (Moodle).
- Actividades de docencia.

En base a las actividades que se realizan en el área de TICS, con la ayuda del Libro II - Catálogo de Elementos Magerit y el coordinador del área de TICS se identificó los activos más relevantes y se los clasificó de la siguiente manera:

3.5.1.1. [D] Datos / Información.

Los datos son el corazón que permiten al área de TICS prestar sus servicios.

- Base de datos de los sistemas académicos GIA, GIA_IDIOMAS, AULA VIRTUAL (MOODLE).
- Código fuente de los sistemas académicos GIA, GIA_IDIOMAS.

3.5.1.2. [SW] Software – Aplicaciones informáticas.

"Con múltiples denominaciones (programas, aplicativos, desarrollos, etc.), este punto hace referencia a tareas que han sido automatizadas para su desempeño en un equipo informático.

En este punto no se considera el "código fuente" ya que se lo considerará como datos" (Consejo Superior de Administración Electrónica y Amutio Gómez, 2012).

Entre las aplicaciones que ostenta el área de TICS, tenemos:

- De desarrollo propio: GIA, GIA_IDIOMAS.

3.5.1.3. [HW] Equipamiento informático (hardware).

Dícese de los medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta el ITSCT, siendo pues depositarios temporales o permanentes de los datos. Los equipos que posee el área de TICS tenemos:

- Computadoras de escritorio (2)
- Router (1).

3.5.1.4. [L] Instalaciones.

Se refiere a los lugares donde se hospedan los sistemas de información y comunicaciones, el área de TICS del ITSCT se encuentra ubicada en el sector El Inca (av. Isaac Albéniz y el Morlán), en las instalaciones del SECAP.

- Oficina TICS.

3.5.1.5. [AUX] Equipamiento auxiliar.

Se considera a los equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con los datos. El área de TICS cuenta con el siguiente equipamiento auxiliar:

- El área de TICS cuenta con Cableado como equipo auxiliar.

3.5.1.6. [PERSONAL] Personal.

Se considera a las personas relacionadas con los sistemas de información.

- Desarrolladores / programadores.
- Administrador de base de datos.

La valoración de activos se lo realiza en base a la disponibilidad, confidencialidad e integridad, esto indica el valor que tienen los activos para el área de TICS y el Instituto Tecnológico Superior Central Técnico en general.

A continuación se describe brevemente las diferentes dimensiones o parámetros de un activo según Consejo Superior de Administración Electrónica (2012a):

- **Confidencialidad**, garantiza que la información sea accesible solamente a aquellas personas que poseen los permisos respectivos, es decir *¿Qué daño causaría que lo conociera quien no debe?*
- **Integridad**, garantiza que los activos de información estén completos y que no exista modificaciones no autorizadas. *¿Qué perjuicio causaría que estuviera dañado o corrupto?*
- **Disponibilidad**, garantiza que los activos sean accesibles y utilizables por los usuarios que lo requieran. *¿Qué perjuicio causaría no tenerlo o no poder utilizarlo?*

Para la valoración de activos se utilizó la combinación de una escala cuantitativa y una escala cualitativa, donde los criterios van desde un nivel 5, en el cual la valoración ante una pérdida de un activo por alguna amenaza es alta y crítica para el área de TICS, y hacia un nivel 0 que representa pérdidas despreciables o nulas para el área de TICS.

Tabla 5 *Criterios de valoración de activos*

Descripción	**Valor**	**Confidencialidad**	**Integridad**	**Disponibilidad**
Extremo	5	*¿Qué daño causaría que lo conociera quien no debe?*	*¿Qué perjuicio causaría que estuviera dañado o corrupto?*	*¿Qué perjuicio causaría no tenerlo o no poder utilizarlo?*
Muy alto	4			
Alto	3			
Medio	2			
Bajo	1			
Depreciable	0			

Fuente: Consejo Superior de Administración Electrónica y Amutio Gómez, 2012, p.19 MAGERIT Libro II Versión 3

En la siguiente tabla se observa la valoración de los activos bajo los criterios de Disponibilidad, Confidencialidad e Integridad.

Tabla 6 *Valoración de activos*

Activo	Disponibilidad	Confidencialidad	Integridad	Promedio	Valoración
[D] Datos / Información					
Base de datos: GIA, GIA_IDIOMAS, AULA VIRTUAL (MOODLE).	5	5	5	5	Extremo
Código fuente de los sistemas académicos GIA, GIA_IDIOMAS.	5	5	5	5	Extremo
[SW] Software – Aplicaciones informáticas					
De desarrollo propio: GIA, GIA_IDIOMAS.	5	5	5	5	Extremo
[HW] Equipamiento informático					
Computadoras de escritorio	4	4	4	4	Muy alto
Router	1	1	1	1	Bajo
[L] Instalaciones					
Oficina de TICS	3	3	3	3	Alto
[AUX] Equipamiento auxiliar					
Cableado	2	2	2	2	Medio
[PERSONAL] Personal					
Desarrolladores / programadores.	5	5	5	5	Extremo
Administrador de base de datos.	5	5	5	5	Extremo

Fuente: Elaborado por la autora de la investigación.

Para obtener el valor del activo, se promedian las calificaciones aplicadas a las dimensiones o parámetros de integridad, disponibilidad y confidencialidad.

Con esta valoración se identifica los activos que representan mayor relevancia e importancia para el ITSCT, por ende, cuales deberán tener un mayor grado de protección, ya que es necesario tasar su valor en términos de importancia a la gestión tanto académica como administrativa del Instituto Tecnológico Superior Central Técnico.

"La valoración se puede ver desde la perspectiva de la **'necesidad de proteger'** pues cuanto más valioso es un activo, mayor nivel de protección requeriremos en la dimensión (o dimensiones) de seguridad que sean pertinentes" (Consejo Superior de Administración Electrónica, 2012a, p.24).

3.5.2. Determinar a qué amenazas y vulnerabilidades están expuestos los activos

Amenazas

"Una amenaza es la causa potencial de un incidente no deseado, el cual puede causar daño a un sistema o a la organización" (Forum et al., 2013).

Las amenazas pueden originarse de manera accidental o meditada. Una amenaza para poder causar daño al activo, tendría que explotar una vulnerabilidad del sistema, aplicación o servicio.

En la identificación de amenazas, Magerit clasifica las principales amenazas sobre cada uno de los activos de la siguiente forma:

Tabla 7 *Clasificación de amenazas*

AMENAZA	DESCRIPCIÓN
[N] Desastres Naturales	Causada directa o indirecta por accidentes naturales (terremotos, inundaciones,...).
[I] De origen industrial	Sucesos derivados de la actividad humana de tipo industrial (contaminación, fallos eléctricos,...). Estas amenazas pueden darse de forma accidental o meditada.
[E] Errores y fallos no intencionados	Fallos no intencionales causados por las personas con acceso al sistema de información.
[A] Ataques intencionados	Fallos deliberados causados por las personas con acceso al sistema de información.

Fuente: Consejo Superior de Administración Electrónica, 2012a, p.27 MAGERIT libro I Versión 3

Tomando en cuenta esta clasificación, se realiza la identificación de las amenazas en los activos ya especificados en el punto anterior.

3.5.2.1. [D] Datos / Información.

Tabla 8 *Datos / Información*

Nro.	Código	Amenaza	Dimensión de seguridad afectada
Activo: Base de datos: GIA, GIA_IDIOMAS, AULA VIRTUAL (MOODLE).			
1	[E.1]	Errores de los usuarios.	▪ Integridad ▪ Confidencialidad ▪ Disponibilidad
2	[E.2]	Errores del administrador.	▪ Integridad ▪ Confidencialidad ▪ Disponibilidad
3	[E.15]	Alteración accidental de la información.	▪ Integridad
4	[E.18]	Destrucción de la información	▪ Disponibilidad
5	[E.19]	Fugas de información.	▪ Confidencialidad
6	[A.5]	Suplantación de identidad del usuario	▪ Confidencialidad ▪ Integridad
7	[A.6]	Abuso de privilegios de acceso	▪ Integridad ▪ Confidencialidad ▪ Disponibilidad
8	[A.11]	Acceso no autorizado	▪ Confidencialidad ▪ Integridad

Nro.	Código	Amenaza	Dimensión de seguridad afectada
9	[A.15]	Modificación deliberada de la información	▪ Integridad
10	[A.18]	Destrucción de información	▪ Disponibilidad
11	[A.19]	Divulgación de información	▪ Confidencialidad
Activo: Código fuente de los sistemas académicos GIA, GIA_IDIOMAS			
12	[E.15]	Alteración accidental de la información.	▪ Integridad
13	[E.18]	Destrucción de la información	▪ Disponibilidad
14	[A.15]	Modificación deliberada de la información	▪ Integridad
15	[A.18]	Destrucción de información	▪ Disponibilidad
16	[A.19]	Divulgación de información	▪ Confidencialidad

Fuente: Elaborado por la autora de la investigación basado en la metodología Magerit

En la tabla 8, se aprecia que las amenazas presentes en el activo Datos/Información son de tipo Ataques intencionados [A] y Errores y fallos no intencionados [E] afectando así las dimensiones de seguridad, para mitigar estas amenazas se deben considerar una salvaguarda que permita asegurar la integridad, confidencialidad y disponibilidad del activo.

3.5.2.2. [SW] Software – Aplicaciones informáticas.

Tabla 9 *Software – Aplicaciones informáticas*

Nro.	Código	Amenaza	Dimensión de seguridad afectada
Activo: De desarrollo propio: GIA, GIA_IDIOMAS.			
1	[I.5]	Avería de origen físico o lógico	▪ Disponibilidad
2	[E.1]	Error de uso	▪ Integridad ▪ Confidencialidad ▪ Disponibilidad
3	[E.20]	Vulnerabilidades de los programas (software)	▪ Integridad ▪ Confidencialidad ▪ Disponibilidad
4	[A.6]	Abuso de privilegios de acceso	▪ Integridad ▪ Confidencialidad ▪ Disponibilidad
5	[A.19]	Copia ilegal de software	▪ Confidencialidad

Fuente: Elaborado por la autora de la investigación basado en la metodología Magerit

En la tabla 9, se aprecia que las amenazas presentes en el activo Software – Aplicaciones informáticas son de tipo Ataques intencionados [A], Errores y fallos no intencionados [E] y

de Origen industrial [I], afectando así en mayor porcentaje la confidencialidad y disponibilidad del activo, para reducir y/o eliminar el impacto de estas amenazas sobre el activo es necesario generar un control que permita asegurar la integridad, confidencialidad y disponibilidad del mismo.

3.5.2.3. [HW] Equipamiento informático.

Tabla 10 *Equipamiento informático*

Nro.	Código	Amenaza	Dimension de seguridad afectada
Activo: Computadoras de escritorio.			
1	[I.6]	Corte del suministro eléctrico	▪ Disponibilidad
2	[E.2]	Errores del administrador (equivocaciones de personas con responsabilidades de instalación y operación)	▪ Integridad ▪ Confidencialidad ▪ Disponibilidad
3	[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	▪ Disponibilidad
4	[A.6]	Abuso de privilegios de acceso	▪ Integridad ▪ Confidencialidad ▪ Disponibilidad
5	[A.11]	Acceso no autorizado	▪ Integridad ▪ Confidencialidad
Activo: Router.			
1	[I.6]	Corte del suministro eléctrico	▪ Disponibilidad

Fuente: Elaborado por la autora de la investigación basado en la metodología Magerit.

En la tabla 10, se evidencia que las amenazas presentes en el activo Equipamiento informático son de tipo Ataques intencionados [A], Errores y fallos no intencionados [E] y de Origen industrial [I], afectando así en mayor porcentaje su disponibilidad, para reducir y/o eliminar el impacto de estas amenazas es necesario crear un control de seguridad.

3.5.2.4. [L] Instalaciones.

Tabla 11 *Instalaciones*

Nro.	Código	Amenaza	Dimension de seguridad afectada
Activo: Oficina de TICS			
1	[A.11]	Acceso no autorizado	▪ Integridad ▪ Confidencialidad
2	[A.26]	Ataque destructivo (vandalismo, terrorismo)	▪ Disponibilidad

Fuente: Elaborado por la autora de la investigación basado en la metodología Magerit.

En la tabla 11, se constata que la Integridad, Disponibilidad y Confidencialidad del activo Instalaciones son afectadas por amenazas de tipo Ataques intencionados [A], es necesario crear un protocolo de seguridad que permita reducir y/o eliminar el impacto de estas amenazas sobre el activo.

3.5.2.5. [AUX] Equipamiento auxiliar.

Tabla 12 *Equipamiento auxiliar*

Nro	Código	Amenaza	Dimension de seguridad afectada
Activo: Cableado			
1	[N.1]	Fuego	▪ Disponibilidad
2	[N.3]	Contaminación	▪ Disponibilidad
3	[N.6]	Fenómeno climático	▪ Disponibilidad
4	[N.7]	Fenómeno sísmico	▪ Disponibilidad
5	[N.10]	Inundación	▪ Disponibilidad

Fuente Elaborado por la autora de la investigación basado en la metodología Magerit.

En la tabla 12, se aprecia que las amenazas presentes en el activo Equipamiento auxiliar son de tipo Desastres Naturales [N] que comprometen su disponibilidad, para lo cual es necesario crear un control que minimice el impacto de las amenaza sobre el activo.

3.5.2.6. [PERSONAL] Personal.

Tabla 13 *Personal*

Nro	Código	Amenaza	Dimension de seguridad afectada
Activo: Desarrolladores / programadores			
1	[E.7]	Deficiencias en la organización	▪ Disponibilidad
2	[E.19]	Fugas de información	▪ Confidencialidad
Activo: Administrador de base de datos			
4	[E.19]	Fugas de información	▪ Confidencialidad

Fuente: Elaborado por la autora de la investigación basado en la metodología Magerit.

En la tabla 13, se determina que las amenazas presentes en el activo Personal son de tipo Errores y fallos no intencionados [E], comprometiendo así su Disponibilidad y Confidencialidad, para lo cual es necesario crear un protocolo de seguridad para el buen uso y manejo de la información y de esta manera reducir el impacto de estas amenazas sobre el activo.

Vulnerabilidades

Las vulnerabilidades son debilidades asociadas con los activos de la organización que, al ser explotadas por las amenazas, causan incidentes no deseados que pudieran causar pérdidas, daño o deterioro a los activos.

Según Escrivá, Romero y Ramada (2013):

> Vulnerabilidades son las probabilidades que existen de que una amenaza se materialice contra un activo. No todos los activos son vulnerables a las mismas amenazas. Por ejemplo, los datos son vulnerables a la acción de los hackers, mientras que una instalación eléctrica es vulnerable a un cortocircuito. Al hacer el análisis de riesgos hay que tener en cuenta la vulnerabilidad de cada activo.

Con el conocimiento claro del área de TICS, se describen las vulnerabilidades o debilidades encontradas que corresponden a las amenazas de los activos.

Tabla 14 *Amenazas y vulnerabilidades de los activos*

Activo	Amenaza	Vulnerabilidad
Base de datos: GIA, GIA_IDIOMAS, AULA VIRTUAL (MOODLE).	Errores de los usuarios.	Falta de manuales de uso y manejo del sistema
	Errores del administrador.	Características y funciones de base de datos innecesariamente habilitadas.
	Alteración accidental de la información.	Configuración débil y/o por defecto.
	Destrucción de la información	Falta de controles en la desvinculación o cambio de cargo
	Fugas de información.	Características y funciones de base de datos innecesariamente habilitadas.
	Suplantación de identidad del usuario	Contraseñas inseguras
	Abuso de privilegios de acceso	Falta de controles sobre la gestión del cambio.
	Acceso no autorizado	Contraseñas inseguras
	Modificación deliberada de la información	Falta de monitoreo de privilegios
	Destrucción de información	Falta de controles en la desvinculación o cambio de cargo
	Divulgación de información	Falta de controles en la desvinculación o cambio de cargo
Código fuente de los sistemas académicos GIA, GIA_IDIOMAS	Alteración accidental de la información.	Falta de manuales de uso y manejo del sistema
	Destrucción de la información	No hay desactivación de cuentas de usuario luego de finalizado el empleo

Activo	Amenaza	Vulnerabilidad
	Modificación deliberada de la información	No hay desactivación de cuentas de usuario luego de finalizado el empleo
	Destrucción de información	No hay desactivación de cuentas de usuario luego de finalizado el empleo
	Divulgación de información	No hay desactivación de cuentas de usuario luego de finalizado el empleo
De desarrollo propio: GIA, GIA_IDIOMAS.	Avería de origen físico o lógico	Falta de claridad en la definición de requerimientos de seguridad
	Avería de origen físico o lógico	Falta de pruebas al software
	Error de uso	Falta de manuales de uso y manejo del sistema
	Vulnerabilidades de los programas (software)	Falta de consideraciones para desarrollo seguro
	Abuso de privilegios de acceso	Falta de entrenamiento en seguridad de la información
	Copia ilegal de software	Falta de control de desarrollo
Computadoras de escritorio	Corte del suministro eléctrico	Falta de equipos que provean energía ininterrumpida
	Errores del administrador (equivocaciones de personas con responsabilidades de instalación y operación)	Puertos USB habilitados
	Errores del administrador (equivocaciones de personas con responsabilidades de instalación y operación)	Falta de antivirus con licencia

Activo	Amenaza	Vulnerabilidad
	Errores de mantenimiento / actualización de equipos (hardware)	Falta de mantenimiento (Hardware y Software)
	Abuso de privilegios de acceso	Falta de entrenamiento en seguridad de la información
	Acceso no autorizado	Falta de controles de bloqueo
Router	Corte del suministro eléctrico	Falta de equipos que provean energía ininterrumpida
Oficina de TICS	Acceso no autorizado	Falta de controles de acceso físico
	Ataque destructivo (vandalismo, terrorismo)	Falta de condiciones ambientales adecuadas
Cableado	Fuego	Falta de equipos contra incendio
	Contaminación	Falta de protección de acceso físico al cableado de red
	Fenómeno climático	Falta de protección de acceso físico al cableado de red
	Fenómeno sísmico	Falta de protección de acceso físico al cableado de red
	Inundación	Falta de protección de acceso físico al cableado de red
Desarrolladores / programadores	Fugas de información	Falta de controles en la vinculación
Administrador de base de datos	Fugas de información	Falta de controles en la vinculación

Fuente: Elaborado por la autora de la investigación basado en la metodología Magerit.

3.5.3. Estimación del impacto

Una vez determinado que una amenaza puede perjudicar a un activo, hay que valorar su influencia en el valor del activo, en dos sentidos:

- **Degradación**: cuán perjudicado resultaría el activo.

Tabla 15 *Estimación del impacto - Degradación*

5	100%	MA	Muy alta	Casi seguro	Fácil
4	90%	A	Alta	Muy alto	Medio
3	50%	M	Media	Possible	Difícil
2	10%	B	Baja	Poco probable	Muy difícil
1	1%	MB	Muy baja	Muy raro	Extremadamente difícil

Fuente: Elaborado por la autora de la investigación basado en la metodología MAGERIT libro III Versión 3, pág. 7

- **Probabilidad**: cuán probable o improbable es que se materialice la amenaza

Tabla 16 *Estimar el impacto - Probabilidad*

MA	5	Muy frecuente	A diario
A	4	Frecuente	Mensualmente
M	3	Normal	Una vez al año
B	2	Poco frecuente	Cada varios años
MB	1	Muy poco frecuente	Siglos

Fuente: Elaborado por la autora de la investigación basado en la metodología MAGERIT libro III Versión 3, pág. 7

Tabla 17 *Mapa de calor de estimación del impacto*

Impacto		**Degradación**				
		1 (MB)	**10% (B)**	**50% (M)**	**90% (A)**	**100% (MA)**
Probabilidad	**MA**	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Fuente: Elaborado por la autora de la investigación basado en la metodología MAGERIT libro III Versión 3, pág. 6

A continuación se detalla la valoración del impacto de las amenazas y vulnerabilidades identificadas sobre los activos.

Tabla 18 *Estimación del impacto*

ESTIMACIÓN DEL IMPACTO						
Activo	**Código**	**Amenaza**	**Vulnerabilidad**	**Degradación**	**Probabilidad**	**Impacto**
Base de datos: GIA, GIA_IDIOMAS, AULA VIRTUAL (MOODLE).	[E.1]	Errores de los usuarios.	Falta de manuales de uso y manejo del sistema	M	MB	**M**
	[E.2]	Errores del administrador.	Características y funciones de base de datos innecesariamente habilitadas.	A	MB	**B**
	[E.15]	Alteración accidental de la información.	Configuración débil y/o por defecto.	MA	M	**A**
	[E.18]	Destrucción de la información	Falta de controles en la desvinculación o cambio de cargo	MA	MB	**B**
	[E.19]	Fugas de información.	Características y funciones de base de datos innecesariamente habilitadas.	A	M	**A**
	[A.5]	Suplantación de identidad del usuario	Contraseñas inseguras	A	MB	**B**

ESTIMACIÓN DEL IMPACTO						
Activo	**Código**	**Amenaza**	**Vulnerabilidad**	**Degradación**	**Probabilidad**	**Impacto**
	[A.6]	Abuso de privilegios de acceso	Falta de controles sobre la gestión del cambio.	A	B	**M**
	[A.11]	Acceso no autorizado	Contraseñas inseguras	A	MB	**B**
	[A.15]	Modificación deliberada de la información	Falta de monitoreo de privilegios	A	M	**A**
	[A.18]	Destrucción de información	Falta de controles en la desvinculación o cambio de cargo	A	MB	**B**
	[A.19]	Divulgación de información	Falta de controles en la desvinculación o cambio de cargo	A	MB	**B**
Código fuente de los sistemas académicos GIA,	[E.15]	Alteración accidental de la información.	Falta de manuales de uso y manejo del sistema	MA	MB	**B**

ESTIMACIÓN DEL IMPACTO						
Activo	**Código**	**Amenaza**	**Vulnerabilidad**	**Degradación**	**Probabilidad**	**Impacto**
GIA_IDIOMAS	[E.18]	Destrucción de la información	No hay desactivación de cuentas de usuario luego de finalizado el empleo	MA	MB	**B**
	[A.15]	Modificación deliberada de la información	No hay desactivación de cuentas de usuario luego de finalizado el empleo	MA	MB	**B**
	[A.18]	Destrucción de información	No hay desactivación de cuentas de usuario luego de finalizado el empleo	MA	MB	**B**
	[A.19]	Divulgación de información	No hay desactivación de cuentas de usuario luego de finalizado el empleo	MA	MB	**B**
De desarrollo propio: GIA, GIA_IDIOMAS.	[I.5]	Avería de origen físico o lógico	Falta de claridad en la definición de requerimientos de seguridad	A	M	**A**
	[I.5]	Avería de origen físico o lógico	Falta de pruebas al software	A	A	**MA**
	[E.1]	Error de uso	Falta de manuales de uso y manejo del sistema	M	M	**M**

ESTIMACIÓN DEL IMPACTO						
Activo	**Código**	**Amenaza**	**Vulnerabilidad**	**Degradación**	**Probabilidad**	**Impacto**
	[E.20]	Vulnerabilidades de los programas (software)	Falta de consideraciones para desarrollo seguro	M	M	**M**
	[A.6]	Abuso de privilegios de acceso	Falta de entrenamiento en seguridad de la información	M	M	**M**
	[A.19]	Copia ilegal de software	Falta de control de desarrollo	B	B	**B**
Computadoras de escritorio	[I.6]	Corte del suministro eléctrico	Falta de equipos que provean energía ininterrumpida	B	B	**B**
	[E.2]	Errores del administrador (equivocaciones de personas con responsabilidades de instalación y operación)	Puertos USB habilitados	B	B	**B**

ESTIMACIÓN DEL IMPACTO						
Activo	**Código**	**Amenaza**	**Vulnerabilidad**	**Degradación**	**Probabilidad**	**Impacto**
	[E.2]	Errores del administrador (equivocaciones de personas con responsabilidades de instalación y operación)	Falta de antivirus con licencia	MA	MA	**MA**
	[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Falta de mantenimiento (Hardware y Software)	M	M	**M**
	[A.6]	Abuso de privilegios de acceso	Falta de entrenamiento en seguridad de la información	M	M	**M**
	[A.11]	Acceso no autorizado	Falta de controles de bloqueo	M	M	**M**
Router	[I.6]	Corte del suministro eléctrico	Falta de equipos que provean energía ininterrumpida	M	M	**M**
Oficina de TICS	[A.11]	Acceso no autorizado	Falta de controles de acceso físico	A	A	**MA**

ESTIMACIÓN DEL IMPACTO						
Activo	**Código**	**Amenaza**	**Vulnerabilidad**	**Degradación**	**Probabilidad**	**Impacto**
	[A.26]	Ataque destructivo (vandalismo, terrorismo)	Falta de condiciones ambientales adecuadas	M	MA	**MA**
Cableado	[N.1]	Fuego	Falta de equipos contra incendio	M	MA	**MA**
	[N.3]	Contaminación	Falta de protección de acceso físico al cableado de red	M	B	**B**
	[N.6]	Fenómeno climático	Falta de protección de acceso físico al cableado de red	M	B	**B**
	[N.7]	Fenómeno sísmico	Falta de protección de acceso físico al cableado de red	M	B	**B**
	[N.10]	Inundación	Falta de protección de acceso físico al cableado de red	M	B	**B**
Desarrolladores / programadores	[E.19]	Fugas de información	Falta de controles en la vinculación	M	B	**B**
Administrador de base de datos	[E.19]	Fugas de información	Falta de controles en la vinculación	M	B	**B**

Fuente: Elaborado por la autora de la investigación basado en la metodología MAGERIT libro III Versión 3

En la tabla 18, se puede apreciar que los activos con mayor impacto en caso de que se materialice la amenaza son:

- Base de datos: GIA, GIA_IDIOMAS, AULA VIRTUAL (MOODLE).
- Software de desarrollo propio: GIA, GIA_IDIOMAS.
- Computadoras de escritorio.
- Oficina de tics y
- Cableado

3.5.4. Estimación del riesgo

Según el Consejo Superior de Administración Electrónica (2012):

El riesgo crece con el impacto y con la probabilidad, pudiendo distinguirse una serie de zonas a tener en cuenta en el tratamiento del riesgo.

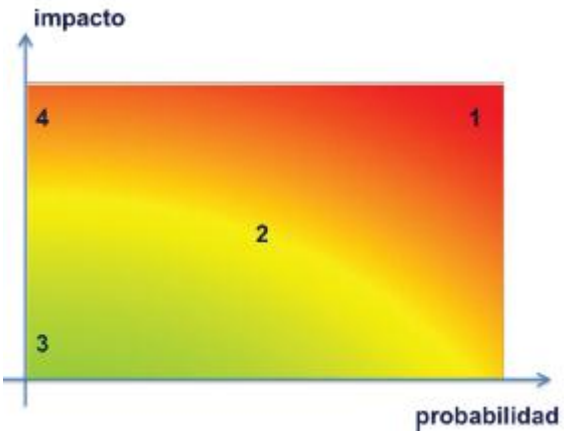

Figura 4 El riesgo en función del impacto y la probabilidad
Fuente: Consejo Superior de Administración Electrónica, 2012a, p.30 MAGERIT libro I Versión 3

- **Zona 1**: riesgos muy probables y de muy alto impacto.
- **Zona 2**: franja amarilla: cubre un amplio rango desde situaciones improbables y de impacto medio, hasta situaciones muy probables pero de impacto bajo o muy bajo.
- **Zona 3**: riesgos improbables y de bajo impacto.

- **Zona 4**: riesgos improbables pero de muy alto impacto.

Definir un rango de valores de riesgo ayuda a la institución a la toma de decisiones, determinando los riesgos a tratar y la prioridad para la implementación del tratamiento.

La probabilidad de impacto y la ocurrencia del riesgo en la matriz de riesgos, fueron ponderadas por el coordinador del área de TICS del Instituto Tecnológico Superior Central Técnico (ITSCT) en base a la siguiente tabla de valores:

Tabla 19 *Estimación del riesgo*

Impacto	Probabilidad	Riesgo
MA: muy alto	MA: prácticamente seguro	MA: critico, daño extremadamente grave.
A: alto	A: probable	A: importante, daño grave
M: medio	M: posible	M: apreciable, daño importante.
B: bajo	B: poco probable	B: bajo, daño menor.
MB: muy bajo	MB: muy raro	MB: despreciable, irrelevante a efectos prácticos.

Fuente: Elaborado por la autora de la investigación basado en la metodología MAGERIT libro III Versión 3, pág. 7

Tabla 20 *Matriz de riesgos*

MATRIZ DE RIESGO - ÁREA DE TICS DEL INSTITUTO TECNOLÓGICO SUPERIOR CENTRAL TÉCNICO								
Activo	**Código**	**Código Riesgo**	**Amenaza**	**Vulnerabilidad**	**Impacto**	**Probabilidad de ocurrencia**	**Evaluación del riesgo**	**Controles aplicables ISO/IEC27002:2013**
								Controles
Base de datos: GIA, GIA_IDIOMAS, AULA VIRTUAL (MOODLE).	[E.1]	R1	Errores de los usuarios.	Falta de manuales de uso y manejo del sistema	M	A	**A**	12.1.1 Documentación de procedimientos de operación
	[E.2]	R2	Errores del administrador.	Características y funciones de base de datos innecesariamente habilitadas.	B	A	**M**	12.1.1 Documentación de procedimientos de operación
	[E.15]	R3	Alteración accidental de la información.	Configuración débil y/o por defecto.	A	B	**A**	9.1.1 Política de control de accesos
	[E.18]	R4	Destrucción de la información	Falta de controles en la desvinculación o cambio de cargo	B	MB	**MB**	9.2.6 Retirada o adaptación de los derechos de acceso
	[E.19]	R5	Fugas de información.	Características y funciones de base de datos innecesariamente habilitadas.	A	MB	**M**	7.2.2 Concienciación, educación y capacitación en seguridad de la información

MATRIZ DE RIESGO - ÁREA DE TICS DEL INSTITUTO TECNOLÓGICO SUPERIOR CENTRAL TÉCNICO								
Activo	**Código**	**Código Riesgo**	**Amenaza**	**Vulnerabilidad**	**Impacto**	**Probabilidad de ocurrencia**	**Evaluación del riesgo**	**Controles aplicables ISO/IEC27002:2013**
								Controles
	[A.5]	R6	Suplantación de identidad del usuario	Contraseñas inseguras	B	MB	**MB**	9.1.1 Política de control de accesos 9.4.2 Procedimientos seguros de inicio de sesión
	[A.6]	R7	Abuso de privilegios de acceso	Falta de controles sobre la gestión del cambio.	M	MB	**B**	14.2.2 Procedimientos de control de cambios en los sistemas.
	[A.11]	R8	Acceso no autorizado	Contraseñas inseguras	B	MB	**MB**	9.1.1 Política de control de accesos 9.4.2 Procedimientos seguros de inicio de sesión
	[A.15]	R9	Modificación deliberada de la información	Falta de monitoreo de privilegios	A	MB	**M**	9.2.3 Gestión de los derechos a acceso con privilegios especiales
	[A.18]	R10	Destrucción de información	Falta de controles en la desvinculación o cambio de cargo	B	MB	**MB**	9.2.6 Retirada o adaptación de los derechos de acceso

MATRIZ DE RIESGO - ÁREA DE TICS DEL INSTITUTO TECNOLÓGICO SUPERIOR CENTRAL TÉCNICO								
Activo	**Código**	**Código Riesgo**	**Amenaza**	**Vulnerabilidad**	**Impacto**	**Probabilidad de ocurrencia**	**Evaluación del riesgo**	**Controles aplicables ISO/IEC27002:2013**
								Controles
	[A.19]	R11	Divulgación de información	Falta de controles en la desvinculación o cambio de cargo	B	B	**B**	9.2.6 Retirada o adaptación de los derechos de acceso
Código fuente de los sistemas académicos GIA, GIA_IDIOMAS	[E.15]	R12	Alteración accidental de la información.	Falta de manuales de uso y manejo del sistema	B	MB	**MB**	12.1.1 Documentación de procedimientos de operación
	[E.18]	R13	Destrucción de la información	No hay desactivación de cuentas de usuario luego de finalizado el empleo	B	MB	**MB**	9.2.1 Gestión de altas/bajas en el registro de usuarios
	[A.15]	R14	Modificación deliberada de la información	No hay desactivación de cuentas de usuario luego de finalizado el empleo	B	MB	**MB**	9.2.1 Gestión de altas/bajas en el registro de usuarios
	[A.18]	R15	Destrucción de información	No hay desactivación de cuentas de usuario luego de finalizado el empleo	B	MB	**MB**	9.2.1 Gestión de altas/bajas en el registro de usuarios
	[A.19]	R16	Divulgación de información	No hay desactivación de cuentas de usuario luego de finalizado el	B	MB	**MB**	9.2.1 Gestión de altas/bajas en el registro de usuarios

MATRIZ DE RIESGO - ÁREA DE TICS DEL INSTITUTO TECNOLÓGICO SUPERIOR CENTRAL TÉCNICO								
Activo	**Código**	**Código Riesgo**	**Amenaza**	**Vulnerabilidad**	**Impacto**	**Probabilidad de ocurrencia**	**Evaluación del riesgo**	**Controles aplicables ISO/IEC27002:2013**
								Controles
				empleo				
De desarrollo propio: GIA, GIA_IDIOMAS.	[I.5]	R17	Avería de origen físico o lógico	Falta de claridad en la definición de requerimientos de seguridad	A	B	**A**	14.2.2 Procedimientos de control de cambios en los sistemas
	[I.5]	R18	Avería de origen físico o lógico	Falta de pruebas al software	MA	B	**MA**	14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas 14.2.9 Pruebas de aceptación
	[E.1]	R19	Error de uso	Falta de manuales de uso y manejo del sistema	M	M	**M**	12.1.1 Documentación de procedimientos de operación
	[E.20]	R20	Vulnerabilidades de los programas (software)	Falta de consideraciones para desarrollo seguro	M	B	**M**	12.1.4 Separación de entornos de desarrollo, prueba y producción 14.2.1 Política de desarrollo seguro de software
	[A.6]	R21	Abuso de privilegios de acceso	Falta de entrenamiento en seguridad de la información	M	MB	**B**	7.2.2 Concienciación, educación y capacitación en seguridad de la información

MATRIZ DE RIESGO - ÁREA DE TICS DEL INSTITUTO TECNOLÓGICO SUPERIOR CENTRAL TÉCNICO								
Activo	**Código**	**Código Riesgo**	**Amenaza**	**Vulnerabilidad**	**Impacto**	**Probabilidad de ocurrencia**	**Evaluación del riesgo**	**Controles aplicables ISO/IEC27002:2013**
								Controles
	[A.19]	R22	Copia ilegal de software	Falta de control de desarrollo	B	MB	**MB**	14.2.1 Política de desarrollo seguro de software. 14.2.6 Seguridad en entornos de desarrollo.
Computadoras de escritorio	[I.6]	R23	Corte del suministro eléctrico	Falta de equipos que provean energía ininterrumpida	B	MB	**MB**	11.2.2 Instalaciones de suministro
	[E.2]	R24	Errores del administrador (equivocaciones de personas con responsabilidades de instalación y operación)	Puertos USB habilitados	B	B	**MB**	9.3.1 Uso de información confidencial para su autenticación 16.1.3 Notificación de puntos débiles de la seguridad 16.1.5 Respuesta a los incidentes de seguridad
	[E.2]	R25	Errores del administrador (equivocaci	Falta de antivirus con licencia	MA	B	**MA**	12.2.1 Controles contra código malicioso

MATRIZ DE RIESGO - ÁREA DE TICS DEL INSTITUTO TECNOLÓGICO SUPERIOR CENTRAL TÉCNICO								
Activo	**Código**	**Código Riesgo**	**Amenaza**	**Vulnerabilidad**	**Impacto**	**Probabilidad de ocurrencia**	**Evaluación del riesgo**	**Controles aplicables ISO/IEC27002:2013**
								Controles
			ones de personas con responsabilidades de instalación y operación)					
	[E.23]	R26	Errores de mantenimiento / actualización de equipos (hardware)	Falta de mantenimiento (Hardware y Software)	M	B	**M**	11.2.4 Mantenimiento de los equipos
	[A.6]	R27	Abuso de privilegios de acceso	Falta de entrenamiento en seguridad de la información	M	B	**M**	7.2.2 Concienciación, educación y capacitación en seguridad de la información
	[A.11]	R28	Acceso no autorizado	Falta de controles de bloqueo	M	MB	**B**	9.3.1 Uso de información confidencial para su autenticación 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla

MATRIZ DE RIESGO - ÁREA DE TICS DEL INSTITUTO TECNOLÓGICO SUPERIOR CENTRAL TÉCNICO								
Activo	**Código**	**Código Riesgo**	**Amenaza**	**Vulnerabilidad**	**Impacto**	**Probabilidad de ocurrencia**	**Evaluación del riesgo**	**Controles aplicables ISO/IEC27002:2013**
								Controles
Router	[I.6]	R29	Corte del suministro eléctrico	Falta de equipos que provean energía ininterrumpida	M	MB	**B**	11.2.2 Instalaciones de suministro
Oficina de TICS	[A.11]	R30	Acceso no autorizado	Falta de controles de acceso físico	MA	MB	**A**	11.1.2 Controles físicos de entrada
	[A.26]	R31	Ataque destructivo (vandalismo, terrorismo)	Falta de condiciones ambientales adecuadas	MA	MB	**A**	11.1.4 Protección contra las amenazas externas y ambientales
Cableado	[N.1]	R32	Fuego	Falta de equipos contra incendio	MA	MB	**A**	11.1.4 Protección contra las amenazas externas y ambientales
	[N.3]	R33	Contaminación	Falta de protección de acceso físico al cableado de red	B	MB	**MB**	11.2.3 Seguridad del cableado
	[N.6]	R34	Fenómeno climático	Falta de protección de acceso físico al cableado de red	B	MB	**MB**	11.2.3 Seguridad del cableado
	[N.7]	R35	Fenómeno sísmico	Falta de protección de acceso físico al cableado de red	B	MB	**MB**	11.2.3 Seguridad del cableado

MATRIZ DE RIESGO - ÁREA DE TICS DEL INSTITUTO TECNOLÓGICO SUPERIOR CENTRAL TÉCNICO								
Activo	**Código**	**Código Riesgo**	**Amenaza**	**Vulnerabilidad**	**Impacto**	**Probabilidad de ocurrencia**	**Evaluación del riesgo**	**Controles aplicables ISO/IEC27002:2013**
								Controles
	[N.10]	R36	Inundación	Falta de protección de acceso físico al cableado de red	B	MB	**MB**	11.2.3 Seguridad del cableado
Desarrolladores / programadores	[E.19]	R37	Fugas de información	Falta de controles en la vinculación	B	B	**B**	7.2.2 Concienciación, educación y capacitación en seguridad de la información
Administrador de base de datos	[E.19]	R38	Fugas de información	Falta de controles en la vinculación	B	B	**B**	7.2.2 Concienciación, educación y capacitación en seguridad de la información

Fuente: Elaborado por la autora de la investigación basado en la metodología MAGERIT libro III Versión 3

Este mapa de calor del riesgo permite clasificar y visualizar los riesgos, mediante la combinación de las categorías de probabilidad e impacto.

Tabla 21 *Mapa de calor*

Riesgo		**Probabilidad**				
		MB	**B**	**M**	**A**	**MA**
Impacto	**MA**	R30, R31, R32	R18, R25			
	A	R5, R9	R3, R17			
	M	R7,R21, R28, R29	R20, R26, R27	R19	R1	
	B	R4, R6,R8, R10, R12, R13,R14, 15, R16, R22, R23, r33, R34, R35, R36	R11, R24, R37, R38		R2	
	MB					

Fuente: Elaborado por la autora de la investigación

En base a lo consignado en la Tabla 20, los activos con riesgo extrema deben ser llevados por lo menos al nivel Moderado, y aquellos activos críticos con nivel de riesgo moderado deben ser llevados al nivel bajo.

Tabla 22 *Aceptación del riesgo*

Tolerancia/Aceptación			
B	Zona de riesgo	Baja	Supervisar y revisar como sea necesario. Riesgos improbables y de bajo impacto
M	Zona de riesgo	Moderada	Evaluar el riesgo y determinar si los controles implementados son suficientes y si están siendo efectivos. Cubre un amplio rango desde situaciones improbables y de impacto medio, hasta situaciones muy probables pero de impacto bajo o muy bajo
A	Zona de riesgo	Alta	Debe otorgarse la atención apropiada. Riesgos improbables pero de muy alto impacto.
MA	Zona de riesgo	Extrema	Requiere respuesta y atención inmediata. Riesgos muy probables y de muy alto impacto

Fuente: Elaborado por la autora de la investigación basado en la metodología MAGERIT libro I Versión 3, pág. 30

3.5.5. Determinar que salvaguardas hay dispuestas frente al riesgo.

El objetivo de las salvaguardas o controles es reducir la probabilidad de una amenaza y limitar la posible degradación que un activo puede sufrir.

Para el desarrollo de esta sección, se utiliza el Anexo 2 de la norma de seguridad ISO/IEC 27002:2013, de acuerdo al activo, amenaza y vulnerabilidad y al resultado obtenido del riesgo, se establece el control respectivo.

Tabla 23 *Norma ISO/IEC 27002:2013*

Dominio	Objetivo de control	Controles
5. POLÍTICAS DE SEGURIAD	5.1 Directrices de la dirección en seguridad de la información.	5.1.1 Conjunto de políticas para la seguridad de la información. 5.1.2 Revisión de las políticas para la seguridad de la información.
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	6.1. Organización interna.	6.1.1 Asignación de responsabilidades para la seguridad de la información 6.1.2 Segregación de tareas
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	7.2 Durante la contratación	7.2.2 Concienciación, educación y capacitación en seguridad de la información.
	7.3 Cese o cambio de puesto de trabajo	7.3.1 Cese o cambio de puesto de trabajo.
9. CONTROL DE ACCESOS	9.1 Requisitos de negocio para el control de accesos.	9.1.1 Política de control de accesos
	9.2 Gestión de acceso de usuarios	9.2.1 Gestión de altas/bajas en el registro de usuarios 9.2.3 Gestión de los derechos a acceso con privilegios especiales 9.2.6 Retirada o adaptación de los derechos de acceso
	9.3 Responsabilidades del usuario	9.3.1 Uso de información confidencial para su
	9.4 Control de acceso a sistemas y aplicaciones	9.4.2 Procedimientos seguros de inicio de sesión.
11 SEGURIDAD FÍSICA Y AMBIENTAL	11.1 Áreas seguras	11.1.2 Controles físicos de entrada 11.1.4 Protección contra las amenazas externas y ambientales
	11.2 Seguridad en los equipos	11.2.2 Instalaciones de suministro 11.2.3 Seguridad del cableado. 11.2.4 Mantenimiento de los equipos.

Dominio	Objetivo de control	Controles
		11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla
12. SEGURIDAD EN LA OPERATIVA	12. 1 Responsabilidades y procedimientos de operación	12.1.1 Documentación de procedimientos de operación. 12.1.4 Separación de entornos de desarrollo, prueba y producción
	12.2 Protección contra código malicioso	12.2.1 Controles contra código malicioso
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	14.2 Seguridad en los procesos de desarrollo y soporte	14.2.1 Política de desarrollo seguro de software. 14.2.2 Procedimientos de control de cambios en los sistemas. 14.2.6 Seguridad en entornos de desarrollo. 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas. 14.2.9 Pruebas de aceptación.
16 GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN	16.1 Gestión de incidentes en la seguridad de la información y mejoras	16.1.3 Notificación de puntos débiles de la seguridad 16.1.5 Respuesta a los incidentes de seguridad

Fuente: NORMA ISO/IEC 27002:2013

CAPÍTULO IV

PROPUESTA

Después de evaluar los riesgos del área de TICS del Instituto Tecnológico Superior Central Técnico (TSCT) y con los parámetros estipulados por la normativa ISO/IEC-27002:2013 se realiza una política de seguridad de los puntos que denotan falencia en el área y de esta manera lograr fortalecer en las actividades la seguridad de la información.

4.1. Introducción

ISOTools Excellence, n.d., afirma. "La norma ISO/IEC 27002 anteriormente denominada ISO 17799, es un estándar para la seguridad de la información publicado por la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional. La versión más reciente es la ISO/IEC 27002:2013".

Esta norma proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad dela información.

El Instituto Tecnológico Superior Central Técnico (ITSCT), es una institución de educación superior, y en el área de TICS se concentra la información personal de docentes, administrativos, como también la información personal y académica de estudiantes en las plataformas académicas como son el GIA, GIA_IDIOMAS y MOODLE. La información es un recurso de gran valor como el resto de los activos, por ende debe ser debidamente protegida para minimizar la probabilidad de ocurrencia e impacto de los riesgos asociados

con las vulnerabilidades y amenazas de seguridad de la información existentes en el área de TICS del Instituto Tecnológico Superior Central Técnico (ITSCT), y garantizar de mejor manera la gestión y continuidad del Instituto.

El diseño de una política de seguridad para el área de TICS del Instituto Tecnológico Superior Central Técnico (ITSCT) basado en la Norma de seguridad ISO/IEC 27002:2013, nace de la necesidad de contar con una metodología de calidad para la seguridad de la información con el objetivo de garantizar la confidencialidad, integridad y disponibilidad de la misma.

4.2. Alcance

El presente documento establece la política de seguridad de la información únicamente para el área de TICS del Instituto Tecnológico Superior Central Técnico (ITSCT).

Este protocolo de seguridad de la información servirá para concientizar a los integrantes del área de TICS y a todos los usuarios del ITSCT, la necesidad del buen uso y manejo de las tecnologías de la información, dando a conocer las responsabilidades y medidas que se deben adoptar para proteger la infraestructura tecnológica y evitar pérdidas y/o divulgación no autorizada de la información.

4.3. Definiciones

a) **Activo**: "Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización" (Consejo Superior de Administración Electrónica, 2012a, p.22)

b) **Seguridad de la información**: Protección que se brinda a los activos de información mediante medidas preventivas con el fin de asegurar la continuidad del negocio y evitar o mitigar la materialización de las amenazas.

c) **Confidencialidad**, garantiza que la información sea accesible solamente a aquellas personas que poseen los permisos respectivos.

d) **Integridad**, garantiza que los activos de información estén completos y que no exista modificaciones no autorizadas.

e) **Disponibilidad**, garantiza que los activos sean accesibles y utilizables por los usuarios que lo requieran.

f) **Política**: Una política de seguridad son un conjunto de directrices, normas, procedimientos instrucciones que guía las instrucciones de trabajo y definen los criterios de seguridad para que sean adoptados a nivel local o institucional, con el objetivo de establecer, estandarizar y normalizar la seguridad tanto en el ámbito humano como tecnológico. (Dussan Clavijo, 2006)

g) **Usuario**: personal que utiliza los recursos informáticos y que interactúan en forma activa en un proceso (docentes, administrativos y estudiantes).

h) **Aplicación académica**: Gestión Integral Académica (GIA y GIA_IDIOMAS) software desarrollado por el área de TICS.

4.4. Responsabilidades

a. Responsable y con autoridad para aprobar, actualizar y vigilar el cumplimiento de estas políticas: Coordinador del área de TICS.

b. Responsable y con autoridad para implementar estas políticas: Rector del Instituto Tecnológico Superior Central Técnico (ITSCT)

c. Responsables de conocer y aplicar estas políticas: área de TICS.

4.5. Referencias

a. ISO/IEC 27002:2013.Guía de buenas prácticas, que describe los objetivos de control y controles recomendables a seguir dentro del marco de la seguridad de la información (ISO/IEC 27002:2013, 2013).

4.6. Políticas específicas de seguridad de la información

4.6.1. Política de seguridad

Objetivo.

Establecer un protocolo para el uso y manejo correcto de los activos de información que permitan mitigar el riesgo de pérdida, alteración de la información, accesos no autorizados a los sistemas académicos e instalaciones donde reposan los equipos de procesamiento de la información, divulgación no controlada, duplicación e interrupción intencional de la información.

4.6.1.1. Directrices de la dirección en seguridad de la información

Conjunto de políticas para la seguridad de la información.

Artículo 1. El coordinador del área de TICS debe aprobar un documento (Anexo 4) de política de seguridad de la información, y comunicar al personal docente y administrativo del área de TICS del Instituto Tecnológico Superior Central Técnico (ITSCT).

Revisión de las políticas para la seguridad de la información

Artículo 2. La política de seguridad debe ser documentada, revisada, actualiza y socializada en intervalos de tiempo planificados o si ocurren cambios significativos, para evitar el acceso no autorizado a los sistemas de información y bases de datos que pongan en peligro la información del personal docente, administrativo y estudiantes, de esta forma asegurar su continua idoneidad, eficiencia y efectividad.

4.6.2. Aspectos organizativos de la seguridad de la información

Objetivo

"Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización" (Inen, 2017, p.4).

4.6.2.1. Organización interna.

Asignación de responsabilidades para la seguridad de la información.

Artículo 3. El coordinador del área de TICS puede delegar por escrito actividades de seguridad de la información a uno o varios integrantes del área de TICS los cuales deben ser competentes en tema, siempre y cuando se hayan identificado los activos de información y definido los procesos de seguridad de la información.

Artículo 4. El coordinador de TICS debe verificar que todas las actividades de seguridad de la información hayan sido ejecutadas correctamente.

Segregación de tareas.

Artículo 5. El coordinador del área de TICS, debe asignar un responsable por cada tarea en el área, con el propósito de mantener un correcto control sobre los activos de información para evitar accesos no autorizados, modificación de la información y/o utilizar los activos sin autorización o sin que se detecte.

Artículo 6. El área de TICS debe considerar controles de monitorización de actividades realizadas por cada uno de los integrantes del área de TICS para verificar que se cumplan adecuadamente.

4.6.3. Seguridad ligada a los recursos humanos

Objetivo.

Asegurar que los usuarios conozcan en cuanto a la seguridad de la información para reducir el riesgo de robo, fraude o uso inadecuado de la misma.

4.6.3.1. Antes de la contratación

Términos y condiciones de contratación

Artículo 7. Los integrantes del área de TICS deben firmar un compromiso (Anexo 4) de confidencialidad y no revelación de información, debido a que en esta área se maneja información sensible de usuarios del Instituto Tecnológico Superior Central Técnico.

4.6.3.2. Durante la contratación

Concienciación, educación y capacitación en seguridad de la información

Artículo 8. El Instituto Tecnológico Superior Central Técnico (ITSCT), a través del área de TICS, deberá brindar mediante charlas periódicas una adecuada educación, concienciación y formación sobre las políticas de seguridad de la información y el uso correcto de los servicios de procesamiento de información antes de obtener acceso a la información o los servicios.

Artículo 9. El Instituto Tecnológico Superior Central Técnico (ITSCT), a través del área de TICS, deberá brindar capacitaciones a los usuarios al inicio de cada semestre académico acerca del uso y manejo de las aplicaciones académicas que se manejan en el Instituto, dichas capacitaciones se deberán realizar en ambientes de prueba y/o simuladores y así reducir el riesgo de error humano.

Artículo 10. El coordinador del área de TICS designará a los usuarios que dominen el tema de en seguridad de la información para realizar las capacitaciones en cada carrera del Instituto.

Artículo 11. Las capacitaciones de seguridad de la información deberán contar con el material de apoyo acorde a la capacitación y este deberá ser proporcionado a los usuarios.

Artículo 12. Es deber de los usuarios del Instituto asistir a las capacitaciones, así como también acatar cada una de las disposiciones dispuestas en cada una de ellas.

Artículo 13. Es responsabilidad de los usuarios del Instituto cumplir las Políticas y Estándares de Seguridad de la Información establecidos en el presente Manual.

Cese o cambio de puesto de trabajo.

Artículo 14. El área de Recursos Humanos del Instituto Tecnológico Superior Central Técnico (ITSCT), debe notificar inmediatamente la renuncia o desvinculación del docente y/o administrativo al área de TICS, para que está proceda a dar de baja al (los) usuario (s) de los sistemas informáticos. Los usuarios que no cumpla esta política se responsabilizan de las acciones que se generen por la omisión.

Artículo 15. El área de Recursos Humanos del Instituto Tecnológico Superior Central Técnico (ITSCT), debe notificar inmediatamente el inicio y fin de los periodos de vacaciones de docentes y/o administrativos del Instituto, para que está proceda a dar de baja al (los) mismos (s) de los sistemas académicos durante las fechas indicadas. Los usuarios que no cumplan esta política se responsabilizan de las acciones que se generen por la omisión.

Artículo 16. El área de TICS del Instituto Tecnológico Superior Central Técnico (ITSCT), debe comunicar las responsabilidades y obligaciones en seguridad de la información que siguen vigentes después del cambio de puesto de trabajo del docente y/o administrativo del Instituto.

Artículo 17. Los activos asignados al personal del área de TICS que finalicen su relación laboral deben ser devueltos en las condiciones y estado que fueron entregados al departamento respectivo para el control de inventarios.

4.6.4. Control de accesos

Objetivo.

Limitar el acceso a la información, sistemas, servicios e instalaciones de procesamiento de información del Instituto Tecnológico Superior Central Técnico.

4.6.4.1. Requisitos de negocio para el control de accesos

Política de control de accesos

Artículo 18. El coordinador del área de TICS proporcionará a los usuarios el manual de usuario para el correcto uso y manejo de los sistemas académicos.

Artículo 19. Obligar a los docentes, administrativos y estudiantes a cambiar las contraseñas temporales en su primer procedimiento de identificación en las aplicaciones académicas.

Artículo 20. Evitar mostrar las contraseñas en pantalla, cuando son ingresadas y/o actualizadas.

Artículo 21. Almacenar las contraseñas utilizando un algoritmo de cifrado.

Artículo 22. Las contraseñas utilizadas por los usuarios deben ser difíciles de deducir, por lo tanto la contraseña debe cumplir los siguientes requisitos:

- Usar una combinación alfanumérica.
- La contraseña debe tener una longitud mínima de 8 caracteres y máxima de 12 caracteres.
- La contraseña debe tener un periodo de vigencia, luego deberá ser cambiada por una nueva y diferente a la anterior.
- No deberá usar datos personales, acrónimos ni datos relacionados directamente con el usuario.
- Usar contraseñas no pronunciables y sin significado obvio.

Artículo 23. El área de TICS se reserva el derecho de monitorear cuentas de usuarios con actividad sospechosa en los activos y de información del Instituto Tecnológico Superior Central Técnico.

Artículo 24. El área de TICS, no proporcionará ningún tipo de acceso adicional a las aplicaciones académicas a los usuarios de cualquier área o carrera, sin haber cumplido con los requisitos para su respectiva autorización.

Artículo 25. Se considerará como ataque a la seguridad de la información y una falta grave, cualquier procedimiento no autorizada, en la que los usuarios realicen exploración de los recursos informáticos en la red del Instituto Tecnológico Superior Central Técnico (ITSCT), así como de las aplicaciones (GIA, AULA VIRTUAL) que sobre dicha red operan, con fines a detectar y explotar una posible vulnerabilidad.

4.6.4.2. Gestión de acceso de usuarios

Gestión de altas/bajas en el registro de usuarios

Artículo 26. El área de Recursos Humanos del Instituto Tecnológico Superior Central Técnico (ITSCT), deberá notificar al área de TICS la nómina de personal nuevo para la asignación de los accesos correspondientes en las aplicaciones académicas que maneja la institución.

Artículo 27. Los accesos lógicos a los activos de información de los usuarios que se desvincularon de la institución deben ser removidos por el coordinador del área de TICS de manera inmediata a. Las cuentas de acceso deben colocarse en estado **Inactivo**.

Gestión de los derechos a acceso con privilegios especiales

Artículo 28. Asignar privilegios de acceso a los sistemas académicos a docentes o administrativos, previa autorización por escrito o correo electrónico por parte de la máxima autoridad del Instituto.

Retirada o adaptación de los derechos de acceso

Artículo 29. El área de TICS debe ajustar inmediatamente los privilegios de acceso de los usuarios que cambiaron sus tareas, o de aquellos a los que se les revocó la autorización por la máxima autoridad del Instituto.

4.6.4.3. Responsabilidades del usuario

Uso de información confidencial para la autenticación

Artículo 30. El usuario deberá velar por la protección de acceso a su equipo de cómputo, mediante protector de pantalla con contraseña cuando requiera ausentarse.

Artículo 31. Ningún usuario deberá acceder a las aplicaciones académicas, utilizando una cuenta de usuario de otro usuario.

Artículo 32. Es responsabilidad de los usuarios el uso que haga de la cuenta de acceso y contraseña proporcionada a los sistemas académicos y equipos de cómputo.

Artículo 33. Los usuarios son responsables de todas las actividades llevadas a cabo con su cuenta de acceso y contraseña.

Artículo 34. Las contraseñas no deberán ser almacenadas en ningún formato legible en archivos desprotegidos, almacenados en lugares o carpetas donde las personas no autorizadas puedan encontrarlas. Las contraseñas en ningún momento deberán estar escritas y a la vista, como en monitores de computadoras y/o escritorios.

Artículo 35. Los usuarios deben reportar de manera obligatoria al área de TICS cualquier daño, falla, riesgo o amenaza detectada en las aplicaciones académicas, base de datos o red.

Artículo 36. El área de TICS del Instituto Tecnológico Superior Central Técnico (ITSCT) no se responsabiliza por el mal uso y manejo que se dé al correo electrónico institucional.

Artículo 37. Cuando un usuario, al que le haya sido autorizado el uso de una cuenta de correo electrónico, se desvincule del instituto su cuenta de correo será desactivada.

Artículo 38. Las cuentas de correos que permanezcan con estado **desactivado** se conservarán por el término de un (1) año, después de ese lapso de tiempo se realizará el proceso de eliminación.

4.6.4.4. Control de acceso a sistemas y aplicaciones

Procedimientos seguros de inicio de sesión.

Artículo 39. Todos los equipos de cómputo, sistemas académicos, bases de datos, etc., deben contar con mecanismos de identificación, autenticación y roles de privilegios de usuario apropiados según la clase de información y el tratamiento que se autorice a la misma.

Artículo 40. Las contraseñas predefinidas de servidores, bases de datos, aplicaciones, Routers, Switchs, deben cambiarse antes de colocarlas en producción.

Artículo 41. El área de TICS asignará cuentas de usuario y contraseña a los usuarios, estos la utilizarán solo en el primer inicio de sesión obligándolo a realizar el cambio para acceder al servicio.

Artículo 42. Los usuarios de los sistemas académicos podrán cambiar su contraseña en el momento que lo consideren necesario o cuando alguna regla de seguridad exija dicho cambio.

Artículo 43. No mostrar la contraseña que se introduce en los sistemas académicos.

Artículo 43. El personal del área de TICS debe emplear obligatoriamente contraseñas con un alto nivel de complejidad.

4.6.5. Seguridad física y ambiental

Objetivo

Proteger los activos de información, fortaleciendo la confidencialidad, disponibilidad e integridad mediante la seguridad física y ambiental.

4.6.5.1. Áreas seguras

Controles físicos de entrada

Artículo 44. Todos los lugares donde se encuentren sistemas de procesamiento informático o de almacenamiento, así como el acceso a oficinas, deben ser protegidos contra accesos no autorizados, utilizando procedimientos o tecnologías de autenticación, monitoreo y registro.

Artículo 45. Los usuarios que ingresen a los lugares donde se encuentra los sistemas de procesamiento de información deben portar de manera obligatoria una credencial de manera visible.

Artículo 46. Los controles de acceso a las áreas de procesamiento de la información o almacenamiento deben ser revisados, actualizados o revocados, según sea el caso.

Protección contra las amenazas externas y ambientales

Artículo 47. Se prohíbe el consumo de líquidos y alimentos dentro de los laboratorios de cómputo o ambientes donde reposen los equipos de procesamiento de información.

Artículo 48. La limpieza y aseo de los ambientes donde se encuentran los equipos de procesamiento de información, debe efectuarse con la presencia de un usuario autorizado. El personal de limpieza debe ser capacitado con respecto a las precauciones mínimas a seguir durante el proceso de limpieza.

Artículo 49. Debe prohibirse el ingreso del personal de limpieza con maletas o elementos que no sirvan para su labor de limpieza y aseo de ambientes.

Artículo 50. El piso de los ambientes que son asignados para los equipos de procesamiento de información, debe ser de material no combustible.

Artículo 51. Se debe contar extintores de incendios en los ambientes en donde reposen equipos de procesamiento de información, con la capacidad de detener el fuego generado por equipos eléctricos o papel.

Artículo 52. Los suministros como papelería deben almacenarse a una distancia considerable de los equipos de procesamiento y almacenamiento de información para evitar daños de un desastre que afecte a los mismos.

4.6.5.2. Seguridad en los equipos

Instalaciones de suministro

Artículo 53. Los equipos de procesamiento de información deben contar con fuentes ininterrumpidas de energía eléctrica.

Seguridad del cableado

Artículo 54. Proteger el cableado que transporta datos de daños ambientales e interceptación cumpliendo con las normas.

Artículo 55. Los cables de red deben estar claramente codificados que permitan identificar fácilmente los elementos conectados y evitar conexiones erróneas.

Mantenimiento de los equipos

Artículo 56. Es responsabilidad del coordinador del área de TICS planificar el mantenimiento de equipos en horarios que no se obstaculice el normal funcionamiento de los equipos de administrativos, docentes y laboratorios de uso estudiantil.

Artículo 57. El mantenimiento, preventivo y/o correctivo de los equipos del personal administrativo, docente y laboratorios, es una actividad exclusiva del área de TICS.

Artículo 58. El área de TICS debe llevar registro del mantenimiento preventivo, correctivo y cambios realizados a los equipos de cómputo y de red.

Artículo 59. Cuando se va a realizar mantenimiento en alguno de los equipos del personal administrativo, docente y/o laboratorios, se debe comunicar con anticipación al (los) usuarios.

Políticas de puesto de trabajo y bloqueo de pantalla

Artículo 60. Cuando el usuario requiera ausentarse debe bloquear el acceso a su equipo de cómputo, utilizando protector de pantalla con contraseña o apagar el mismo.

Artículo 61. Se prohíbe a los usuarios, mover, reinstalar, reubicar los equipos, retirar los sellos de los mismos sin autorización del coordinador del área de TICS.

Artículo 62. Los cambios de reubicación de equipos de cómputo, debe ser notificado al coordinador del área de TICS con 3 días de anticipación.

Artículo 63. Al terminar la jornada laboral, los usuarios deberán dejar apagados los equipos de cómputo para evitar el acceso no autorizado a terceros.

Artículo 64. El coordinador del área de TICS asignará un responsable para el registro de uso de laboratorios informáticos.

Artículo 65. Los equipos de procesamiento de información del área de TICS del Instituto Tecnológico Superior Central Técnico, no podrán abandonar las instalaciones a menos que

estén acompañados por la autorización de la máxima autoridad y la validación del coordinador del área de TICS.

4.6.6. Seguridad en la operativa

Objetivo:

Definir las reglas para asegurar las operaciones correctas y seguras del área de TICS.

4.6.6.1. Responsabilidades y procedimientos de operación

Documentación de procedimientos de operación

Artículo 66. El área de TICS elaborará los manuales de usuario de las aplicaciones informáticas que desarrolla el área de TICS, para el correcto uso y manejo de las mismas.

Artículo 67. El área de TICS elaborará el manual del programador de la aplicación informática desarrollada en el área.

Artículo 68. El área de TICS debe mantener actualizada la documentación de los respectivos procedimientos de las aplicaciones informática que se desarrollan en el área de TICS.

Separación de entornos de desarrollo, prueba y producción

Artículo 69. Se debe separar los ambientes de desarrollo, pruebas y producción para reducir los riesgos de acceso no autorizado a los sistemas en producción.

4.6.6.2. Protección contra código malicioso

Controles contra código malicioso

Artículo 70. Todos los equipos del área de TICS deben tener instalado un antivirus actualizado.

Artículo 71. Es responsabilidad de cada usuario revisar que todos los medios extraíbles sean analizados por un antivirus, antes de procesarlos en los computadores personales.

4.6.6.3. Copias de seguridad

Copias de la seguridad de la información.

Artículo 72. Las copias de seguridad de la información de los sistemas académicos que maneja el Instituto Tecnológico Superior Central Técnico deben contar con un control de acceso restringido al personal autorizado.

Artículo 73. El coordinador del área de TICS, definirá el tiempo de periodicidad de generación de copias de seguridad de la información.

Artículo 74. Solamente el coordinador del área de TICS puede eliminar las copias de seguridad de la información con la autorización por escrito de la máxima autoridad del Instituto Tecnológico Superior Central Técnico siempre y cuando éste considere la caducidad de la misma.

Artículo 75. Las copias de seguridad de la información deben ser almacenadas en distintos soportes que no se encuentren en mal estado como disco externo y la nube.

Artículo 76. Los soportes de almacenamiento de copias de seguridad de la información que se encuentren en mal estado deben ser eliminados o dados de baja de forma segura mediante procedimientos formales mediante técnicas que imposibilite la recuperación de la información original, para asegurar que la información contenida en los mismos no se accesible.

Artículo 77. La eliminación de soportes de información sensible deberá quedar registrada a fin de mantener trazabilidad para su auditoría.

4.6.7. Seguridad en las telecomunicaciones

Objetivo.

"Asegurar la protección de la información en redes y sus instalaciones de soporte en el procesamiento de información" (Inen, 2017, p.57).

4.6.7.1. Gestión de la seguridad en las redes

Controles de red

Artículo 78. Únicamente el área de TICS administrará la red del Instituto Tecnológico Superior Central Técnico y otorgará los accesos a los usuarios solicitantes siempre y cuando sea para realizar tareas y actividades institucionales.

Artículo 79. Los usuarios autorizados a acceder a la red del Instituto Tecnológico Superior Central Técnico (ITSCT), deberán acercarse al área de TICS a proporcionar la dirección MAC de su computador, previa autorización de la máxima autoridad de la institución.

Artículo 80. Se considerará como uso aceptable de la red del Instituto Tecnológico Superior Central Técnico (ITSCT), la navegación para realizar actividades relacionadas con las funciones institucionales.

Artículo 81. El área de TICS es responsable de la implementación de herramientas informáticas para la administración del servicio de red para minimizar los riesgos que se puedan presentar.

Artículo 82. La revocación del servicio de red del Instituto Tecnológico Superior Central Técnico se lo realizará cuando se detecte la navegación a sitios o páginas Web con contenidos pornográficos, comunidades de hackers, vulnerar o intentar vulnerar la seguridad de los sistemas académicos de la institución, violar los derechos de privacidad confidencialidad y protección de datos, utilizar el servicio para fines personales, etc.

4.6.8. Adquisición, desarrollo y mantenimiento de los sistemas de información

Objetivo:

Asegurar que la seguridad de la información sea parte integral de los sistemas de información a través de todo el ciclo de vida. Esto también incluye los requisitos para los nuevos sistemas de información o mejora a os sistemas de información existentes. (Inen, 2017, p.63)

4.6.8.1. Seguridad en los procesos de desarrollo y soporte

Política de desarrollo seguro de software

Artículo 83. El área de TICS será la única dependencia autorizada para realizar copia de seguridad del software original.

Artículo 84. Se debe manejar un ambiente de desarrollo con control de versiones para las actualizaciones de software.

Procedimientos de control de cambios en los sistemas

Artículo 85. Los cambios que se realizan en las aplicaciones informáticas desarrolladas por el área de TICS deben documentarse y controlarse mediante procedimientos formales de control de cambios.

Artículo 85. Los cambios que requiera efectuarse en los sistemas desarrollados por el área de TICS, debe ser evaluados, para analizar el impacto que pueda incidir en el funcionamiento o seguridad de los mismos.

Artículo 86. Se debe llevar un de registro de auditoría de todas las solicitudes de cambio.

Seguridad en entornos de desarrollo

Artículo 86. Los accesos al ambiente de desarrollo deben ser restringidos por segregación de funciones y permisos de administrador.

Pruebas de funcionalidad durante el desarrollo de los sistemas

Artículo 87. Realizar pruebas de funcionalidad del sistema, con la finalidad de detectar.

Artículo 88. Asegurar que los cambios en los sistemas operativos están previstos en un plazo que permita realizar pruebas y revisiones apropiadas antes de la implementación

Pruebas de aceptación

Artículo 89. Antes que un nuevo sistema de información se desarrolle en el área de TICS del Instituto Tecnológico Superior Central Técnico (ITSCT), se deberá definir las especificaciones y requerimientos de seguridad necesarios para su implementación.

Artículo 90. La seguridad en el acceso a las aplicaciones académicas debe ser implementada por los desarrolladores del sistema desde el inicio del ciclo de vida del sistema hasta la conversión a un sistema en producción.

Artículo 91. Identificar y definir los requisitos y controles necesarios de seguridad, desde el análisis hasta el diseño del sistema.

Artículo 92. Todos las aplicaciones académicas que operan y administran información sensible, valiosa y crítica para el Instituto Tecnológico Superior Central Técnico (ITSCT), deberán generar registros de auditoría o logs de registro de sucesos de la operación, las cuales

deben proporcionar información necesaria para apoyar el monitoreo, control y las mismas auditorias.

Artículo 93. Identificar todos los elementos que obligatoriamente requieren de modificaciones y/o actualizaciones, obtener la aprobación por parte del coordinador del área de TICS para cumplir con los requerimientos del software.

4.6.9. Gestión de incidentes en la seguridad de la información

Objetivo:

Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, para obtener una respuesta rápida, efectiva y adecuada ante los incidentes de seguridad de información (Inen, 2017).

4.6.9.1. Gestión de incidentes en la seguridad de la información y mejoras

Notificación de puntos débiles de la seguridad

Artículo 94. Todos los usuarios que utilizan los sistemas académicos de información del Instituto Tecnológico Superior Central Técnico (ITSCT), tienen la obligación de notificar oficialmente al área de TICS cualquier debilidad de seguridad de la información que observen o sospechen que exista en los sistemas académicos. Bajo ninguna circunstancia los usuarios deben probar las sospechas de vulnerabilidad o fallas de los sistemas.

Respuesta a los incidentes de seguridad

Artículo 95. El área de TICS debe documentar y comunicar los reportes de incidentes de seguridad de información, para que estos sean atendidos oportunamente con el fin de tomar acciones correctivas.

Artículo 96. Se debe llevar un registro detallado de los incidentes de Seguridad de la Información y la respuesta que fue implementada en cada uno de ellos, contemplando los daños que se causaron por el mismo y, de ser posible, la valoración de los daños.

CAPÍTULO V

Conclusiones y trabajos futuros

5.1. Conclusiones

- Se diseñó una política de seguridad para el área de TICS, en base a la criticidad de los activos de información para salvaguardar su confidencialidad, integridad y disponibilidad acorde a los controles de la norma ISO/IEC 27002:2013, ya que esta norma puede ser aplicada a cualquier tipo de organización.
- Mediante el análisis (Tabla 20. Matriz de riesgos) realizado al área de TICS, se pudo evidenciar que existen amenazas y vulnerabilidades a las que están expuestos los activos de información, como también se constató que el área de TICS no cuenta con una metodología para el tratamiento de riesgos y con medidas de seguridad de la información que permitan el buen uso y manejo de la misma.
- En base al resultado del análisis realizado a los procesos que lleva el área de TICS y mediante la utilización de la Metodología MAGERIT, se determinó las amenazas y vulnerabilidades que afectan la gestión de la información en el área de TICS, constatando que el mayor impacto en caso que se materialicen las amenazas se encuentra en los siguientes activos: De desarrollo propio: GIA, GIA_IDIOMAS, Computadoras de escritorio, Oficina de TICS y Base de datos: GIA, GIA_IDIOMAS, AULA VIRTUAL (MOODLE).
- Considerando todas las amenazas y vulnerabilidades a las que están expuestos los activos de información identificadas en la etapa de gestión de riesgos, se realizó la

selección de medidas de control utilizando la Norma ISO/IEC 27002:2013, ya que esta Norma se adapta a las necesidades de seguridad de la información del área de TICS.

- Mediante los resultados obtenidos en el análisis de riesgos y la elaboración de la política de seguridad para el área de TICS, se concluye que no es necesario considerar todos los controles recomendados por la norma ISO/IEC 27002, sino que se debe priorizar y seleccionar los controles que se alinean con el riesgo, teniendo en cuenta la capacidad presupuestaria del Instituto y sus necesidades de negocio.
- Después de haber finalizado este proyecto de tesis, el área de TICS del ITSC obtuvo un manual de controles para la seguridad de la información, los cuales permitirían mitigar los riesgos identificados en el área de TICS.

5.2. Recomendaciones

- Se recomienda que la política de seguridad de la información sea aprobada por las autoridades del Instituto Tecnológico Superior Central Técnico (ITSCT) y sea revisada con regularidad por el encargado del área de TICS o en caso que ocurran cambios significativos para garantizar el manejo correcto de los activos de información de la Institución.
- Se recomienda que la política de seguridad de la información sea socializada a todo el personal docente y administrativo de la Institución para que contribuyan con la seguridad de la misma y conozcan las posibles amenazas a las cuales están expuestos.
- Se recomienda implementar la política de seguridad en el área de TICS para el buen uso y manejo de los recursos informáticos y así garantizar la confidencialidad, integridad y disponibilidad de la información.
- Se recomienda implementar la política de seguridad en el área de TICS, ya que esta serviría como guía para tomar acciones preventivas y correctivas para minimizar los

riesgos que se puedan presentar, como también para evitar daños y pérdidas significativas en los activos de información institucionales.

Bibliografía

Aceves, I. (n.d.). Principios de Seguridad de la Información. *Roa.uveg.edu.mx*. Retrieved from http://roa.uveg.edu.mx/repositorio/licenciatura2015/237/PrincipiosdeSeguridaddelaInformacin.pdf

Ana, A., Jarol, P., & Bohada, J. A. (2013). Risk Analysis in Security of Information. *Risk Analysis in Security of Information*, 39–53.

Andrés, A., & Gómez, L. (2009). *Guía de aplicación de la Norma UNE-ISO / IEC 27001 sobre seguridad en sistemas de información para pymes*. Retrieved from www.aenor.es

Burgos, J., & Campos, P. (2008). Modelo Para Seguridad de la Información en TIC. *Ceur-Ws.Org*, 20. Retrieved from http://ceur-ws.org/Vol-488/paper13.pdf

Cano, J. J., María, G., & Meza, S. (2017). *IX INFORME DE ENCUESTA LATINOAMERICANA DE SEGURIDAD DE LA INFORMACIÓN*. Retrieved from http://acis.org.co/archivos/JornadaSeguridad/2017/Memorias/18.pdf

Consejo Superior de Administración Electrónica. (2012a). *MAGERIT - versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. *Libro I - Método*. Retrieved from http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Consejo Superior de Administración Electrónica. (2012b). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III - Guía de Técnicas*. Retrieved from http://administracionelectronica.gob.es/ctt/resources/Soluciones/184/Area

descargas/Libro-III-Guia-de-Tecnicas.pdf?idIniciativa=184&idElemento=87&idioma=en

Consejo Superior de Administración Electrónica, & Amutio Gómez, M. A. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos*. Retrieved from administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Documentacion/Metodologias-y-guias/Mageritv3/2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8/2012_Magerit_v3_libro2_catalogo de elementos_es_NIPO_630-12-171-8.pdf

Dussan Clavijo, C. A. (2006). *Políticas de seguridad informática*. *Entramado* (Vol. 2). Retrieved from http://www.redalyc.org/html/2654/265420388008/

electrónica, J. P.-V., & 2017, U. (2017). Exposición del activo más valioso de la organización, la "información." *Dialnet.unirioja.es*, *11*(1). https://doi.org/10.14483/22484728.12345

Escrivá Gascó, Gema, Romero Serrano, Rosa María, Ramada, D. J. (2013). Seguridad informática, 10. Retrieved from http://site.ebrary.com/lib/bibliouniminutosp/reader.action?docID=10820963&ppg=8

Forum, I., Council, E.-, Security, D. E. S., & Management, S. (2013). Conceptos de seguridad informática y su reflejo en la Cámara de Cuentas de Andalucía. *Conceptos de Seguridad Informática Y Su Reflejo En La Cámara de Cuentas de Andalucía*, *61*(1 al 17), 111–117.

Gaona Vásquez, K. del R. (2013). *Aplicación de la metodología MAGERIT para el análisis y gestión de riesgos de la seguridad de la información aplicado a la empresa pesquera e industrial Bravito s.a. en la ciudad de Machala*. Retrieved from https://dspace.ups.edu.ec/bitstream/123456789/5272/1/UPS-CT002759.pdf

Gomez Vieites, A. (2014). Enciclopedia de la Seguridad Informática. 2ª edición - Álvaro

Gómez Vieites - Google Libros. Retrieved September 12, 2018, from https://books.google.es/books?hl=es&lr=&id=Bq8-DwAAQBAJ&oi=fnd&pg=PT2&dq=Enciclopedia+de+la+seguridad+informática+(Vol.+6)&ots=dwn84hZjgL&sig=ekOCaw9EEph-eUduq_GpRV_g6Lg#v=onepage&q&f=false

Grupa, P. (2015). ISO27000.es - El portal de ISO 27001 en español. Gestión de Seguridad de la Información. Retrieved September 12, 2018, from http://www.iso27000.es/iso27000.html

Guato, G., Fernando, H., Muenala, Q., & Geovanna, M. (2016). *Aplicación de las normas técnicas iso/iec 27001 e iso/iec 27002 para el cumplimiento del esquema gubernamental de seguridad de la información (egsi) en la*. Retrieved from http://bibdigital.epn.edu.ec/handle/15000/15191

Horváth, M., & Jakub, M. (2009). Implementation of security controls according to ISO / IEC 27002 in a small organisation. *Security*, 48–54. Retrieved from http://www.qip-journal.eu/files/2009/2009-2/QIP_2_2009_Horvath.pdf

Inen, P. O. R. (2017). TECNOLOGÍAS DE LA INFORMACIÓN ─ TÉCNICAS DE SEGURIDAD ─ CÓDIGO DE PRÁCTICA PARA LOS CONTROLES DE SEGURIDAD DE LA INFORMACIÓN (ISO/IEC 27002:2013+Cor. 1:2014+Cor. 2: 2015, IDT), 1–5.

ISO/IEC 27002:2013. (2013). Controles ISO 27002, 27002. Retrieved from http://iso27000.es/download/ControlesISO27002-2013.pdf

ISOTools Excellence. (n.d.). Norma ISO 27002: El dominio política de seguridad. Retrieved February 16, 2019, from https://www.pmg-ssi.com/2017/08/norma-iso-27002-politica-seguridad/

ITSCT. (n.d.-a). No Title. Retrieved from https://itsct.edu.ec/portal/historia/

ITSCT. (n.d.-b). No Title. Retrieved from https://itsct.edu.ec/portal/mision/

Ledezma, D. (2015). *Desarrollo de políticas de seguridad de la información basadas en las Normas ISO 27002 para una Coordinación Zonal del INEC*. Retrieved from http://repositorio.pucesa.edu.ec/handle/123456789/1555

Mendez-Vilas, A., Gonzalez, J., González, J., & Bote, V. (2003). Techno-Legal Aspects of Information Society and New Economy: an Overview. Retrieved from http://mario.elinos.org.mx/publication/papers/2003/002.pdf

Ochoa Arévalo, P. A. (2015). Gobierno de Seguridad de la Información, un enfoque hacia el cumplimiento regulatorio. *Revista Tecnológica ESPOL-RTE*, *28*(3), 1–17. Retrieved from http://www.rte.espol.edu.ec/index.php/tecnologica/article/viewFile/373/258

Orrego, V. M. (2013). La gestión en la seguridad de la información según Cobit, Itil e Iso 27000. *Revista Pensamiento Americano*, *4*(6), 21–23. https://doi.org/10.21803/penamer.4.6.57

Posso, R. (2009). Desarrollo De Políticas De Seguridad Informática E Implementación De Tres Dominios En Base a La Norma 27002 Para El Área De Hardware En La Empresa Uniplex Systems S.a. En Quito. *Researchgate.net*, 277. Retrieved from https://www.researchgate.net/profile/Jose_Patino_Sanchez/publication/28796014_Desarrollo_De_Politicas_De_Seguridad_Informatica_E_Implementacion_De_Cuatro_Dominios_En_Base_A_La_Norma_27002_Para_El_Area_De_Hardware_En_La_Empresa_Uniplex_Systems_SA_En_Guayaq

Secretaria Nacional de Administración Pública. Acuerdo Ministerial 166 - Esquema gubernamental de seguridad de la información EGSI, Registro Oficial Nro. 88 § (2013). Retrieved from www.lexis.com.ec

Solarte, F. N. S., Rosero, E. R. E., & Benavides, M. del C. (2015, December 31). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y

de información bajo la norma ISO/IEC 27001. *Revista Tecnológica - ESPOL*. Escuela Superior Politécnica del Litoral (ESPOL). Retrieved from http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456/321

Velasco, A. (2008). EL DERECHO INFORMÁTICO Y LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN UNA PERSPECTIVA CON BASE EN LA NORMA ISO 27 001. (Spanish). *Revista de Derecho*, (29), 333–366. Retrieved from http://www.scielo.org.co/scielo.php?pid=S0121-86972008000100013&script=sci_arttext&tlng=pt

ANEXO 1: Autorización para el desarrollo del proyecto de tesis

Quito, 11 de septiembre de 2018

Ing. José Luis Flores

RECTOR DEL INSTITUTO TECNOLÓGICO SUPERIOR CENTRAL TÉCNICO (ITSCT)

Presente.

Yo, Hilda Yecenia Cevallos Jarro, docente del instituto Tecnológico Superior Central Técnico, con un atento saludo ante usted me dirijo respetuosamente para solicitarle de la manera más cordial, me autorice diseñar una política de seguridad de la información para el área de TICS del ITSCT, lo cual me servirá como proyecto de titulación de la Maestría en Tecnologías de la Información de la Universidad Internacional SEK.

Agradezco su favorable atención a la presente.

Atentamente

Ing. Yecenia Cevallos

1104224108

ANEXO 2: NORMA ISO/IEC 27002:2013

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.
- 5.1 Directrices de la Dirección en seguridad de la información.
  - 5.1.1 Conjunto de políticas para la seguridad de la información.
  - 5.1.2 Revisión de las políticas para la seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
- 6.1 Organización interna.
  - 6.1.1 Asignación de responsabilidades para la segur. de la información.
  - 6.1.2 Segregación de tareas.
  - 6.1.3 Contacto con las autoridades.
  - 6.1.4 Contacto con grupos de interés especial.
  - 6.1.5 Seguridad de la información en la gestión de proyectos.
- 6.2 Dispositivos para movilidad y teletrabajo.
  - 6.2.1 Política de uso de dispositivos para movilidad.
  - 6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
- 7.1 Antes de la contratación.
  - 7.1.1 Investigación de antecedentes.
  - 7.1.2 Términos y condiciones de contratación.
- 7.2 Durante la contratación.
  - 7.2.1 Responsabilidades de gestión.
  - 7.2.2 Concienciación, educación y capacitación en segur. de la informac.
  - 7.2.3 Proceso disciplinario.
- 7.3 Cese o cambio de puesto de trabajo.
  - 7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.
- 8.1 Responsabilidad sobre los activos.
  - 8.1.1 Inventario de activos.
  - 8.1.2 Propiedad de los activos.
  - 8.1.3 Uso aceptable de los activos.
  - 8.1.4 Devolución de activos.
- 8.2 Clasificación de la información.
  - 8.2.1 Directrices de clasificación.
  - 8.2.2 Etiquetado y manipulado de la información.
  - 8.2.3 Manipulación de activos.
- 8.3 Manejo de los soportes de almacenamiento.
  - 8.3.1 Gestión de soportes extraíbles.
  - 8.3.2 Eliminación de soportes.
  - 8.3.3 Soportes físicos en tránsito.

9. CONTROL DE ACCESOS.
- 9.1 Requisitos de negocio para el control de accesos.
  - 9.1.1 Política de control de accesos.
  - 9.1.2 Control de acceso a las redes y servicios asociados.
- 9.2 Gestión de acceso de usuario.
  - 9.2.1 Gestión de altas/bajas en el registro de usuarios.
  - 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
  - 9.2.3 Gestión de los derechos de acceso con privilegios especiales.
  - 9.2.4 Gestión de información confidencial de autenticación de usuarios.
  - 9.2.5 Revisión de los derechos de acceso de los usuarios.
  - 9.2.6 Retirada o adaptación de los derechos de acceso
- 9.3 Responsabilidades del usuario.
  - 9.3.1 Uso de información confidencial para la autenticación.
- 9.4 Control de acceso a sistemas y aplicaciones.
  - 9.4.1 Restricción del acceso a la información.
  - 9.4.2 Procedimientos seguros de inicio de sesión.
  - 9.4.3 Gestión de contraseñas de usuario.
  - 9.4.4 Uso de herramientas de administración de sistemas.
  - 9.4.5 Control de acceso al código fuente de los programas.

10. CIFRADO.
- 10.1 Controles criptográficos.
  - 10.1.1 Política de uso de los controles criptográficos.
  - 10.1.2 Gestión de claves.

11. SEGURIDAD FÍSICA Y AMBIENTAL.
- 11.1 Áreas seguras.
  - 11.1.1 Perímetro de seguridad física.
  - 11.1.2 Controles físicos de entrada.
  - 11.1.3 Seguridad de oficinas, despachos y recursos.
  - 11.1.4 Protección contra las amenazas externas y ambientales.
  - 11.1.5 El trabajo en áreas seguras.
  - 11.1.6 Áreas de acceso público, carga y descarga.
- 11.2 Seguridad de los equipos.
  - 11.2.1 Emplazamiento y protección de equipos.
  - 11.2.2 Instalaciones de suministro.
  - 11.2.3 Seguridad del cableado.
  - 11.2.4 Mantenimiento de los equipos.
  - 11.2.5 Salida de activos fuera de las dependencias de la empresa.
  - 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
  - 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
  - 11.2.8 Equipo informático de usuario desatendido.
  - 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.
- 12.1 Responsabilidades y procedimientos de operación.
  - 12.1.1 Documentación de procedimientos de operación.
  - 12.1.2 Gestión de cambios.
  - 12.1.3 Gestión de capacidades.
  - 12.1.4 Separación de entornos de desarrollo, prueba y producción.
- 12.2 Protección contra código malicioso.
  - 12.2.1 Controles contra el código malicioso.
- 12.3 Copias de seguridad.
  - 12.3.1 Copias de seguridad de la información.
- 12.4 Registro de actividad y supervisión.
  - 12.4.1 Registro y gestión de eventos de actividad.
  - 12.4.2 Protección de los registros de información.
  - 12.4.3 Registros de actividad del administrador y operador del sistema.
  - 12.4.4 Sincronización de relojes.
- 12.5 Control del software en explotación.
  - 12.5.1 Instalación del software en sistemas en producción.
- 12.6 Gestión de la vulnerabilidad técnica.
  - 12.6.1 Gestión de las vulnerabilidades técnicas.
  - 12.6.2 Restricciones en la instalación de software.
- 12.7 Consideraciones de las auditorías de los sistemas de información.
  - 12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.
- 13.1 Gestión de la seguridad en las redes.
  - 13.1.1 Controles de red.
  - 13.1.2 Mecanismos de seguridad asociados a servicios en red.
  - 13.1.3 Segregación de redes.
- 13.2 Intercambio de información con partes externas.
  - 13.2.1 Políticas y procedimientos de intercambio de información.
  - 13.2.2 Acuerdos de intercambio.
  - 13.2.3 Mensajería electrónica.
  - 13.2.4 Acuerdos de confidencialidad y secreto.

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
- 14.1 Requisitos de seguridad de los sistemas de información.
  - 14.1.1 Análisis y especificación de los requisitos de seguridad.
  - 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
  - 14.1.3 Protección de las transacciones por redes telemáticas.
- 14.2 Seguridad en los procesos de desarrollo y soporte.
  - 14.2.1 Política de desarrollo seguro de software.
  - 14.2.2 Procedimientos de control de cambios en los sistemas.
  - 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
  - 14.2.4 Restricciones a los cambios en los paquetes de software.
  - 14.2.5 Uso de principios de ingeniería en protección de sistemas.
  - 14.2.6 Seguridad en entornos de desarrollo.
  - 14.2.7 Externalización del desarrollo de software.
  - 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
  - 14.2.9 Pruebas de aceptación.
- 14.3 Datos de prueba.
  - 14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.
- 15.1 Seguridad de la información en las relaciones con suministradores.
  - 15.1.1 Política de seguridad de la información para suministradores.
  - 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
  - 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
- 15.2 Gestión de la prestación del servicio por suministradores.
  - 15.2.1 Supervisión y revisión de los servicios prestados por terceros.
  - 15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
- 16.1 Gestión de incidentes de seguridad de la información y mejoras.
  - 16.1.1 Responsabilidades y procedimientos.
  - 16.1.2 Notificación de los eventos de seguridad de la información.
  - 16.1.3 Notificación de puntos débiles de la seguridad.
  - 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
  - 16.1.5 Respuesta a los incidentes de seguridad.
  - 16.1.6 Aprendizaje de los incidentes de seguridad de la información.
  - 16.1.7 Recopilación de evidencias.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
- 17.1 Continuidad de la seguridad de la información.
  - 17.1.1 Planificación de la continuidad de la seguridad de la información.
  - 17.1.2 Implantación de la continuidad de la seguridad de la información.
  - 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
- 17.2 Redundancias.
  - 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.
- 18.1 Cumplimiento de los requisitos legales y contractuales.
  - 18.1.1 Identificación de la legislación aplicable.
  - 18.1.2 Derechos de propiedad intelectual (DPI).
  - 18.1.3 Protección de los registros de la organización.
  - 18.1.4 Protección de datos y privacidad de la información personal.
  - 18.1.5 Regulación de los controles criptográficos.
- 18.2 Revisiones de la seguridad de la información.
  - 18.2.1 Revisión independiente de la seguridad de la información.
  - 18.2.2 Cumplimiento de las políticas y normas de seguridad.
  - 18.2.3 Comprobación del cumplimiento.

ISO27002.es PATROCINADO POR:

GES CONSULTOR

ANEXO 3: ENTREVISTA

ENTREVISTA PARA EL COORDINADOR DEL ÁREA DE TICS DEL INSTITUTO TECNOLÓGICO SUPERIOR CENTRAL TÉCNICO, QUE PERMITIRÁ EXPLORAR ASPECTOS DE SEGURIDAD INFORMÁTICA.

La presente entrevista coadyuvará a la realización de una tesis de maestría en Tecnologías de la información; y tiene por objeto elaborar un estudio diagnóstico de los elementos de seguridad informática donde usted trabaja.

La información que usted proporcione tendrá un carácter confidencial y anónimo.

Agradezco de antemano su participación.

1. ¿El área de TICS del ITSCT, posee un manual de políticas de seguridad de la información?

   NO

2. ¿Se cumplen estas políticas de seguridad de la información?

   NO

3. ¿Cada que tiempo actualiza el Manual de seguridad de la información?

   NUNCA

4. ¿Existe un área o persona responsable de la seguridad informática y seguridad de la información en el ITSCT?

   NO

5. ¿Qué tipo de herramientas de seguridad tiene implementado en el ITSCT? (Hardware, Software, otros)

   LA QUE VIENE CON EL CPANEL.

6. ¿Cuáles son los beneficios que otorgan al tener políticas de seguridad de la información?

   - MANTENER LA INFORMACIÓN RESGUARDADA
   - " CONFIDENCIALIDAD
   - " INTEGRIDAD
   - " DISPONIBILIDAD.

7. De las siguientes medidas de seguridad, ¿Cuáles cree usted que son más importantes?
   - [✓] Desarrollo de políticas de seguridad dela información.
   - [✓] Capacitación a usuarios acerca la seguridad de la información
   - [✓] Monitoreo y reporte de actividades.
   - [ ] Otros, indique cuales: .....

8. ¿Existen procedimientos establecidos en el área de TICS con los respectivos responsables y estos procedimientos se encuentran documentados?

   SI, EN LA MAYORÍA DE CASOS.

9. ¿Con que frecuencia actualiza los procedimientos?

TRIMESTRAL

10.¿Tiene instalado un antivirus en los equipos de cómputo?

NO

11.¿Qué mecanismos de autenticación, utilizan en el ITSCT?

CLAVE DE ACCESO CON MDS

12.Pide a los docentes que cambien de contraseña con regularidad

NO

13.¿Realiza mantenimiento informático periódico sobre los ordenadores del área de TICS?

NO

14.¿El ITSCT tiene restricciones de seguridad para el acceso a la conexión WIFI? ¿Cuáles?

SÍ, FILTRADO POR MAC

15.¿Cómo se integran los smartphones de los docentes a la red del ITSCT?

NO SE INTEGRAN

16.¿Realiza una copia de seguridad de la información del ITSCT? ¿Con qué frecuencia lo realiza?

SEMANAL.

17.¿Se utiliza mecanismos de bloqueo automático de las estaciones de trabajo para cuando se encuentran detenidos?

NO

18.¿Existen equipos que provean de energía ininterrumpida a los servidores y computadores del personal docente y administrativo del ITSCT?

NO

19.¿Tuvieron algún incidente grave de seguridad de la información durante el último año? ¿Cuál?

BASE DE DATOS SIN RESTRICCIONES Y EXISTIAN MODIFICACIONES NO AUTORIZADAS

20.¿Mantiene un registro de fallas cuando ocurre algún evento en servidores, computadores, redes, etc.?

NO

ANEXO 4: ACUERDO DE CONFIDENCIALIDAD

ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE LA INFORMACIÓN PARA EL ÁREA DE TICS DEL INSTITUTO TECNOLÓGICO SUPERIOR CENTRAL TÉCNICO

Intervienen en la celebración del presente "*ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE LA INFORMACIÓN"*, por una parte, [nombres y apellidos] con cédula de ciudadanía Nro. xxxxxxxxxx, en mi calidad de **Coordinador(a)** del área de TICS del Instituto Tecnológico Superior Central Técnico (ITSCT) en adelante y para efectos del presente instrumento en calidad de **Proveedor de Información**; y por otro lado [nombres y apellidos] con cédula de ciudadanía Nro. xxxxxxxxxx en mí calidad de [cargo] del Instituto Tecnológico Superior Central Técnico, en adelante y para efectos del presente instrumento en calidad de **Receptor de la Información** quienes libre y voluntariamente celebran el presente acuerdo.

Ambas partes reconocen recíprocamente su capacidad para obligarse, por lo que suscriben el presente Acuerdo de Confidencialidad y de No Divulgación de Información con base a las siguientes cláusulas.

CLÁUSULA PRIMERA. - ANTECEDENTES:

El artículo 226 de la Constitución de la República del Ecuador prevé que: *"Las instituciones del Estado sus organismos y dependencias, y las servidoras o servidores públicos, tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la Constitución"*;

En virtud de lo establecido en el numeral 19 del artículo 66 de la Norma Suprema se dispone: *"Se reconoce y garantizará a las personas: (...) El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección,*

archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la Ley";

El artículo 178 del Código Orgánico Integral Penal establece: *"La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años…";*

El artículo 190 ibídem señala: "*La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años(…)*";

El artículo 230 del Código Orgánico Integral Penal determina: *"Será sancionada con pena privativa de libertad de tres a cinco años: (…) La persona que sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible. (…)";*

La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, en los artículos 2 y 44, respectivamente, reconoce ante el Estado la validez jurídica de los mensajes de datos electrónicos, así como el valor y efecto jurídicos de cualquier actividad, transacción mercantil, financiera o de servicios que se realice con los mismos por medio de redes electrónicas;

La Carta Iberoamericana de Gobierno Electrónico, en la sección 24, recomienda a los gobiernos tomar en consideración la importancia de la interoperabilidad de las comunicaciones y servicios, así como disponer las medidas necesarias, para que todas las entidades públicas, cualquiera que sea su nivel y con independencia del respeto a su autonomía, establezcan sistemas que sean interoperables;

La Ley del Sistema Nacional de Registro de Datos Públicos publicada en el Registro Oficial No. 162 de 31 de marzo de 2010, en su artículo 4, cita: *"Las instituciones del sector público y privado y las personas naturales que actualmente o en el futuro administren bases o registros de datos públicos, son responsables de la integridad, protección y control de los registros y bases de datos a su cargo. Dichas instituciones responderán por la veracidad, autenticidad, custodia y debida conservación de los registros. La responsabilidad sobre la veracidad y autenticidad de los datos registrados, es exclusiva de la o el declarante cuando esta o este provee toda la información…";*

El artículo 27 de la Ley ibídem establece: *"Las Registradoras o Registradores y máximas autoridades, a quienes se autoriza el manejo de las licencias para el acceso a los registros de datos utilizados por la ley, serán las o los responsables directos administrativa, civil y penalmente por el mal uso de las mismas";*

Bajo este marco regulatorio, la información que se dispone en los servicios institucionales se clasifica como reservada y/o confidencial, a tal efecto se acuerda suscribir el presente *"Acuerdo de Confidencialidad y No Divulgación de la Información"* entre la entidad que solicita el acceso a los servicios institucionales y la entidad proveedora del servicio con la finalidad de proteger la información que se consuma cuando ésta tenga el carácter de reservada y/o confidencial.

Se garantizará la confidencialidad, integridad, disponibilidad, reserva y protección de los datos e información que se comparta e intercambie entre las entidades, de acuerdo a la normativa vigente.

CLÁUSULA SEGUNDA. - OBJETO:

En virtud de los antecedentes expuestos, por medio del presente instrumento **el RECEPTOR DE LA INFORMACIÓN** se obliga expresamente a guardar sigilo, confidencialidad y reserva sobre el contenido de toda la información generada, verbal o escrita, que se comparta entre las partes.

Además, **el RECEPTOR DE LA INFORMACIÓN** se compromete a hacer uso de la información, únicamente para las actividades relacionadas con las funciones que desempeña, conforme a las obligaciones y prohibiciones legales pertinentes.

CLÁUSULA TERCERA. - DERECHOS Y OBLIGACIONES:

Son obligaciones del área de TICS las siguientes:

1. Suministrará al **RECEPTOR DE LA INFORMACIÓN** el informe/la información que estime necesaria para la ejecución de las actividades asignadas.

Son deberes de quien haga las veces de **RECEPTOR DE LA INFORMACIÓN**:

1. Guardar la reserva y confidencialidad, sin el deterioro de cualquier tipo de información que se le suministre o a la cual llegare a tener acceso o conocimiento;
2. Todo funcionario público de cualquier entidad pública y/o empleado de empresa privada que haga uso y tenga acceso a la información proporcionada por el área de TICS del ITSCT, deberá suscribir el presente instrumento.
3. Mantener en forma estrictamente reservada y confidencial toda la información que por razón de su competencia tendrá acceso, por lo tanto, se obliga a abstenerse de usar, disponer, divulgar y/o publicar por cualquier medio, oral, escrito, y/o tecnológico y en general, aprovecharse de ella en cualquier otra forma para efectos ajenos a los intereses de la Institución a la cual pertenece.
4. Utilizar la información suministrada por el área de TICS, únicamente para los fines acordados por las partes.

No realizar copia o duplicado alguno de la información mencionada en este acuerdo sin la autorización previa y escrita de la otra parte; tampoco podrán divulgar dicha información a terceras personas sin que medie igualmente la respectiva autorización previa y escrita de la otra parte. Se excluye de esta obligación la información que sea de dominio público o que sea del conocimiento previo del área de TICS, sin constituir discreción de la información en los términos del presente acuerdo y, cuya revelación no cause agravio o perjuicio alguno a su titular.

CLÁUSULA CUARTA. - PATRÓN DE CONDUCTA, IMPLICACIONES DE LA RECEPCIÓN DE LA INFORMACIÓN Y RESPONSABILIDAD

Las partes actuarán con responsabilidad en el buen uso de la información, lo que supone entre otros deberes, el de limitar la divulgación autorizada al menor número de personas, y el de tomar las medidas idóneas y eficaces para evitar el tráfico y fuga indebida de la información, así como su uso por fuera de los límites de este convenio.

El incumplimiento del deber de reserva establecido en la Cláusula Cuarta de este acuerdo, constituye violación de secreto y justa causa de terminación unilateral de la relación, sin desmedro de las indemnizaciones (sólo para proveedores) legales correspondientes.

El **RECEPTOR DE LA INFORMACIÓN** reconoce que la información confidencial a la que se refiere el presente acuerdo posee una valoración en imagen institucional y su indebida divulgación o utilización causa un perjuicio.

CLÁUSULA QUINTA. - MATERIALES:

Todos los materiales como documentos, actas de reunión, respaldo de bases de datos, código fuente de los sistemas académicos, entre otras que son entregadas al **RECEPTOR DE LA INFORMACIÓN** por parte del área de TICS se considera como información confidencial y se debe guardar absoluta reserva de la misma.

CLÁUSULA SEXTA. - SANCIONES:

Para la aplicación de sanciones se tomará en cuenta lo establecido en la Constitución de la República del Ecuador, la Ley Orgánica de Transparencia y Acceso a la Información Pública, Ley Orgánica del Sistema Nacional de Registro de Datos Púbicos y demás normativa aplicable; sin perjuicio de las acciones civiles y penales que procedan en cada caso.

Los funcionarios públicos que incumplieren las estipulaciones de este instrumento, podrán ser sancionados por la máxima autoridad de la entidad en la que prestan sus servicios, de conformidad con lo determinado en la Ley Orgánica del Servicio Público y su Reglamento.

CLÁUSULA SÉPTIMA. -:

En los casos en que la información sea calificada como “Reservada” o “Confidencial” por mandato legal, las entidades que suscriben el presente acuerdo evaluarán la pertinencia de entregar o no dicha información.

CLÁUSULA OCTAVA. - DOCUMENTOS HABILITANTES:

Para la suscripción del presente instrumento, las partes presentarán las respectivas delegaciones o nombramientos que les permita actuar en representación de las entidades intervinientes.

CLÁUSULA NOVENA. - VIGENCIA:

El presente instrumento tendrá una vigencia de cinco años a partir de la fecha de suscripción.

CLÁUSULA DÉCIMA - ACUERDO TOTAL:

Este acuerdo incluye el total entendimiento entre las partes con relación a la materia de la cual se trata este documento. Cualquier añadidura o modificación a este acuerdo deberá ser hecha por escrito y firmada por ambas partes.

CLÁUSULA DÉCIMA PRIMERA: NOTIFICACIONES. -

En el evento de que se produzca el incumplimiento de alguna de las cláusulas estipuladas en el presente acuerdo, la parte afectada, notificará del incumplimiento a la máxima autoridad de la institución involucrada, sin perjuicio de las acciones y sanciones previstas en la normativa vigente.

Una vez comprendido por los comparecientes el contenido y efectos del presente instrumento expresamente se ratifican en él, para fe y constancia se firma el presente documento por quienes en él intervinieron, en la ciudad de Quito, el día___ del mes de_____del año_____, en dos ejemplares del mismo tenor y validez.

Nombres y apellidos	**Nombres y Apellidos:**
Coordinador del área de TICS del ITSCT	**CARGO:**