UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE TECNOLOGÍAS DE LA INFORMACIÓN, TELECOMUNICACIONES E INDUSTRIAL

MAESTRÍA EN GERENCIA DE SISTEMAS DE INFORMACIÓN

Tema: "Gestión de la Seguridad de la Información basado en la Norma ISO/IEC 27001 y su incidencia en las Instituciones de Educación Superior de la ciudad de Machala"

Trabajo de Investigación, previo a la obtención del Grado Académico de Magister en Gerencia de Sistemas de Información

Autor : Ing. Wilson Enrique Cuenca León.

Director: Ing. Kléver Renato Urvina Barrionuevo, Mg.

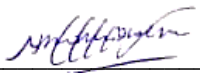
Ambato – Ecuador

2019

A la Unidad Académica de Titulación de la Facultad de Tecnologías de la Información, Telecomunicaciones e Industrial.

El Tribunal receptor del Trabajo de Investigación presidido por la Ingeniera Elsa Pilar Urrutia Urrutia, Mg., e integrado por los señores Ingeniero Edwin Hernando Buenaño Valencia, Mg., Ingeniero David Omar Guevara Aulestia, Mg., Ingeniero Franklin Oswaldo Mayorga Mayorga, Mg., designados por la Unidad Académica de Titulación de Posgrado de la Facultad de Tecnologías de la Información, Telecomunicaciones e Industrial de la Universidad Técnica de Ambato, para receptar el Trabajo de Investigación con el tema: "Gestión de la Seguridad de la Información basado en la Norma ISO/IEC 27001 y su incidencia en las Instituciones de Educación Superior de la ciudad de Machala", elaborado y presentado por el señor Ingeniero Wilson Enrique Cuenca León, para optar por el Grado Académico de Magister en Gerencia de Sistemas de Información; una vez escuchada la defensa oral del Trabajo de Investigación el Tribunal aprueba y remite el trabajo para uso y custodia en las bibliotecas de la UTA.

Ing. Elsa Pilar Urrutia Urrutia, Mg,
Presidenta del Tribunal.



Ing. Edwin Hernando Buenaño Valencia, Mg,
Miembro del Tribunal.

Ing. David Omar Guevara Aulestia, Mg,
Miembro del Tribunal.

Ing. Franklin Oswaldo Mayorga Mayorga, Mg,
Miembro del Tribunal.

AUTORÍA DEL TRABAJO DE INVESTIGACIÓN

La responsabilidad de las opiniones, comentarios y críticas emitidas en el Trabajo de Investigación presentado con el tema: "Gestión de la Seguridad de la Información basado en la Norma ISO/IEC 27001 aplicado a Instituciones de Educación Superior", le corresponde exclusivamente a: Ingeniero Wilson Enrique Cuenca León, Autor bajo la Dirección de Ingeniero Kléver Renato Urvina Barrionuevo, Mg, Director(a) del Trabajo de Investigación; y el patrimonio intelectual a la Universidad Técnica de Ambato.

Ing. Wilson Enrique Cuenca León

C.I, 0703803932

AUTOR

Ing. Kléver Renato Urvina Barrionuevo.

C.I, 1802667970

DIRECTOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que el Trabajo de Investigación, sirva como un documento disponible para su lectura, consulta y procesos de investigación, según las normas de la Institución.

Cedo los Derechos de mi trabajo, con fines de difusión pública, además apruebo la reproducción de este, dentro de las regulaciones de la Universidad.

Ing. Wilson Enrique Cuenca León

C.I, 0703803932

AUTOR

INDICE GENERAL DE CONTENIDOS

INDICE DE FIGURAS.

INDICE DE TABLAS.

AGRADECIMIENTO

Agradezco a Jehová Dios por permitirme culminar esta etapa de mi vida. A mis padres Rosario y Eloy por haber inculcado estudiar y superarme, a las personas que estuvieron en este ciclo profesional de mi vida, agradecerles por su amistad, consejo y apoyo.

Al Ing. Renato Urvina, director de proyecto de investigación, por su tiempo y dedicación como guía para el desarrollo de este trabajo.

Wilson

DEDICATORIA

Con inmenso amor dedico este trabajo a mis padres, hermana y amigos quienes siempre han sido mi fuente de inspiración, han confiado en mí y me han apoyado para alcanzar las metas propuestas.

Wilson

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE TECNOLOGÍAS DE LA INFORMACIÓN, TELECOMUNICACIONES E INDUSTRIAL.

MAESTRÍA EN GERENCIA DE SISTEMAS DE INFORMACIÓN

TEMA:

"Gestión de la Seguridad de la Información basado en la Norma ISO/IEC 27001 y su incidencia en las Instituciones de Educación Superior de la ciudad de Machala**"**

AUTOR: Ing. Wilson Enrique Cuenca León.

DIRECTOR: Ing. Renato Urvina Barrionuevo, Mg.

FECHA: 26 de marzo de 2019.

RESUMEN EJECUTIVO

La información en la actualidad es el activo más importante que tiene una organización, de ella depende el éxito o fracaso de la misma, su seguridad, administración y óptimo desempeño requieren de un análisis para protegerla de cualquier riesgo a la que está expuesta. Este antecedente permite realizar esta investigación, que trata sobre la gestión de la seguridad de la información basada en la norma ISO/IEC 27001 y su incidencia en la información de las Instituciones de Educación Superior de la Ciudad de Machala.

Se ha creado políticas de seguridad, que permiten una mejor gestión de la seguridad de la información, basada en la norma de seguridad ISO/IEC 27001:2013, que incorpora 14 dominios, 35 objetivos de control y 114 controles que facilitan el tratamiento, preservación, confiabilidad, integridad y disponibilidad de la información que gestiona toda organización, además del uso de instrumentos de monitoreo que permiten monitorear amenazas y vulnerabilidades que se presentan en este estudio.

La metodología utilizada se sustentó en el ciclo de mejora continua P.D.C.A. (Planear, Hacer, Chequear y Actuar), que está constituida por 4 fases, donde cada fase comprende etapas y actividades que permiten planificar, determinar su alcance, realizar un inventario y la valoración de los activos con el objetivo de evaluar y analizar los riesgos,

amenazas y vulnerabilidad que intervienen en la gestión de la seguridad de la información.

La metodología permitió seleccionar e implementar controles para mitigar y evitar los riesgos detectados en las diferentes etapas con el objetivo de medir y determinar el grado de incidencia que tiene la aplicación de esta metodología en la gestión de la seguridad de la información de las instituciones de Educación Superior de la ciudad de Machala, fomentado las buenas prácticas de gestión de seguridad de la información en los departamentos de tecnologías de la información y comunicación.

Referencias: Gestión, Seguridad de información, ISO/IEC 27001, sistema, vulnerabilidad, metodología, modelo, control, proceso, dominio, Tics, PDCA, riesgo.

.

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE TECNOLOGÍAS DE LA INFORMACIÓN, TELECOMUNICACIONES E INDUSTRIAL.

MAESTRÍA EN GERENCIA DE SISTEMAS DE INFORMACIÓN

THEME:

"Information Security Management based on the ISO / IEC 27001 Standard and its impact on the Higher Education Institutions of the city of Machala"

AUTHOR: Ing. Wilson Enrique Cuenca León.

DIRECTED BY: Ing. Renato Urvina Barrionuevo, Mg.

DATE: March 26st, 2019.

EXECUTIVE SUMMARY

The information currently is the most important asset that an organization has, it depends on the success or failure of it, its security, administration and optimal performance require an analysis to protect it from any risk to which it is exposed. This background allows us to carry out this research, which deals with the management of information security based on the ISO / IEC 27001 standard and its impact on the information of the Higher Education Institutions of the City of Machala.

Security policies have been created, which allow a better management of information security, based on the ISO / IEC 27001: 2013 security standard, which incorporates 14 domains, 35 control objectives and 114 controls that facilitate the treatment, preservation, reliability, integrity and availability of the information managed by any organization, in addition to the use of monitoring tools that allow monitoring of the threats and vulnerability presented in this study.

The methodology used was based on the continuous improvement cycle P.D.C.A. (Plan, Do, Check and Act), which consists of 4 phases, where each phase includes stages and activities that allow planning, determine its scope, perform an inventory and the valuation of assets in order to assess and analyze the risks, threats and vulnerability that intervene in the management of information security.

The methodology allowed to select and implement controls to mitigate and avoid the risks detected in the different stages with the objective of measuring and determining the degree of incidence that the application of this methodology has in the management of information security of educational institutions. Superior of the city of Machala, fostered good information security management practices in the departments of information and communication technologies.

Keywords: Management, Information Security, ISO / IEC 27001, system, vulnerability, methodology, model, control, process, domain, Tics, PDCA, risk.

INTRODUCCIÓN

La presente investigación está orientada a la gestión de la seguridad de la información basado en políticas de seguridad de la norma ISO/IEC 27001, donde se analiza como esta gestión incide en la información de las instituciones de educación superior de la ciudad de Machala, destacando que la aplicación de esta normar tendrá un impacto positivo, pues se obtendrá los resultados esperados si los requerimientos para llevar a cabo esta gestión son tomados en cuenta (Garcés Suárez, Garcés Suárez, & Alcívar Fajardo, 2016), al mismo tiempo garantice seguridad en los diferentes servicios críticos que ofrecen los departamentos de Tecnologías de la Información y Comunicación, académicos, administrativos, por ejemplo, servicios de: registros, admisión, matriculación, administración, contabilidad, informática entre otros servicios que prestan las instituciones de educación superior (Sevillano, 2016).

Es sustancial cuando las instituciones de educación superior se enfocan en el proceso de gestionar la seguridad de la información; cambiará en algunos casos las modalidades de trabajo, se modificarán procesos vitales institucionales, se implantarán nuevos controles (Cruz Micán, Perea Sandoval, & Ruiz López, 2018); ante estas circunstancias cabe destacar que el personal que toma decisiones dentro de las instituciones tengan la convicción y el conocimiento avanzado, además su apoyo será indispensable para llevar adelante los cambios. (Isotools, 2018).

El CAPÍTULO 1, EL PROBLEMA, describe el tema de investigación, el planteamiento del problema, su contexto, el análisis crítico, prognosis, la formulación del problema, las interrogantes, la delimitación, la justificación de la investigación, los objetivos tanto general como los específicos.

El CAPÍTULO 2, MARCO TEÓRICO, detalla los antecedentes de la investigación con la revisión de la literatura y el estado del arte del tema, la fundamentación filosófica y legal sobre la cual se enmarca la investigación, las categorías fundamentales, las variables dependiente e independiente, la hipótesis y el señalamiento de variables.

El CAPÍTULO 3, METODOLOGÍA, está constituido por el enfoque, modalidad y tipo de investigación, la determinación de la población y la muestra que serán parte de la investigación, la operación de variables, las técnicas e instrumentos de investigación, y los planes de recolección y de procesamiento de la información.

El CAPÍTULO 4, ANALISIS E INTEPRETACIÓN DE RESULTADOS, detalla el análisis e interpretación de los resultados obtenidos a través de los métodos de investigación utilizados y la comprobación de la hipótesis planteada.

El CAPÍTULO 5, CONCLUSIONES Y RECOMENDACIONES, detalla las conclusiones y recomendaciones en base a la investigación realizada dando cumplimiento a los objetivos de la investigación planteada.

El CAPÍTULO 6, describe una propuesta de solución al problema con el detalle necesario para que sea comprendida por los lectores: datos informativos, antecedentes y justificación, objetivo general y objetivos específicos, análisis de factibilidad, fundamentación y metodología del modelo operativo y previsión de evaluación.

Finalmente, se incluyen los anexos y la bibliografía que sustenta la investigación planteada.

CAPÍTULO I.

1. EL PROBLEMA DE INVESTIGACIÓN

1.1 Tema de Investigación.

Gestión de la Seguridad de la Información basado en Norma ISO/IEC 27001 y su incidencia en la información de las Instituciones de Educación Superior de la ciudad de Machala.

1.2 Planteamiento del problema

1.2.1 Contextualización

La evolución de los métodos de almacenamiento de la información, los protocolos de comunicación y por ende las técnicas de ataques a sistemas informáticos en los últimos años ha tenido un fuerte avance en Latinoamérica, especialmente a instituciones educativas de nivel superior en países como Argentina, Chile que se encuentra en proceso de mejoramiento de seguridad de información. (Sullivan, 2016)

En Ecuador, algunas instituciones de educación superior consideran a la información como un problema de tipo tecnológico, demandando el replanteamiento de normas de seguridad de información y los mecanismos que las instituciones de educación superior deben aplicar para mantener con seguridad sus activos más productivos. La seguridad de información tiene por obligación estar acorde estratégicamente con el listado de servicios generales que prestan las instituciones educativas y apoyarse en la tolerancia a los riesgos de la misma (Albornoz, Barrere, Castro Martínez, & Fernández de Lucio, 2016).

En la provincia de El Oro, las instituciones de educación superior cuentan con diferentes sistemas informáticos que colaboran en gran medida a la gestión de la información, sin embargo, la mayoría de los mismos no cuentan con mecanismos y estrategias para hacer frente a ataques externos, riesgo de seguridad y resguardar información producidos por el alarmante crecimiento de ataques de información a nivel mundial (Vera-Cruz, 2016).

Al mismo tiempo en algunos departamentos de las Instituciones de Educación Superior de la ciudad de Machala aún se mantiene la gestión de administrar equipos servidores de datos sin las protecciones que requiere el caso, es decir, protección física contra intrusos y lógica de no respaldo de datos, originando diferentes causas y efectos que resulta en la problemática generalizada como se puede observar en la Fig. 1.

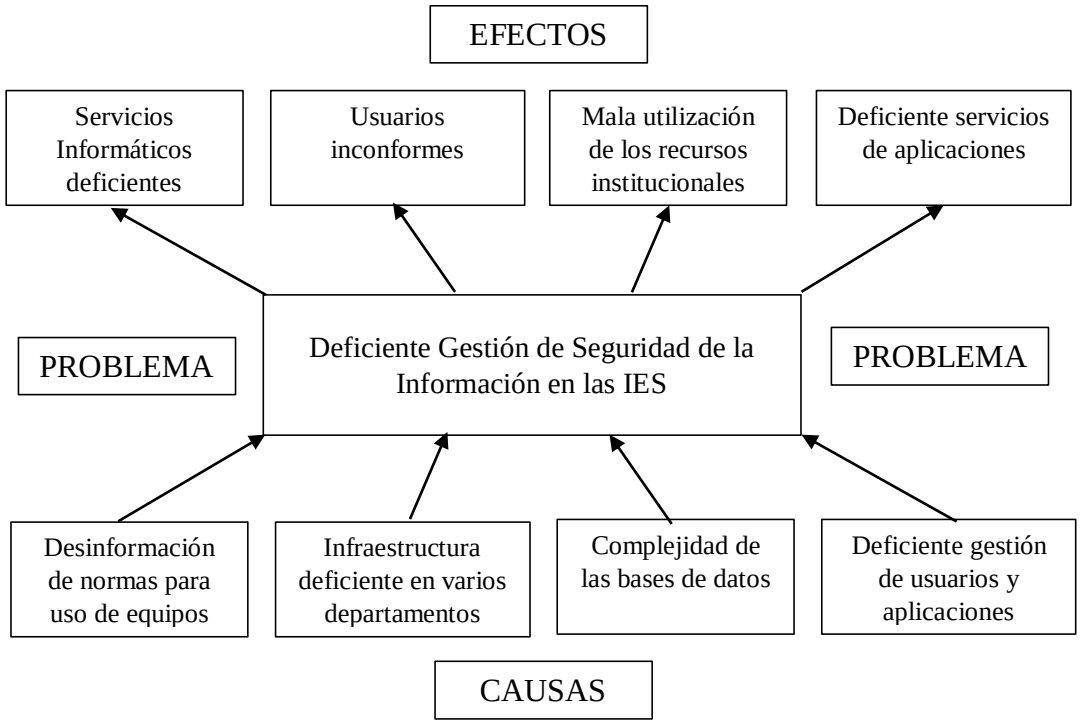


Figura 1. Árbol de Problemas.

Elaborado por: Investigador.

1.2.2 Análisis crítico

Las instituciones de Educación Superior de la ciudad de Machala, junto a sus máximas autoridades, personal docente y administrativo vienen ejecutando en su gestión de procesos, sistemas informáticos que son aplicados y comprendidos por el alto número de evidencias requeridas, sin embargo, la ejecución y desempeño de estos procesos en la práctica real no han cubierto la demanda de necesidades requeridas, al contrario han ocasionado problemas de gestiones de seguridad y mala organización en la administración de sus recursos informáticos.

A su vez es latente la falta de políticas y lineamientos para el control, administración y manejo de información, además se corroboró en algunos departamentos de las instituciones de educación superior, aún se lleva manualmente la recopilación de datos.

Estos inconvenientes presentados han provocado una mala gestión de información y su vez han ocasionado problemas tanto para usuarios como para el personal que administra y procesa datos en las instituciones educativas superiores, debido a la lentitud al momento de ingresar información, lo que repercute en la reiteración de procesos, que, a su vez, resulta pérdida de tiempo, dinero y recursos, ocasionando en los activos y hardware de comunicación una mala y deficiente respuesta.

Además pueden ocurrir fraudes informáticos, impresión de dudosos reportes del status real de equipos presentes, pobre administración de usuarios, claves y permiso de acceso a los sistemas, originando un alto riesgo en cuanto a pérdida y robo de información, que muchas de las veces ocurre y que no se actúa a tiempo (Pearson, 2016).

Debido a la falta de aplicación de una gestión de seguridad de información basada en una norma de seguridad establecida, que permita definir soluciones prácticas y efectivas para una mejor organización de los procesos de seguridad de la información que se presentan diariamente en las instituciones de educación superior, se hace necesario definir una norma de seguridad de información ISO/IEC 27001 para medir, controlar, monitorear y mejorar el grado de peligrosidad, amenazas y vulnerabilidades a las que están expuestos los activos.

1.2.3 Prognosis.

Las instituciones de educación superior en su mayoría no cuentan con sistemas que gestionen procesos que conlleva la seguridad de la información y no perciben el peligro al que está expuesta su información en caso de ataques externos y en el caso de no tomar medidas necesarias y correctivas en cuanto a la inseguridad de la información que poseen, la vulnerabilidad de la misma se ve expuesta, poniendo en riesgo la gestión de la seguridad de su información cuando se requiere tener confiabilidad, integridad y disponibilidad (Heinekn, 2016).

De no aplicarse la gestión de la seguridad de la información, se seguirán ejecutando procesos inadecuados, que se verán reflejados en pérdidas de tiempo y dinero, porque el éxito de las instituciones de educación superior depende del personal que labora y las tareas que realizan, por esta razón es fundamental invertir en capacitaciones en cuanto a seguridad de información, para tener una mejor organización gracias a la gestión de la seguridad de la información, y además se fomentará un mejor trabajo en equipo, mejor clima laboral y una mayor seguridad para los datos de las instituciones de educación superior.

1.2.4 Formulación del problema

¿Incide la gestión de seguridad de la información basada en la norma ISO/IEC 27001 en la información de las instituciones de educación superior de la ciudad de Machala?

1.2.5 Interrogantes (Subproblemas)

- ¿Cuáles son las normas de seguridad aplicadas a la gestión de la seguridad de la información en las Instituciones de Educación Superior?

- ¿Cuáles son las técnicas de protección y seguridad de la información aplicados actualmente en el procesamiento de datos de las Instituciones de educación superior?

- ¿Cuáles son los niveles de confiabilidad, integridad y disponibilidad con que cuentan los sistemas de información y comunicación de las Instituciones de Educación Superior?

1.3 Justificación.

La realización de la presente investigación es de gran relevancia, porque permite gestionar la seguridad de la información basada en la norma ISO/IEC 27001 en las instituciones de educación superior de la ciudad de Machala, para que cumplan con sus objetivos enfocados en la gerencia informática y los resultados ayuden para que estas organizaciones cuenten con normativas adecuadas para gestionar y proteger sus datos, procesos, privacidad y estrategia de seguridad de la información.

La importancia de los crecientes cambios tecnológicos y las amenazas a las están expuestas las instituciones educación superior conllevan a la necesidad de una gestión de la seguridad de la información que ayude a proteger tanto los datos como los recursos institucionales por medio de la aplicación de normas de seguridad establecidas, permitiendo su ajuste en un entorno de organizaciones competitivas en base a identificar, tasar y evaluar activos, además de analizar riesgos y vulnerabilidades a las que están expuestos estos activos.

Actualmente, los departamentos de Tecnologías de la Información y Comunicación (Tics) de las Instituciones de Educación Superior de la ciudad de Machala no disponen de un Sistema de Gestión de Seguridad de la Información que ayude a gestionar la seguridad de la información, por lo que es necesario aplicar una metodología que permita integrar y organizar de forma cíclica los requisitos para gestionar la seguridad de la información basada en la norma ISO/IEC 27001.

Este proyecto será factible porque cuentan con los recursos bibliográficos y tecnológicos para desarrollar la solución planteada, además gestionar la seguridad de la información basada en la norma ISO/IEC 27001 es fundamental en una organización, porque en ella se establecerán procesos que permitirán mejorar la calidad de la gestión informática en sus departamentos de Tecnologías de la Información y Comunicación, la misma que podrá servir como modelo de seguridad, beneficiando a otras instituciones para que puedan adaptar esta gestión a su sistema de mejora continua.

1.4 Objetivos

1.4.1 Objetivo General

Determinar la incidencia de la Gestión de la Seguridad de la Información basada en la Norma ISO/IEC 27001 en la información de las Instituciones de Educación Superior.

1.4.2 Objetivos Específicos

- Establecer un modelo de seguridad para la Gestión de la Seguridad de la Información basada en la norma ISO/IEC 27001.

- Establecer una metodología para un modelo de seguridad para la gestión de la seguridad de la información basada en la norma ISO/IEC 27001.

- Evaluar los diferentes parámetros de confidencialidad, integridad y disponibilidad de los sistemas de información y comunicación de las instituciones de educación superior.

- Implementar el Sistema de Gestión de Seguridad de la Información sustentado en la norma ISO/IEC 27001 para operar monitorear, revisar, mantener y mejorar la gestión de la seguridad de la información de las Instituciones de Educación Superior.

CAPÍTULO II.
2. MARCO TEÓRICO

2.1 Antecedentes investigativos

Revisadas similares investigaciones en la universidad y otras fuentes alternativas bibliográficas se han localizado los siguientes proyectos de investigación.

Luis Miguel Pazmiño Vallejo en el año 2015, en su proyecto de investigación, Calidad de la Gestión en la Seguridad de la Información basada en la norma ISO/IEC 27001 en Instituciones Públicas en la ciudad de Quito, donde utilizó una metodología de evaluación basada en la norma de seguridad informática ISO/IEC 27001:2011 para entender el nivel de calidad de la gestión en lo que respecta la seguridad de información en las instituciones públicas y en sus conclusiones menciona lo siguiente: Debido a la falta de implementar una norma de seguridad, controles y políticas para gestionar la seguridad de la información en las instituciones públicas han ocurrido varios imprevistos en sus sistemas de información y comunicación, ocasionando pérdidas en cuanto a tiempo y dinero y generando el temor informático en los usuarios.

Holguer Eduardo Chaso Salazar, en el año 2017, en su proyecto de investigación, Gestión de Seguridad Informática y su incidencia en la información de la Universidad Técnica de Ambato, donde utilizó la metodología PDCA de mejora continua basada en la norma de seguridad informática ISO/IEC 27001 para analizar la incidencia de la gestión de la seguridad de la Información, los procesos, la organización y la protección de la información del Departamento de Tecnologías de la Información y Comunicación (DITIC) de la Universidad Técnica de Ambato y en sus conclusiones menciona lo siguiente: La norma ISO/IEC 27001 cuenta con lineamientos establecidos para gestionar la seguridad de la información en una organización, y a través de esta gestión se pueden prevenir, eliminar y mitigar riesgos, amenazadas y vulnerabilidades a la que está expuesta la información, sin embargo, la aplicación de la gestión informática con esta norma no siempre se ejecuta porque no existe los conocimientos que conlleva el manejo de la información en las instituciones por parte de sus autoridades y funcionarios.

Sandra Maribel Criollo Tasincha en el año 2017, en su proyecto de investigación, Análisis e Implantación de la Norma ISO/IEC 27002:2013 para el departamento Informático del Gobierno Autónomo Descentralizado Municipal del Cantón Salcedo, donde utilizó la metodología basada en la norma de seguridad informática ISO/IEC 27002:2013 para analizar e implantar políticas y controles de seguridad en la gestión de la información del departamento de informática y en sus conclusiones menciona lo siguiente: La importancia de la restricción de la información en los centros de procesamiento, estableciendo lineamientos de seguridad para la información en base a la norma ISO 27002:2013, porque las políticas de seguridad minimizan pérdidas de información y garantizan los procesos, además de estar actualizados en los ámbitos de tecnología, telecomunicaciones, documentación y manuales para la estandarización de los procesos. La implantación de la norma ISO propuso planes para elaborar formatos en base de las necesidades del departamento informático para buscar la mejora en los servicios prestados y contribuir con el crecimiento y excelencia.

2.2 Fundamentación filosófica.

La presente investigación se enmarca en el paradigma Crítico Propositivo, Crítico debido a que realiza un Análisis Crítico del problema y Propositivo debido a la búsqueda de proponer una solución factible al problema.

2.3 Fundamentación legal.

Cuando se ejecuta una Gestión de Seguridad de la Información, toda organización tiene requerimientos que cumplir, apegarse a leyes, estándares, mandatos aplicables en la obtención de objetivos y avance de actividades englobadas en estos proyectos.

En lo que se expone detalladamente en cuanto a Seguridad de la Información, algunas de las leyes y normas de la legislación ecuatoriana tomados de (Deloitte, 2017).

La presente tesis de investigación se basa en las siguientes leyes:

Ley de comercio electrónico, firmas y mensajes de datos

Ley No. 67. R.O. Suplemento 557 de 17 de abril del 2002.

TÍTULO PRELIMINAR

Artículo 1.- Objeto de la Ley. – Este decreto reglamenta los mensajes de datos, la firma electrónica, los servicios de certificación, la protección a los usuarios de estos sistemas, el comercio electrónico, la contratación electrónica, la prestación de los servicios electrónicos, por medio de las redes de información y disciplina científica y tecnología de la telemática (Congreso , 2017).

TÍTULO I

DE LOS MENSAJES DE DATOS

CAPÍTULO I

PRINCIPIOS GENERALES

Artículo 2.- Identificación jurídica de los mensajes de datos. - Los mensajes de datos mantendrán igual valor jurídico semejante a los documentos escritos. La eficiencia, valoración y efectos de los mensajes de datos permanecerán sujetos al cumplimiento definido en este reglamento y su estatuto.

Artículo 3.- Inclusión por remisión. - Se distingue valor jurídico a la información no contemplada en los mensajes de datos y que resida en el mismo, de manera de remisión por medio de una dirección electrónica, inspeccionando su contenido y admitido por las partes.

Artículo 4.- Propiedad Intelectual. - Los mensajes de datos estarán sujetos a las reglas internacionales reconocidos relacionadas a la propiedad intelectual.

Artículo 5.- Confidencialidad y reserva. - Se definen valores de confidencialidad y reserva para los mensajes de datos, la manera que sea. Si no se cumple con estos términos, específicamente a las asociadas a la intromisión electrónica, transferencia ilícita de mensajes de los datos, se condenará lo establecido en esta ordenanza y otros reglamentos que rigen la materia.

Artículo 6.- Información escrita. - Cuando ocurra el evento este estatuto necesitará que la información, se dé por escrito, esta condición estará cumplida con los mensajea de datos, siempre y cuando la información que comprenda sea entendible para luego consultarla.

Artículo 7.- Información Verídica. - Cuando suceda el evento que este reglamente condicionará que la información sea mostrada en su manera original, este condicionamiento estará cumplido con un mensaje de dato, se considera mensajes de datos íntegros, si los mismo no tienen alterado su contenido, excepto alguna modificación, propio del transcurso de su visualización.

Artículo 8.- Preservación de los mensajes de datos. - La información sujeta a este reglamento, podrá mantenerse; está condición estará cumplida por medio del archivo del mensaje de datos, si se cumplen las condiciones a continuación se detallan.

a) La información abarcada sea procesable para su posterior consulta;
b) La conservación de datos con la manera con que se haya generado, enviado o receptada sea demostrable, que reproduce exactamente la información generada, enviada o receptada;
c) La preservación de los datos que permitan definir su origen, el destino del mensaje, la fecha y la hora en que fue creado, producida, procesado, enviado, recibido y archivado; y,
d) La integridad de datos mantenida por el lapso de tiempo que se determine en el reglamento a esta norma.

Artículo 9.- Preservación de los datos. - Para el establecimiento, transferencia y uso de bases de datos, se requerirá del permiso del propietario de éstos, quien podrá escoger la información a distribuir con otras personas.

Artículo 10.- Pertenencia e identidad de los mensajes de datos. – Se comprende que los mensajes de datos pertenecen de quien envía y permite quien reciba, para actuar lo dispuesto al contenido del mismo, si en su revisión hay concordancia entre la identificación del emisor y su firma electrónica, salvo en los siguientes casos.

a) Se comunica que el mensaje de dato no proviene de quien se considera emisor; en este caso, el aviso se lo realiza antes de que la persona que lo recibe actúe conforme a dicho mensaje. Caso contrario, quien sea considerado emisor tiene que justificar que el mensaje de datos no se produjo o no se modificó por orden del mismo,

b) Si la persona que envía no hubiese efectuado los controles adecuados de su resultado.

Artículo 11.- Emisión y recepción de los mensajes de datos. - Excepto acuerdo en contrario, se supondrá que el tiempo y el lugar de la emisión y recepción del mensaje de datos, son los detallado a continuación.

a) **Instante de envío del mensaje de datos. -** Cuando el mensaje de datos sea ingresado en un sistema de información y este no contenga el seguimiento del emisor que envió el mensaje en nombre del dispositivo electrónico facilitado para el efecto;

b) **Instante de recepción del mensaje de datos. -** Cuando el mensaje de datos sea ingresado al sistema de información por la persona que lo recibe, si este designa otro sistema de información, el instante de recepción se supondrá cuando se origine la recuperación del mensaje de datos. Si no se designa un sitio determinado de recepción, se comprenderá que ésta ocurre cuando el mensaje de datos ingresa a un sistema de información de la persona que lo envía, independientemente de haberse recuperado o no el mensaje de datos; y,

c) **Sitios de envío y recepción. -** Los establecidos por las partes, domicilios verídicos que estén registrados en el certificado de firma electrónica, del emisor y del receptor. Si no se podría establecer por estas vías, se comprenderá el lugar de trabajo donde desarrollen sus actividades asociadas con el mensaje de datos.

Artículo 12.- Duplicación de los mensajes de datos. - Los mensajes de datos será considerados diferentes. Si existe la sospecha de alguna irregularidad, las partes requerirán la confirmación del nuevo mensaje y disponer del derecho de revisar la integridad del mismo (Congreso , 2017).

2.4 Categorías fundamentales

2.4.1 Supra-ordenación de variables

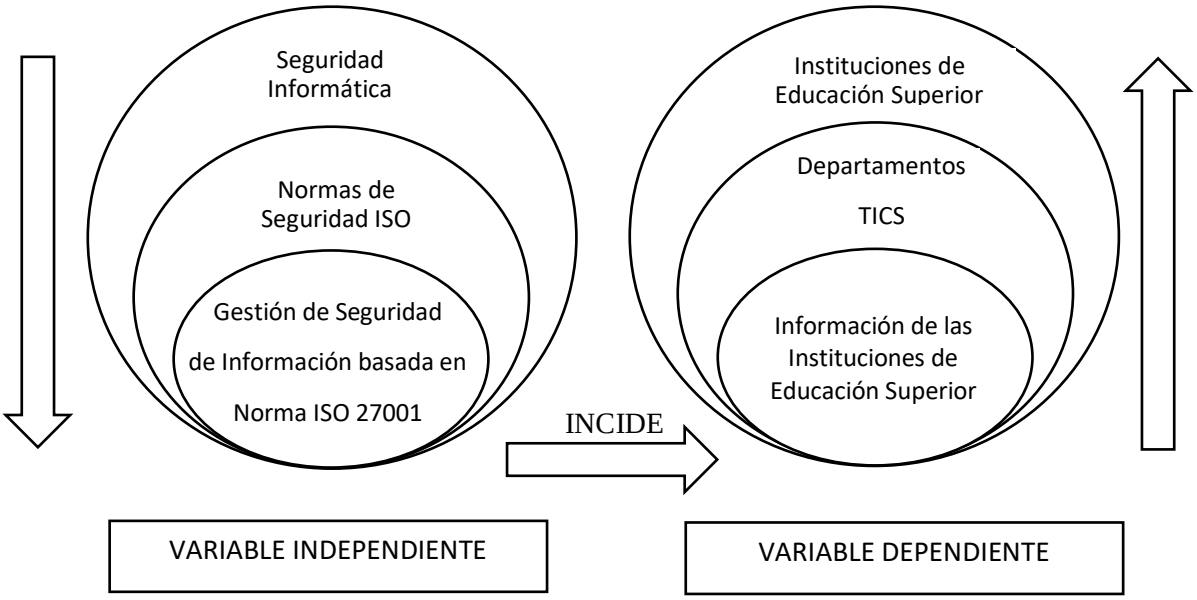


Figura 2. Inclusiones conceptuales.

Elaborado por: Investigador

2.4.2. Sub-ordenación de variables.

Figura 3. Constelación de ideas de Variable Independiente.

Elaborado por: Investigador.

2.4.3 Sub-ordenación de variables.

Figura 4. Constelación de ideas de la Variable Dependiente.

Elaborado por: Investigador

2.4.4 Categorías de la Variable Independiente

Gestión de Seguridad de Información.

Conjunto de sistemas que ejecutan técnicas sistematizadas para garantizar la seguridad de la información, está enmarcada en procesos documentados y de conocimiento público por los encargados de la organización.

La gestión de la seguridad de la información está basada en un Sistema de Gestión de Seguridad de la Información, que es un conjunto de herramientas y operaciones tales como: Planificar, Implementar, Monitorear, Mantener y Mejorar la gestión para garantizar la seguridad de la información en una organización (Excellence I. , IsoTools Blog Calidad y Excelencia, 2016), mitigando peligros, riesgos, vulnerabilidades de la información, permitiendo una mejor organización de los recursos de la organización y al mismo tiempo lograr un impacto positivo en la confidencialidad, integridad y disponibilidad de la información, (Cordova, Viñas, & Coria, 2017).

Norma.

Conforme a la investigación del archivo (equipoteccelaya, 2018), una norma es la redacción y admisión de reglas que se establecen para garantizar la adaptación de componentes construidos independientemente, también garantiza el repuesto en caso de ser necesario, manteniendo la calidad de elementos fabricados y la seguridad de su funcionamiento.

Según la ISO (International Organization for Standarization) la normalización es la actividad que tiene por finalidad establecer, de acuerdo a los problemas, disposiciones orientadas a aplicaciones generales y repetidas, para lograr un grado de ordenamiento ideal en un entorno, por ejemplo, en un ambiente del tipo tecnológico, político o económico (Serrano Antón, 2017).

ISO.

Conforme a la investigación del archivo (Gobierno del Estado, 2016), la Organización Internacional de Estandarización (ISO) es una confederación de nivel global constituida por reglamentos de estandarización nacionales de 164 países, uno por cada país. La ISO es una institución que no depende de ningún gobierno, fundada en el año de 1947.

La misión de la ISO es fomentar el desarrollo de la estandarización en el mundo relacionadas con esta norma, cuyo fin es ayudar permutando servicios y bienes, además de fomentar la cooperación en el campo intelectual, económico, científico, tecnológico.

ISO/IEC 27001.

Como señala la 27001 Academia, la ISO/IEC 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una organización. La primera revisión se publicó en el año 2005 y fue desarrollada con base en el estándar británica BS 7799-2 (Bustamante Maldonado & Osorio Cano, Metodología de la seguridad de la información como medida, 2017).

ISO 27001 puede ser implementada en toda organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información dentro de una organización. Permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización, en cumplimiento con la norma ISO 27000 (Bustamante Maldonado & Osorio Cano, Metodología de la seguridad de la información como medida, 2017).

La norma ISO 27001 es una herramienta técnica de mejora continua basada en la metodología del ciclo PDCA, que permite implementar un Sistema de Gestión de Seguridad de la Información (SGSI) para analizar y evaluar diferentes tipos de vulnerabilidades, riesgos o amenazas susceptibles que atenten contra la información de una organización, sea esta propia o datos de terceros (Excellence I. , 2016).

Esta norma, está establecida por cláusulas, dominios, objetivos de control y controles, donde la parte fundamental del Sistema de Gestión de Seguridad de Información está comprendido por siete clausulas (Ver Anexo 2) y 14 Dominios, 35 Objetivos de dominio y 114 controles (Ver Anexo 3).

Las cláusulas estas constituidas por los procedimientos que deben implementarse, documentos que deben elaborarse y los registros que deben ser conservarse en la organización. El anexo 3 señala los dominios, los objetivos de control y los controles a implementarse en el sistema de gestión de seguridad de la información.

ISO/IEC 27001, es un sistema basado en la metodología de sistema de gestión enfocados en el ciclo de mejora continua PDCA o ciclo de Deming, llamado así en honor a su creador el estadista estadounidense William Edwards Deming, el cual se sustenta en cuatro fases fundamentales: Planificar-Hacer-Verificar-Actuar (acrónimo de sus siglas en inglés Plan-Do-Check-Act) (Excellence I. , 2016).

Ciclo Deming o PDCA.

Comprende, como principal objetivo, caracterizar una metodología que genere conciencia sobre la importancia de la seguridad de la información y la aplicabilidad de la misma en pequeñas empresas, que garantice un tratamiento seguro de la integridad, disponibilidad y confidencialidad para evitar que dicha información se vuelva pública de una manera no autorizada.

La norma ISO 27001 adopta el ciclo de Deming como metodología, la cual se puede aplicar a todos los procesos que abarca el SGSI. Esta metodología es conocida por sus siglas en inglés PDCA: Plan-Do- Check-Act (Bustamante Maldonado & Osorio Cano, Metodología de la seguridad de la información como medida, 2014).

El ciclo de mejora continua PDCA es un modelo estratégico para la mejora continua, diseñado por físico norteamericano Walter Shewhart en el año de 1920 y presentada por el estadista estadounidense Edwards Deming en el año de 1950, modelo que se sustenta en un ciclo de cuatro fases (Díaz, 2010). Plan (planificar), Do (hacer), Check (verificar) y Act (actuar). A continuación, en la figura 5 se describen brevemente los pasos a seguir en cada fase del ciclo de mejora continua PDCA o ciclo de Deming.

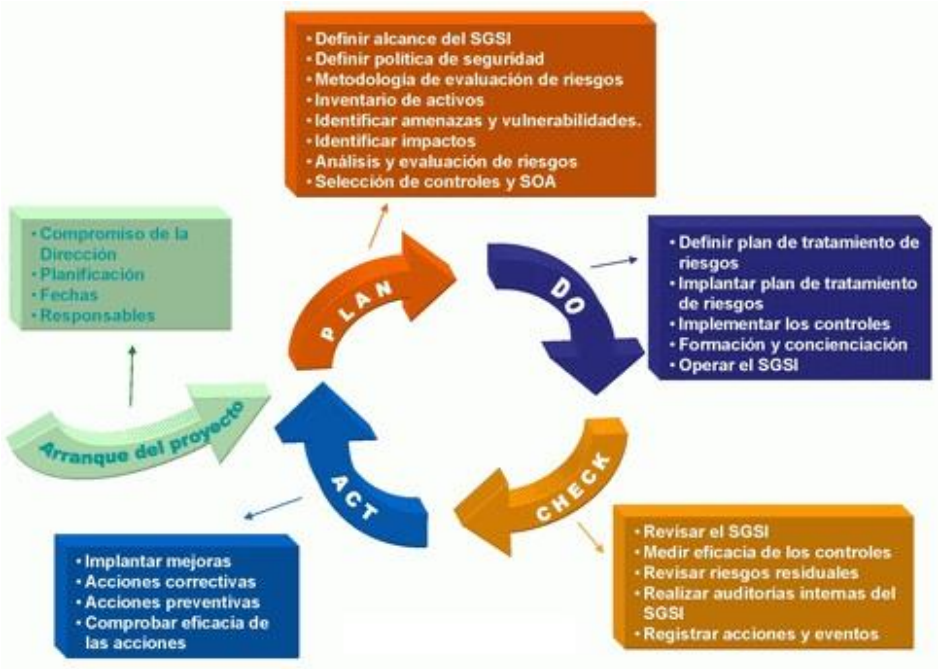


Figura 5. Ciclo PDCA de mejora continua.

Elaborado por: Investigador

Sistema de Gestión de Seguridad de la Información (SGSI)

Conjunto estratégico de herramientas y operaciones tales como: Planificación, Desarrollo, Implementación y Seguimiento para gestionar y garantizar la seguridad de la información en una organización (Excellence I. , IsoTools Blog Calidad y Excelencia, 2016), mitigando peligros, riesgos, vulnerabilidades de la información y al mismo tiempo lograr un impacto positivo en la confidencialidad, integridad y disponibilidad de la información (Cordova, Viñas, & Coria, 2017).

La seguridad de la información, según lo establecido en la norma ISO/IEC 27001, tiene que ver con la preservación, confidencialidad, integridad y disponibilidad de los datos, así como de los sistemas involucrados en su procesamiento en una organización (iso27000.es, 2012).

Para verificar que la gestión seguridad de la información está adecuadamente aplicada se tiene primeramente que identificar su ciclo de vida y las características más destacadas acopladas para garantizar su confidencialidad, integridad y disponibilidad (iso27000.es, 2012):

- Confidencialidad: Información no disponible a personas, organizaciones o procesos indebidos.
- Integridad: Asegurando la exactitud de la información y sus técnicas para procesarla
- Disponibilidad: Autorizaciones y aplicaciones de la información y sistemas de aplicación de la información por usuarios, organizaciones o procesos autorizados cuando estos lo requieran (Cybersecurity, 2018).

Seguridad Informática.

Conjunto de herramientas, políticas, controles, procedimientos y mecanismos que tienen como objetivo principal garantizar la seguridad de la información, además de preservar la confiabilidad, integridad y disponibilidad de los datos de una organización en un sistema. (Informática, 2019).

Auditoria Informática.

Disciplina del campo de la informática que se encarga de la revisión práctica que se realiza sobre los recursos informáticos con que cuenta una organización con el objetivo de analizar, evaluar y emitir un informe o dictamen sobre la situación en que se desarrollan y su utilizan esos recursos. (Aguirre Bautista, 2018).

Gestión de Recursos.

Procesos directivos de obtención, distribución y articulación de recursos humanos, financieros y materiales necesarios para lograr los objetivos de aprendizaje y desarrollo propuestas por la organización. La gestión de personas considera las actividades enfocadas a la implementación de estrategias de mejoramiento de recursos humanos, desarrollo del trabajo en equipo y la generación de un adecuado ambiente de trabajo. (Piñeira Alonso, 2018)

Políticas de Seguridad.

Conjunto de requisitos definidos por los responsables directos o indirectos de un sistema que indica en términos generales que esta y que no está permitido en el área de seguridad durante la operación general de dicho sistema. Concepto amplio para todos los sistemas que quieran ser seguros, pero no da especificaciones concretas para cada uno de los sistemas seguros. La política de seguridad aplicada a un sistema en concreto se denominará política de aplicación específica. (Hernández Figueroa, 2018)

Control y Prevención de Riesgos.

El control de riesgos se orienta a evitar, reducir y eliminar los peligros en una organización, además de a minimizar las causas de los accidentes, evitar daños a la integridad física de los trabajadores, a las maquinarias y las instalaciones; así como evitar pérdidas económicas en general y crear un clima de confianza y tranquilidad en la empresa. (Martinez Acuña, 2018)

2.4.5 Categorías de la Variable Dependiente

Información.

Constituida por un conjunto de datos ya supervisados y ordenados acerca de algún suceso, que sirven para construir un mensaje basado en un hecho, fenómeno o situación, que organizados en un contexto determinado tienen su significado, cuyo propósito puede ser el de reducir la incertidumbre o incrementar el conocimiento acerca de algo. La información permite tomar resolver problemas y tomar decisiones, ya que su aprovechamiento racional es la base del conocimiento. (Thompson, 2018)

Instituciones de Educación Superior (IES).

Organizaciones encargadas de formar profesionales de nivel técnico, tecnológico, tercer y cuarto nivel. Las Instituciones de Educación Superior se clasifican en institutos, universidades y politécnicas. (Senescyt, 2018)

Tecnologías de la Información y Comunicación (Tics).

Las Tics son recursos, herramientas y programas que se usan para procesar, administrar y compartir la información por medio de diversos soportes tecnológicos: computadoras, dispositivos móviles, TV, etc.

Las TIC en la sociedad son necesarias debido a los servicios que ofrecen: banca en línea, correo electrónico, búsqueda de información, descarga de música, cine, comercio electrónico, etc. Así, las Tics han incursionado en diferentes entornos de la vida, principalmente la educación. (Unam, 2018)

Departamento de Tics

Departamento encargado de realizar actividades tales como: planificar, definir mecanismos, direccionar y estudiar diferentes arquitecturas de tecnologías de la información. Tiene en su responsabilidad:

- Plantear nuevos mecanismos, estrategias, estándares y juicios para la planificación, establecimiento de técnicas y la mejor elección de la arquitectura TIC que sea requerida.
- Elaborar diseños, implementaciones y supervisión de la correcta ejecución de políticas en materia de TIC en una organización.
- Administras nuevos proveedores y recursos de la información de la organización.
- Administrar el buen uso de las licencias de software y su respectiva distribución en los departamentos que lo requieran. (Van Der Horst, 2017).

Aplicaciones informáticas.

Cuando mencionamos aplicaciones informáticas hablando de programas asociados con esa temática que representan una herramienta fundamental para que los usuarios puedan ejecutar diferentes tipos de labores, donde las aplicaciones informáticas se diferencian de los sistemas operativos, porque estos últimos permiten que estas aplicaciones puedan funcionar. (Comunicaciones, 2018)

Redes de datos.

Las redes de datos se han originado de la necesidad de transferir información a través del intercambio de datos. Las redes de datos son elaboradas y basadas en una arquitectura tecnológica que facilite los logros aplicativos de una organización. Estas redes de datos generalmente están basadas en la intercambio de comunicaciones de paquetes y se caracterizan por su magnitud, longitud que recorre y su arquitectura física. (Rodriguez Velez, 2017)

Datos.

Los datos permiten visualizar situaciones que independientemente no suministran información, Es la unión de la examinación y la experiencia que ayudan a que un dato puede adquirir algún valor instruccional. Además, los datos cuentan con aspectos pertenecientes a cualquier ente. (Conceptodefincion, 2017)

2.5 Hipótesis.

La Gestión de la Seguridad de la Información basado en norma ISO/IEC 27001 si incide en la información de las instituciones de educación superior.

2.6 Señalamiento de variables.

2.6.3 Variable Independiente: Gestión de Seguridad de la Información basado Norma ISO/IEC 27001.

2.6.4 Variable Dependiente : Información de las Instituciones de Educación Superior.

CAPITULO III

3. METODOLOGÍA

3.1 Enfoque

La presente investigación tiene un enfoque cuali-cuantitativo, porque se utilizarán parámetros de medición en la variable independiente; también es cualitativa porque se emitirán juicios de valor respecto al uso de la norma ISO/IEC 27001 en procesos de gestión de seguridad de la información.

3.2 Modalidad básica de la investigación.

Investigación Aplicada.

La presente tesis de investigación tiene un enfoque aplicado porque buscar encontrar estrategias, políticas y mecanismos que permitan mejorar la seguridad de la información en las instituciones de educación superior.

Investigación Bibliográfica.

La presente investigación será bibliográfica apoyada en libros, documentos técnicos, trabajos investigativos anteriores, revistas, artículos y leyes existentes para la elaboración del marco teórico acerca de la gestión de la seguridad de la información sustentada en la norma ISO/IEC 27001 y su incidencia en los procesos de seguridad de la información.

3.3 Nivel o tipo de investigación.

Investigación Experimental.

La investigación se ha desarrollado de forma experimental porque se aplica la gestión de la seguridad de la información por medio del Sistema de Gestión de Seguridad de la Información implementado en diferentes procesos de análisis de datos utilizando la norma ISO-IEC 27001 para observar resultados y determinar condiciones actuales de la gestión de la seguridad de los sistemas de información.

Investigación Descriptiva

La investigación es descriptiva para dar a conocer con profundidad el problema, estableciendo sus causas y consecuencias, así como las dificultades por lo que está atravesando.

Explicativa

La investigación es explicativa porque se puede sustentar la importancia que tiene la Gestión de Seguridad de la Información en la gerencia de procesos de seguridad de la información aplicando la norma ISO/IEC 27001.

3.4 Población y muestra

La presente investigación trabajará con la población t, que se limita al personal de los departamentos de Tecnologías de la Información y Comunicación de las Instituciones de Educación Superior de la ciudad de Machala, Universidad Técnica de Machala e Instituto Tecnológico Superior El Oro, ya que el valor de la población es menos de 100 no se requiere ejecutar un muestreo.

Tabla 1. Población

Población	Número	Porcentaje
Director de Tics	2	8,00%
Jefe de Sistemas	2	8,00%
Departamento de Base de Datos	3	12,00%
Departamento de Desarrollo y Aplicaciones	7	28,00%
Departamento de Redes y Mantenimiento	11	44,00%
Total	25	100,00%

Elaborado por: Investigador

3.5 Operacionalización de variables.

3.5.1 Variable Independiente.

Tabla 2. Operacionalización de la Variable Independiente: Gestión de Seguridad de Información basada en Norma ISO 27001.

Conceptualización	Dimensiones	Indicadores	Ítems Básicos	Técnicas e Instrumentos
Los Gestión de Seguridad de Información es la secuencia de acciones correspondientes a planificar, Implementar, Medir y Mejorar con el objetivo de preservar la confidencialidad, integridad y disponibilidad de la información.	- Alcance de la Gestión de Seguridad de la Información (Numero de procesos que se llevara). - Relaciones de Control que se va a implementar - Grado de Fortaleza de cada uno de los controles. - Grado de Intensidad (Profundidad) con que se va a aplicar.	- Acceso a datos - Datos confiables - Herramientas utilizadas - Tiempos empleados - Información Requerida - Decisiones en base a información obtenida	¿Existen políticas, controles o normas que garanticen la gestión de la seguridad de la información en las Instituciones de Educación Superior? ¿Se aplican políticas de gestión de seguridad de la información en el procesamiento de información de las Instituciones de Educación Superior? ¿El personal tienen conocimiento sobre los Sistema de Gestión de seguridad de la información (SGSI)? ¿Considera necesario que se implemente una normativa de Gestión de Seguridad de la información? ¿Existe alguna política, controles o restricciones de seguridad para evitar el acceso a sitios no autorizados, uso de navegadores y correo electrónico en internet? -	- Encuestas. - Cuestionario.

Elaborado por: Investigador

3.5.2 Variable Dependiente.

Tabla 3. Operacionalización de Variable Independiente: Información de las IES.

Conceptualización o Descripción	Dimensiones	Indicadores	Ítems Básicos	Técnicas e Instrumentos
Información de las Instituciones de Educación Superior, es aquélla información relativa a las operaciones realizadas por una departamento o entidad; su finalidad fundamental es servir de apoyo en los diferentes procesos de decisión y en la determinación de objetivos, ejecución, control y evaluación de resultados de los programas institucionales.	- Conocer los riegos a los que se encuentra la información de los departamentos de tecnologías de la Información y Comunicación de las instituciones. - Generan información diariamente. - Acciones por realizar. - Los recursos limitados que se manejan	- Riesgo de ataques informáticos - Medidas de control para prevenir ataques - Disponibilidad de los recursos con que se cuenta	¿Firmó usted un certificado de confidencialidad y buen uso de las claves de acceso a diferentes sistemas de gestión de procesos de la información? ¿La información que usted gestiona para el desempeño de sus actividades se respalda frecuentemente? ¿Se aplican en la institución mantenimientos preventivos periódicos a los equipos de cómputo establecidos para la ejecución de sus actividades? ¿Ha constatado que el personal al no utilizar un SGSI que ayuda a la gestión de seguridad de la información ha originado una mala toma de decisiones? ¿Considera necesario contar un SGSI para la gestión de la seguridad de la información?	- Encuesta - Cuestionario

Elaborado por: Investigador

3.6 Plan de recolección de información.

La técnica a emplearse es la encuesta dirigida, utilizando como instrumento el cuestionario a través de preguntas cerradas, lo que ayuda significativamente a la obtención más concreta de la información a obtener.

Tabla 4. Recolección de la información.

Preguntas	Explicación
¿Para qué?	Para alcanzar los objetivos de la investigación
¿De qué personas u objetos?	Director de Tics Jefe de Sistemas Responsables del Departamento de Base de Datos Responsables del Departamento de Desarrollo. Responsables del Departamento de Redes y Mantenimiento.
¿Sobre qué aspectos?	Gestión de seguridad de la información.
¿Quién, Quiénes?	Investigador: Ing. Wilson Enrique Cuenca León
¿Cuándo?	Primer Semestre del 2019
¿Dónde?	Departamentos de Tics de la Universidad Técnica de Machala y del Instituto Tecnológico Superior El Oro.
¿Cuántas veces?	Una.
¿Qué técnicas de recolección?	Encuesta. Entrevista. Datos Estadísticos.
¿Con qué?	Cuestionario. Entrevistas. Inspecciones.
¿En qué situación?	Dentro del horario de trabajo con profesionalismo investigativo y absoluta confidencialidad y reserva.

Elaborado por: Investigador

3.7 Procesamiento y Análisis.

Para procesar la información recolectada, se siguieron los pasos a continuación descritos:

- Revisión juiciosa de la información reunida .
- Tabulación o cuadros variables de la hipótesis y objetivos:
  - Manejo de información (reajuste de cuadros con casillas vacías o con datos tan reducidos cuantitativamente que no influyen significativamente en los análisis).
  - Estudio estadístico de datos para presentación de resultados.

3.8 Análisis de Resultados.

- Análisis de resultados estadísticos, tomando en cuenta primero acuerdos con los propósitos y su respectiva hipótesis.
- Interpretación de los resultados sustentado en el marco teórico.
- Verificación oportuna de la hipótesis para su respectiva revisión estadística.
- Establecimiento de conclusiones y recomendaciones.

CAPÍTULO IV

4. ANÁLISIS E INTERPRETACION DE RESULTADOS.

4.1 Análisis e Interpretación de Resultados.

Los resultados que se visualizan a continuación están basados en una encuesta realizada a Directores de Tics, Jefes de sistemas, Responsables de la gestión de base de datos, desarrollo, redes y mantenimiento de los Departamentos de Tecnologías de la Información y Comunicación(Tics) de las Instituciones de Educación Superior(IES) de la ciudad de Machala. La encuesta consta de 10 preguntas y fue aplicada a 25 personas con funciones administrativas y operativas. (Ver Anexo 1),

1. ¿Existen políticas, controles o normas que garanticen la gestión de la seguridad de la información en las Instituciones de Educación Superior?

Tabla 5. Existencia de Políticas de Seguridad de la Información.

Alternativa	Frecuencia	Porcentaje
SI	4	16%
NO	21	84%
Total	25	100%

Fuente: Encuesta.

Elaborado por: Investigador

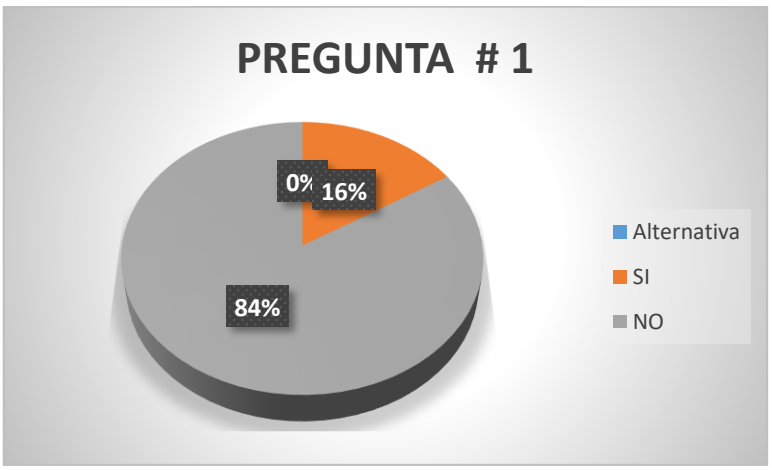


Figura 6. Existencia de políticas que garanticen la gestión de la información.

Elaborado por: Investigador.

Análisis: El 84% de los encuestados indican que no existen políticas que garanticen la gestión de seguridad de la información, mientras que el 16% indica que se gestiona según la necesidad o requerimientos que existan por parte de los usuarios o las autoridades de las instituciones de educación superior.

Interpretación: En los departamentos de Tics de las IES no existe una gestión de seguridad de la información cuando se verifican alteraciones en el tratamiento y procesamiento de los datos.

2. ¿Se aplican políticas de gestión de seguridad de la información en el procesamiento de información de las Instituciones de Educación Superior?

Tabla 6. Políticas de Gestión de Seguridad en Procesamiento de Datos.

Alternativa	Frecuencia	Porcentaje
SI	0	0%
NO	25	100%
Total	25	100%

Fuente: Encuesta.

Elaborado por: Investigador

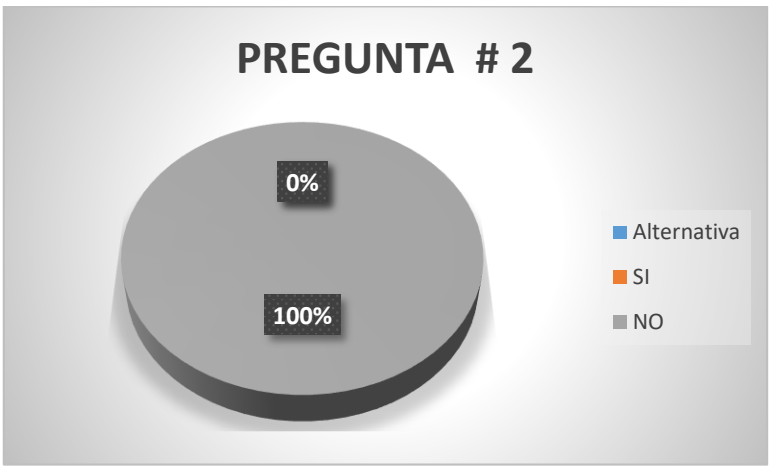


Figura 7. Políticas de Gestión de Seguridad en Procesamiento de Datos.

Elaborado por: Investigador.

Análisis: El 100% de los encuestados, menciona que no se aplican políticas de gestión de seguridad de la información en el manejo y procesamiento de los datos.

Interpretación: En los departamentos de Tics de las IES no se aplica políticas de gestión de seguridad de la información cuando se detectan anomalías en el procesamiento de la información.

3. ¿El personal tienen conocimiento sobre los Sistema de Gestión de seguridad de la información (SGSI)?

Tabla 7. Conocimiento de Sistema de Gestión de Seguridad de Información.

Alternativa	Frecuencia	Porcentaje
SI	2	8%
NO	23	92%
Total	25	100%

Fuente: Encuesta.

Elaborado por: Investigador

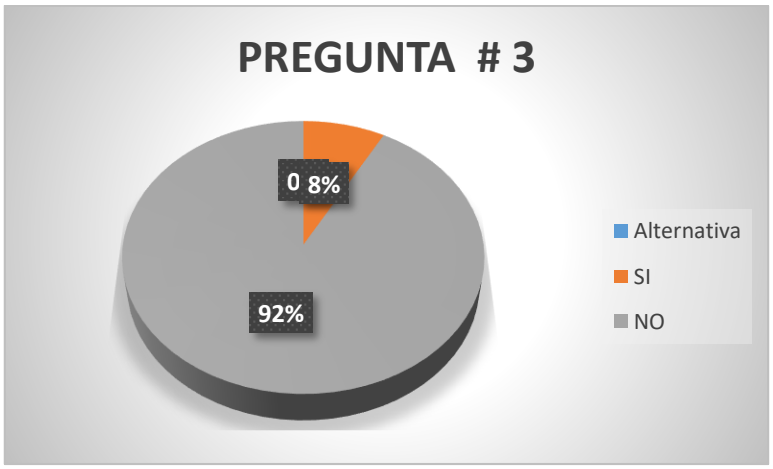


Figura 8. Conocimiento de Sistema de Gestión de Seguridad de Información.

Elaborado por: Investigador.

Análisis: En la encuesta realizada el 92% mencionaron que no tienen conocimiento sobre un sistema de gestión de seguridad de la información, al mismo tiempo el 8% respondió que tienen algún conocimiento mínimo de lo que es un SGSI.

Interpretación: Los departamentos de Tics de las IES no cuenta con un SGSI y el conocimiento de estos sistemas es reducido en cuanto a aplicación de controles, normas y reglas para la gestión de seguridad de la información.

4. ¿Considera necesario que se implemente una normativa de Gestión de Seguridad de la información?

Tabla 8. Necesidad de Implementación de SGSI en la institución.

Alternativa	Frecuencia	Porcentaje
SI	25	100%
NO	0	0%
Total	25	100%

Fuente: Encuesta.

Elaborado por: Investigador

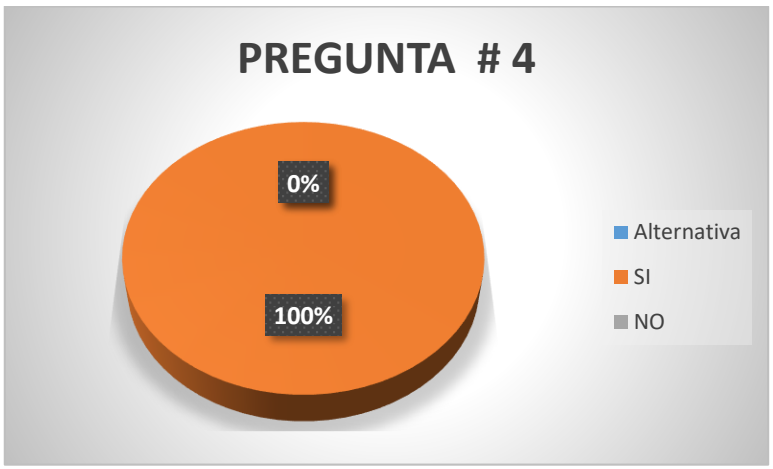


Figura 9. Necesidad de Desarrollo e Implementación de SGSI en institución.

Elaborado por: Investigador.

Análisis: El 100% de los encuestados respondieron que si necesitan la implementación de un SGSI que permita tener una mejor gestión de la seguridad de la información y optimizar los tiempos y requerimientos.

Interpretación: Dentro de los departamentos de Tics de las IES no se aplican políticas de gestión de seguridad de la información como debería ser el caso, o si se aplican, estos controles son mínimos y los riesgos son altos, ya que no se cuenta con la implementación de un SGSI.

5. **¿Existe alguna política, controles o restricciones de seguridad para evitar el acceso a sitios no autorizados, uso de navegadores y correo electrónico en internet?**

Tabla 9. Políticas de uso de navegadores y correos electrónico.

Alternativa	Frecuencia	Porcentaje
SI	1	4%
NO	24	96%
Total	25	100%

Fuente: Encuesta.

Elaborado por: Investigador

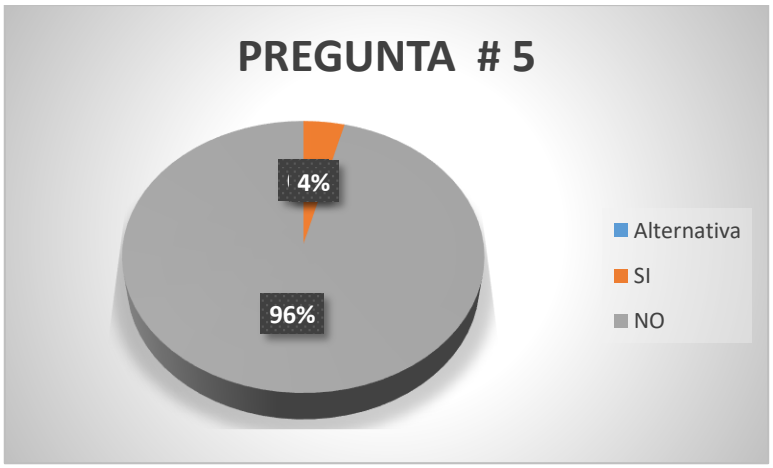


Figura 10. Políticas de uso de navegadores y correos electrónico.

Elaborado por: Investigador.

Análisis: El 96% de los encuestados menciona que no existen políticas del uso de navegadores y gestión del correo electrónico, mientras que el 4% indica que si hay estos controles o políticas en las instituciones.

Interpretación: En los departamentos de Tic de las IES no se aplican adecuadas políticas de restricción para el uso de software entre los cuales se destaca los navegadores y gestión del correo electrónico.

6. ¿Firmó usted un certificado de confidencialidad y buen uso de las claves de acceso a diferentes sistemas de gestión de procesos de la información?

Tabla 10. Certificado de confiabilidad y uso de claves de accesos.

Alternativa	Frecuencia	Porcentaje
SI	2	8%
NO	23	92%
Total	25	100%

Fuente: Encuesta.

Elaborado por: Investigador

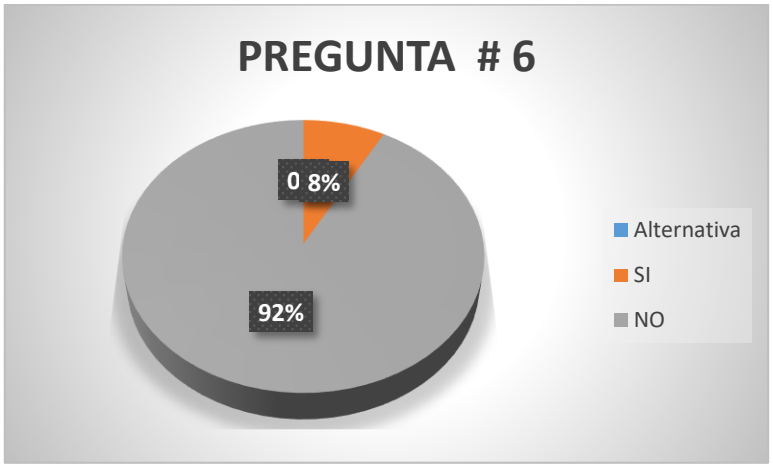


Figura 11. Certificado de confiabilidad y uso de claves de accesos.

Elaborado por: Investigador.

Análisis: El 92% de los encuestados menciona que no han firmado un documento o certificado de confiabilidad aplicado al procesamiento de datos, así como también a la administración del uso de claves de accesos, mientras que el 8% indica que si firmo algún documento que sirva para proteger la integridad de los datos.

Interpretación: En los departamentos de Tics de las IES no cuenta con políticas de gestión del aseguramiento de la información que permita tener un documento físico de confiablidad para el uso correcto de claves y manejo adecuado de la información.

7. ¿La información que usted gestiona para el desempeño de sus actividades se respalda?

Tabla 11. Respaldo de información gestionada en la institución.

Alternativa	Frecuencia	Porcentaje
Siempre	2	8%
Con frecuencia	2	8%
A veces	2	8%
Rara vez	4	16%
Nunca	15	60%
TOTAL	25	100%

Fuente: Encuesta.

Elaborado por: Investigador

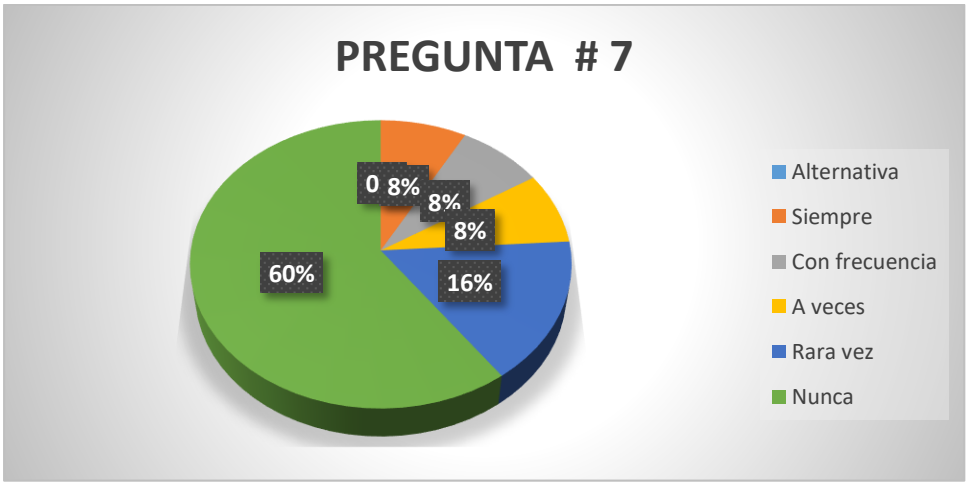


Figura 12. Respaldo de información gestionada en la institución.

Elaborado por: Investigador.

Análisis: En base a la encuesta realizada el 60% de los encuestados mencionaron que nunca se respaldan los datos, mientras que el 16% afirmo que rara vez se lo hace y finalmente el 8% menciono que a veces, con frecuencia y siempre se realizan respaldos.

Interpretación: En los departamentos de Tics de las IES no existe la cultura técnica de respaldos de datos e información para prevenir pérdidas, alteraciones, robos o caídas de datos.

8. ¿Se aplican en la institución mantenimientos preventivos periódicos a los equipos de cómputo establecidos para la ejecución de sus actividades?

Tabla 12. Mantenimiento preventivo en equipos informáticos de la institución.

Alternativa	Frecuencia	Porcentaje
Siempre	2	8%
Con frecuencia	2	8%
A veces	5	20%
Rara vez	5	20%
Nunca	11	44%
TOTAL	25	100%

Fuente: Encuesta.

Elaborado por: Investigador

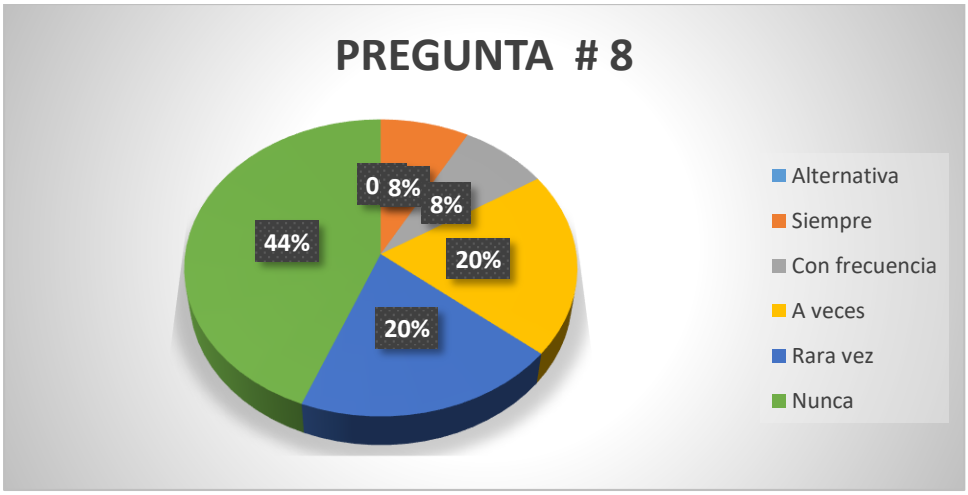


Figura 13. Mantenimiento preventivo en equipos informáticos de la institución.

Elaborado por: Investigador.

Análisis: El 44% de los encuestados menciona que nunca se ejecutan mantenimientos preventivos a sus equipos, solo si se llega a ocurrir un imprevisto o fallas lo realizan, mientras que el 20% indica que, si se realizan los chequeos y mantenimientos de los equipos informáticos rara vez o a veces, finalmente el 8% menciono que frecuente y siempre se realiza estas actividades.

Interpretación: En los departamentos de Tics de las IES no se aplican políticas de gestión de mantenimientos preventivos y correctivos, no existe una organización para controlar el tiempo de trabajo de los equipos informáticos, no hay bitácora de control de actividades, cambios y reparaciones que han tenido los computadores.

9. ¿Ha constatado que el personal al no utilizar un SGSI que ayuda a la gestión de seguridad de la información ha originado una mala toma de decisiones?

Tabla 13. Mala toma de decisiones por no contar con SGSI.

Alternativa	Frecuencia	Porcentaje
SI	25	100%
NO	0	0%
Total	25	100%

Fuente: Encuesta.

Elaborado por: Investigador

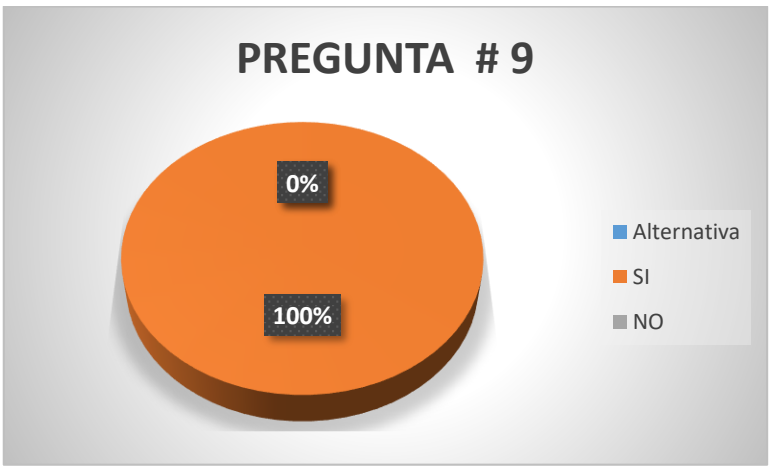


Figura 14. Mala toma de decisiones por no contar con SGSI.

Elaborado por: Investigador.

Análisis: El resultado de la encuesta nos muestra que el 100% de los funcionarios menciona que no contar con un SGSI ha permitido que se tomen malas decisiones, además que se acumulen problemas que se venían generando con anterioridad y otros inconvenientes de gestión de información.

Interpretación: En los departamentos de Tics de las IES no aplican políticas de gestión de seguridad de la información, que repercute en los servicios que prestan, ya que existen riesgos y vulnerabilidades por parte de equipos informáticos por no contar con software adecuado, antivirus actualizados y seguridades contra ataques externos.

10. ¿Considera necesario contar un SGSI para la gestión de la seguridad de la información de las Instituciones de Educación Superior?

Tabla 14. SGSI impacta positivamente en la calidad de la gestión.

Alternativa	Frecuencia	Porcentaje
SI	25	100%
NO	0	0%
Total	25	100%

Fuente: Encuesta.

Elaborado por: Investigador

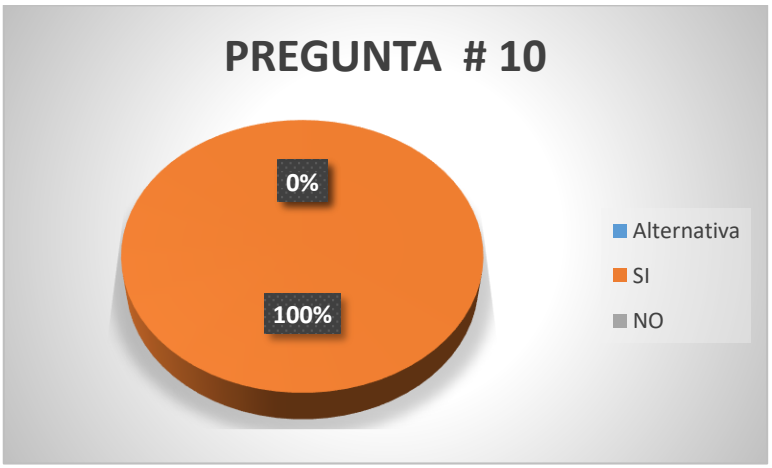


Figura 15. SGSI impacta positivamente en la calidad de los servicios.

Elaborado por: Investigador.

Análisis: El 100% de los encuestados menciona que es necesario contar con un SGSI para la gestión de la seguridad de la información, que incluya políticas de permisos, procesamientos de datos, mantenimientos de equipos, entrenamientos y capacitación al personal que labora en los departamentos de Tics de las IES.

Interpretación: La implementación de un SGSI en los departamentos de Tics de las IES impactará positivamente, ya que, gracias a este sistema, se reflejará una óptima gestión de la seguridad de la información, además de los servicios prestados.

4.2 Verificación de la Hipótesis.

En base a los resultados obtenidos en las encuestas realizadas a los funcionarios que laboran en los departamentos de Tics de las instituciones de educación superior, la Gestión de Seguridad de Información basado en Normas ISO/IEC 27001 facilitara una excelente relación entre la toma de decisiones de las altas autoridades y del personal que gestiona la seguridad de la información en los departamentos de Tics.

Para determinar si la propuesta es factible teniendo en cuenta que la muestra o población es reducida se ha aplicado el método Estadístico Chi-cuadrado, donde eligieron las preguntas 1 y 2 de la encuesta aplicada a los funcionarios, ya que los resultados obtenidos se orientan al requerimiento de la investigación, porque permite corroborar que no se cuenta con estándares, normativas, políticas y controles para la gestión de la seguridad de la información;

Esto a su vez permite medir y establecer el efecto positivo de la solución propuesta en los departamentos de Tics para ofrecer una mejor calidad de gestión de seguridad de la información.

Pregunta 1. ¿Existen políticas, controles o normas que garanticen la gestión de la seguridad de la información en las Instituciones de Educación Superior?

Tabla 15. Verificación de la hipótesis Pregunta 1.

Alternativa	Frecuencia	Porcentaje
SI	4	16%
NO	21	84%
Total	25	100%

Fuente: Encuesta.

Elaborado por: Investigador

Pregunta 2. ¿Se aplican políticas de gestión de seguridad de la información en el procesamiento de información de las Instituciones de Educación Superior?

Tabla 16. Verificación de la hipótesis Pregunta 2.

Alternativa	Frecuencia	Porcentaje
SI	0	0%
NO	25	100%
Total	25	100%

Fuente: Encuesta.

Elaborado por: Investigador

4.2.1 Planteamiento de la hipótesis

La Gestión de Seguridad de Información basada en la Norma ISO/IEC 27001incide en la información de las Instituciones de Educación Superior de la ciudad de Machala.

Modelo lógico

H_0: La Gestión de Seguridad de la Información basado en norma ISO/IEC 27001 NO incide en la información en las Instituciones de Educación Superior.

H_1: La Gestión de Seguridad de la Información basado en norma ISO/IEC 27001 SI incide en la información en las Instituciones de Educación Superior de la ciudad de Machala.

Modelo matemático

H_0: Observado (O) = Esperado (E)

H_1: Observado (O) ≠ Esperado (E)

Modelo estadístico

Los resultados obtenidos a través de las encuestas ejecutadas al personal de los Departamentos de Tecnologías de la Información y Comunicación de las Instituciones de Educación Superior de la ciudad de Machala, Universidad Técnica de Machala e Instituto Tecnológico Superior El Oro, se procedió a verificar la hipótesis planteada mediante el uso de la prueba no paramétrica de Chi Cuadrado, la misma que ayudó a obtener resultados que determinan si existe o no relación entre las variables por medio la siguiente formula.

$$X^2 = \sum_{i=1}^{n} \frac{(fo - fE)^2}{fE}$$

En donde:

X^2 = Chi Cuadrado.

$\sum_{i=1}^{n}$ = Sumatoria

f o = Frecuencias Observadas.

f E = Frecuencias Esperadas.

Nivel de Significancia (α)

Realizada la prueba respectiva, se estableció un rango de significancia de 0,01 que da un rango de fiabilidad del 99%.

4.2.2 Cálculo del Chi-Cuadrado X^2.

Tabla 17. Cálculo del Chi-Cuadrado.

Alternativas / Preguntas	SI	NO	Total
¿Existen políticas, controles o normas que garanticen la gestión de la segurida de la información en las IES.	4	21	25
¿Se aplican políticas de gestión de seguridad de la información en el procesamiento de información de las IES	0	25	25
TOTAL	4	46	50

Fuente: Encuesta.

Elaborado por: Investigador

Tabla 18. Cálculo del Chi-Cuadrado

Frecuencias Observadas (f o)	Frecuencias Esperadas (f E)	$(f o - f E)^2$	$(f o - f E)^2 / E$
4,00	2,00	4,00	2,00
21,00	23,00	4,00	0,17
0,00	2,00	4,00	2,00
25,00	23,00	4,00	0,17
SUMATORIA			4,35

Fuente: Encuesta.

Elaborado por: Investigador

Resultado: $X^2 = 4,35$.

4.2.3 Nivel de Significancia (α)

En la investigación se escogió un nivel de significancia del 5%, donde α = 0,05 por lo tanto el nivel de confianza que nos da es del 95%.

4.2.4 Grado de Libertad.

Para calcular la zona de aceptación o rechazo, se requiere calcular los grados de libertad y para la para la obtención de este valor, aplicaremos la siguiente formula.

gl = (c - 1) (f - 1)

donde:

c = columnas de la tabla.

f = filas de la tabla

gl = (2 -1) (2 -1)

gl = (1) (1)

gl = 1

4.2.5 Grado de Significancia.

α = 0,05

X^2 t = 3,84

Tabla de Distribución del CHI CUADRADO.

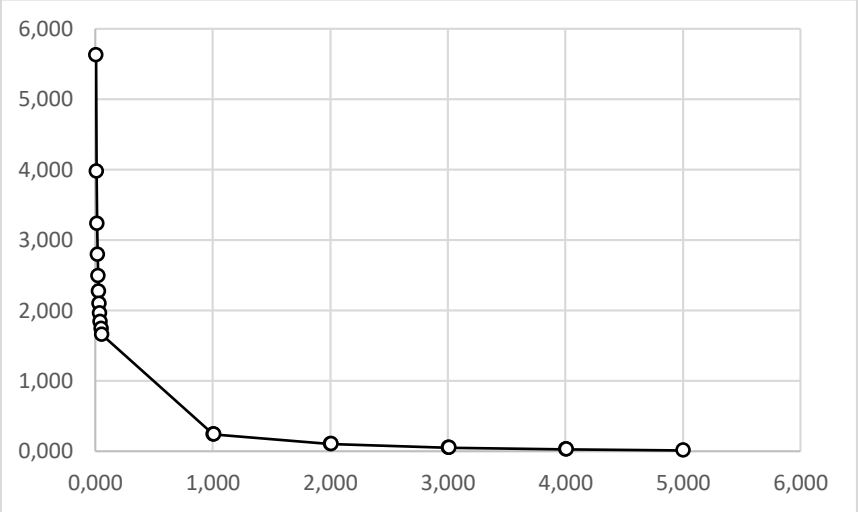
Tabla 19. Chi Cuadrado.

ν	0,005	0,01	0,025	0,05	0,95	0,975	0,99	0,995
1	0,00003935	0,000157	0,000982	0,00393	3,841	5,024	6,635	7,879
2	0,010	0,020	0,051	0,103	5,991	7,378	9,210	10,597
3	0,072	0,115	0,216	0,352	7,815	9,348	11,345	12,838
4	0,207	0,297	0,484	0,711	9,488	11,143	13,277	14,860
5	0,412	0,554	0,831	1,145	11,070	12,832	15,086	16,750

Elaborado por: Investigador

Grafica Del Cálculo Del Chi Cuadrado

Tabla 20. Calculo del Chi Cuadrado.



Elaborado por: Investigador

4.2.5 Decisión.

X^2c = 4,35 Valor obtenido del cálculo del Chi-cuadrado.
X^2t = 3.84 Valor obtenido de la tabla de distribución del Chi – Cuadrado.

Conclusión:

Como $X^2c = 4,35 > X^2t = 3.84$, el valor que se obtuvo y calculó es mayor al valor de la distribución, por ende, tomamos como aceptada la hipótesis de investigación, la cual es: Gestión de Seguridad de Información basado en Norma ISO/IEC 27001 SI incide en la información de las instituciones de educación superior de la ciudad de Machala. Corroborando que existe una relación de dependencia entre las variables de la Gestión de la Información basada en la Norma ISO/IEC 27001 y la información de las Instituciones de Educación Superior de la ciudad de Machala.

CAPITULO V

5. CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- La investigación demostró que las Instituciones de Educación Superior de la ciudad de Machala cuentan con activos tanto físicos como activos de información en sus departamentos de Tecnologías de la Información y Comunicación, pero a estos activos no se le presta la atención requerida en cuanto a tener implementados controles, políticas o normas que permitan se adecuada gestión de seguridad de la información.

- En la investigación realizada se evidenció un gran problema en las Instituciones de Educación Superior, porque en sus Departamentos de Tecnologías de la Información y Comunicación no cuentan con políticas o controles de seguridad, esto ocasiona que los funcionarios en un 60% desconozcan de normas para gestionar correctamente la información que manejan.

- En los Departamentos de Tecnologías de la Información y Comunicación de las Instituciones se detectó graves inconvenientes porque no disponen de una norma de seguridad establecida, esto impacta en los funcionarios en un 65% porque no tienen conocimientos y la capacitación adecuada sobre temas de gestión de la seguridad de la información.

- La falta de capacitación por parte de las Instituciones de Educación Superior de la ciudad de Machala permite que el 75% de sus funcionarios de los departamentos de tecnologías de las información y comunicación ejecuten acciones que amenazan la gestión de la seguridad de la información a través de intercambios de contraseñas para acceder a los sistemas y aplicaciones restringidas, instalación de programas piratas y acciones personales como la navegación en sitios prohibidos.

5.2 Recomendaciones.

- El Personal de los Departamentos de Tecnologías de Información y Comunicación de las Instituciones de Educación Superior deben establecer políticas, controles y estrategias que ayuden a mejorar la gestión de seguridad de la información para garantizar su confidencialidad, integridad y disponibilidad y a su vez tener un impacto positivo en la toma de decisiones de las instituciones.

- El Personal de los Departamentos de Tecnologías de Información y Comunicación de las Instituciones de Educación Superior deben implementar normas y controles que permiten evidenciar una mejor calidad de servicios, procesos y actividades que el personal de tecnología ejecuta en cuanto a mantenimientos de equipos, gestión de redes, desarrollo y auditorías informáticas.

- El Personal de los Departamentos de Tecnologías de Información y Comunicación de las Instituciones de Educación Superior deben generar documentos y formatos que permitan tener un mejor control de las actividades que ejecutan en cuanto a mantenimientos, reparaciones, actualizaciones de equipos informáticos y la gestión de redes.

- Revisar periódicamente el desempeño de las nomas y controles implementados, donde la alta dirección junto con los responsables de los departamentos de Tics determinará si se ha cumplido con el objetivo de la gestión de la seguridad de la información, a más de aportar ideas para mejorar las normas y controles implementados.

CAPITULO VI

6. PROPUESTA.

6.1 Datos Informativos.

Tema : Implementación de Sistema de Gestión de Seguridad de la Información basado en la Norma ISO/IEC 27001 para la gestión de la seguridad de la información de las Instituciones de Educación Superior de la ciudad de Machala.

Institución : Universidad Técnica de Machala.

Provincia : El Oro

Cantón : Machala

Dirección : Avenida Loja y calle 10 de agosto.

Beneficiarios: Rector, Decanos, Coordinadores, Director de Tics, Jefes de Sistemas, Personal administrativo y Comunidad estudiantil

Responsable: Ing. Wilson Enrique Cuenca León.

Director : Ing. Klever Renato Urvina Barrionuevo, Mg.

6.2 Antecedentes de la Propuesta.

Actualmente la información es el activo principal de toda institución de educación superior y esta debe ser confidencial, integra y disponible, libre de alteraciones o cambios que afecten el normal desenvolvimiento de los procesos de sistemas de información.

La Universidad Técnica de Machala cuenta con el Departamento de Tecnologías de la Información y Comunicación, que es el encargado de la gestión de la seguridad de la información, además de procesar, administrar y desarrollar diferentes sistemas de aplicación de información y comunicación.

El Departamento de Tecnologías de la Información y Comunicación no cuenta con la implementación de normas o estándares para la gestión de la seguridad de la información, así como también la fiabilidad de los servicios informáticos, ya que la organización posee información fundamental que maneja en sus procesos tanto administrativos como académicos y si estos se ven afectados y expuestos a ataques externos de hackers, perdida de información, alteración o modificación de los datos, ocasionará el retraso tanto en tiempo como en dinero para las dos instituciones.

6.3 Justificación.

En base al análisis ejecutado en el proceso de recolección de datos en las encuestas, los antecedentes y con los objetivos de asegurar una adecuada gestión de la seguridad de la información y la calidad de los servicios informáticos del departamento de Tecnologías de la Información y Comunicación de la Universidad Técnica de Machala, ya que no cuenta con metodologías contra ataques externos, es indispensable realizar una Gestión de Seguridad de la Información basada en la norma ISO/IEC 27001, para determinar la incidencia de la información de la institución.

El autor de la presente investigación implementa un sistema de gestión de seguridad de la información, que basado en un conjunto de sistemas cumplen con los estándares indicados en la norma ISO/IEC 27001 bajo una estrategia de mejora continua de procesos de gestión de seguridad de la información de instituciones de educación superior. Adicionalmente la propuesta es factible realizarla porque cuenta con el apoyo de las autoridades, departamento de tecnologías de las información y comunicación y personal de la entidad para la obtención de la información.

6.4 Objetivos.

6.4.1 Objetivo General.

Implementar un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001 para la gestión de seguridad de información en el departamento de Tecnologías de Información y Comunicación de la Universidad Técnica de Machala.

6.4.2 Objetivos Específicos.

- Establecer el modelo PDCA de mejora continua para determinar los parámetros y lineamientos para la implementación del Sistema de Gestión de Seguridad de la Información en el departamento de Tics de la Universidad Técnica de Machala.

- Establecer la metodología del Ciclo Deming para definir la planificación, implementación, revisión, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información.

- Establecer un plan de políticas y procedimientos para gestionar, evaluar y analizar la seguridad de la información en cumplimiento con los objetivos de control de la norma ISO27001:2013.

- Implementar el Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001 en el Departamento de Tecnologías de la Información y Comunicación de la Universidad Técnica de Machala.

6.5 Análisis de Factibilidad.

6.5.1 Factibilidad Técnica.

La propuesta de este proyecto técnicamente es factible de desarrollar, porque cuenta con los medios tecnológicos requeridos, es decir, cuenta con el apoyo de la infraestructura informática, herramientas tecnológicas, acceso a usuarios, datos e información requerida por parte del departamento de tecnología de la información y comunicación de la Universidad Técnica de Machala.

Para llevar a cabo la implementación del Sistema de Gestión de Seguridad de la Información basado en la norma de seguridad informática ISO 27001 en el departamento de tecnología de la información y comunicación de la Universidad Técnica de Machala se dispone con la documentación a continuación:

- ISO/IEC 27001
- ISO/IEC 27001-norma-e-implemenntacion-SGSI
- ISO/IEC 27002

6.5.2 Factibilidad Operativa.

El proyecto operativamente es factible porque tiene el apoyo de la Universidad Técnica de Machala, lo que permite tener disponibilidad requerida con el personal de la institución para facilitar la información necesaria y garantizar los resultados de la presente investigación.

Para el cumplimiento de los objetivos, se implementará el Sistema de Gestión de Seguridad de la Información. bajo la norma de seguridad informática ISO/IEC 27001 con el apoyo del rector y del personal del departamento de tecnología de la información y comunicación de la Universidad Técnica de Machala. Se desarrollará un documento detallando los procedimientos que se llevaran a cabo para la realización de una metodología que asegure el cumplimiento de la norma de seguridad informática ISO/IEC 27001:2013.

6.5.3 Factibilidad Organizacional.

El presente proyecto es organizacionalmente factible, porque el rector y jefe de sistemas del departamento tecnologías de la información de la institución tienen el interés por disponer y tener a la mano medidas para mejorar la gestión de la seguridad de la información.

6.5.4 Factibilidad Económica.

El presente proyecto es económicamente factible de realizar porque se va a implementar con relación al contenido descrito en la norma, escogiendo las fases del estándar ISO/IEC 27001, además los costos que conllevan el estudio, análisis, tiempo empleado en desarrollar este proyecto serán asumidos por el investigador, mientras que las dos instituciones asumen los tiempos de su personal involucrados en el desarrollo de la presente propuesta.

6.6 Fundamentación.

La finalidad fundamental que tienen los sistemas de gestión seguridad de la información es mejorar la gestión de la seguridad de la información que está expuesta a todo tipo de riesgo, amenazada y vulnerabilidad existentes en la actual tecnología, y que gracias a este tipo de sistemas se puede combatir estos factores que atentan contra la información, ya que este sistema permite hacer realizar un análisis detallado de cómo hacer frente a estos ataques gracias su metodología, documentación y otras herramientas que ayuda a prevenir, mitigar y en el mayor de la casos a eliminar una amenaza en particular (iso27000.es, 2012).

Toda información permite la aplicación de procesos y sistemas para tratamiento, actualmente la información es el activo primordial de toda organización, por esta causa, su confidencialidad, integridad y disponibilidad será un factor determinante al momento de lograr los objetos y metas propuestas en cualquier organización, si se gestiona de manera adecuada se logra el éxito de la organización, si no se ha llevado a cabo la gestión de la información de forma adecuada con herramientas y mecanismos para salvaguardar los datos, se tendrá al final un resultado no deseado (iso27000.es, 2012).

6.7 Propuesta de Implementación de Sistema de Gestión de Seguridad de la Información.

6.7.1 Metodología.

Para la gestión de la seguridad de la información de la Universidad Técnica de Machala se planteó la metodología basada en el ciclo de mejora continua PDCA (Planear, Hacer, Verificar, Actuar) de la norma ISO/IEC 27001 que facilita la implementación de un Sistema de Gestión de Seguridad de la Información, el mismo que permite saber cómo incide la aplicación de este sistema en la gestión de la seguridad de la información de las instituciones de educación superior.

Esta metodología su sustenta en cuatro fases cíclicas:

Fase 1: Planear (Establecer el SGSI)

Fase 2: Hacer (Implementar y aplicar el SGSI)

Fase 3: Revisar (Monitorear y Chequear el SGSI)

Fase 4: Actuar (Mantener y Mejorar el SGSI)

Estas cuatro fases se pueden visualizar en la figura 16.

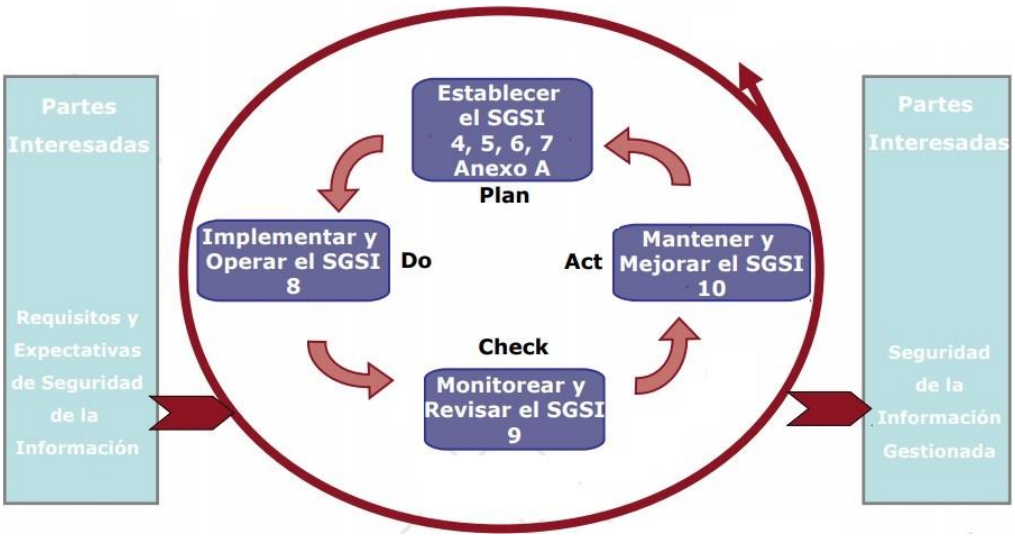


Figura 16. Fases del Ciclo PDCA.

Elaborado por: Investigador.

La tabla a continuación (Ver Tabla 2) enlaza cada una de cuatro fases y sus respectivas actividades para la aplicación de la metodología propuesta:

Tabla 21. Fases y Actividades del Ciclo PDCA.

Fase	Ciclo PDCA	Actividad (Etapas)
1	PLANEAR. (Establecer)	a) Definir alcance del SGSI. b) Definir política de seguridad. c) Metodología para la evaluación y control de riesgos. d) Identificar los riesgos (Inventario y Tasación de Activos) e) Analizar y evaluar los riesgos f) Identificar y evaluar opciones del tratamiento de riesgos. g) Seleccionar controles para el tratamiento del riesgo. h) Declaración de Aplicabilidad
2	HACER. (Implementar y operar el SGSI)	a) Definir plan de tratamiento de riesgos b) Implantar el plan de tratamiento de riesgos. c) Implementar los controles. d) Definir un sistema de métricas e) Formar y concientizar. f) Gestionar recursos del SGSI. g) Implantar procedimientos y controles.
3	VERIFICAR. (Monitorizar y revisar el SGSI)	a) Monitorear y Revisar el SGSI b) Revisar y medir la efectividad de los controles del SGSI (métricas del SGSI) c) Revisar los riesgos residuales d) Realizar auditorías internas del SGSI e) Revisar el SGSI por parte de la dirección
4	ACTUAR. (Mantener y mejorar el SGSI)	a) Implementar mejoras al SGSI. b) Realizar acciones preventivas y correctivas. c) Evaluar sugerencias y definir la implementación de mejoras. d) Comunicar acciones y mejoras del SGSI. e) Asegurar alcanzar los objetivos previstos.

Elaborado por: Investigador

Se detallan las fases que componen el ciclo de mejora continua PDCA con sus respectivas etapas y actividades a ejecutarse para la gestión de la seguridad de la información, la misma que servirá como un modelo base de seguridad, para gestionar y mejorar la seguridad de la información de las instituciones de educación superior.

Fase 1: Planear (Establecer el SGSI ISO/IEC 27001).

Esta fase contempla las siguientes etapas o actividades:

Tabla 22. Etapas del Ciclo Planear

Fase	Ciclo	Etapa	Actividad
1	Planear (Establecer el SGSI)	A	Alcance
		B	Políticas
		C	Metodología de evaluación de riesgos
		D	Identificar los riesgos (Aplicación de la metodología de evaluación de riesgos)
		E	Analizar y Evaluar los Riesgos
		F	Identificar y evaluar opciones del tratamiento de riesgo.
		G	Seleccionar controles para el tratamiento del riesgo.
		H	Declaración de Aplicabilidad

Elaborado por: Autor.

a) Alcance del SGSI.

La finalidad de esta etapa es definir el alcance del SGSI, mostrar el entorno organizacional, evaluar la situación actual de la seguridad de información por medio del personal e identificar las expectativas a través de las partes interesadas (máximas autoridades, profesionales del área de TICS y en general todos quienes laboran en una organización), además de incluir pormenores de la justificación a su alcance.

Además, este alcance se implanta en función de la organización y en función de su localización, que puede englobar un proceso, un conjunto de procesos, un servicio o un conjunto de servicios y oportunamente ser definido para prevenir confusiones y determinar la definición de un proyecto alcanzable en términos de tiempo y recursos.

Se sugiere establecer el alcance, desarrollando previamente matrices que permitan obtener los procesos de la organización con las condiciones o dominios de la norma ISO 27001:2013 coordinados en el anexo 3 y que son aplicables a la organización.

b) Políticas del SGSI.

En esta etapa se define la política y objetivos de seguridad de la información, es decir que la política de seguridad muestre lo que la organización planea realizar con relación a la seguridad de la información, los objetivos que aspira lograr, considerando las condiciones legales y reglamentarios aplicables y teniendo presente el compromiso de la Dirección de la organización para obtenerlos.

Una política es una directiva que apoya la ejecución de los objetivos, definida en función del alcance, y está considerada como el primer control de la norma ISO/IEC 27002. Es importante tener presente que la política de seguridad de información de una organización es una sola, y luego partiendo de esta política general establecida se pueden definir las distintas políticas determinadas en los diferentes niveles, por ejemplo: política de acceso a equipos y usuarios, política de uso de equipos informáticos y dispositivos móviles, política de respaldos de base de datos, entre otras políticas.

Además, la política de seguridad define los siguientes parámetros:

- Tomar en cuenta requisitos legales relacionados a la seguridad de la información;
- Ser admitida por la alta dirección.
- Englobar objetivos y el marco general de seguridad de información de la organización;
- Estar acorde con el contexto estratégico de gestión de riesgos de la organización en el que se definirá y sostendrá el SGSI;
- Establecer criterios con los que se va a evaluar el riesgo;

c) Metodología de Evaluación de Riesgos.

La metodología que será aplicada en el análisis de riesgos será Magerit. Metodología que posee la ventaja de manifestar sus resultados en valores cuantitativos, o sea en

términos económicos, lo que facilita la toma decisiones y su validación por las máximas autoridades.

Esta etapa está compuesta por los siguientes objetivos:

- Identificar activos: realizar una identificación y tasación de activos, que serán los elementos a proteger.
- Valorar activos: los activos deben contar con una valoración.
- Identificar amenazas: Identificar y valorar las amenazas a las que están expuestos los activos.
- Calcular el impacto: Se refiere al cálculo del daño que puede generar sobre el activo al ejecutarse la amenaza.

  Impacto = Valor del activo x Porcentaje de impacto
- Calcular el riesgo: Después de calcular el impacto potencial, se calcula el riesgo potencial asociado.

  Riesgo = Frecuencia x Impacto
- Selección apropiada de tratamiento: Identificados los riesgos, se debe evaluarse las acciones apropiadas.
- Reducción del riesgo y riesgos residual: en los riesgos tratados se ha restado el riesgo en un valor "X" quedando un riesgo menor a el inicial, al cual se llama riesgo residual.

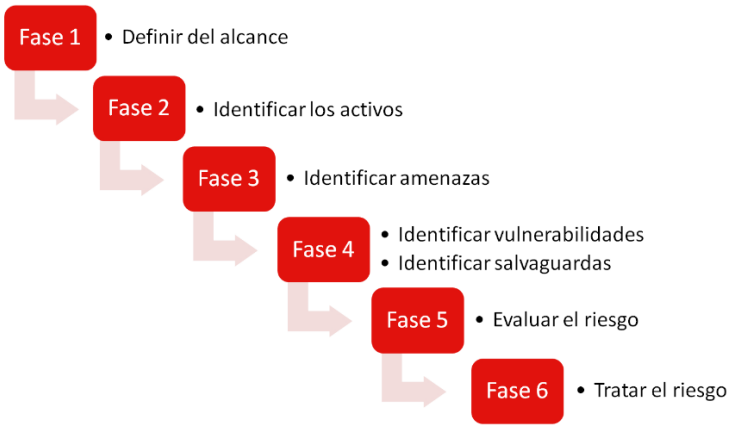


Figura 17. Metodología de gestión de riesgos Magerit

Elaborado por: Investigador

d) Identificar los riesgos (Identificar y Valorar activos).

Esta etapa está constituida por los siguientes procesos:

- Identificación de activos de información.
- Valoración de activos de información.
- Identificación de amenazas y vulnerabilidades.
- Identificar los impactos.

Identificar activos de información: En esta etapa se ejecuta un inventario de activos señalando su localización, personal responsable y las funciones que estos llevan a cabo, facilitando un análisis y valoración de los riesgos para establecer las amenazas, vulnerabilidades y efectos que presentan en las organizaciones.

Comprendiendo la norma ISO 27001:2013, se destaca como un activo de información, comprendiendo un activo como un elemento que represente valor para la organización, como por ejemplo activos de información tales como bases de datos, documentación, equipos informáticos, departamentos, manuales de usuario, software de aplicación y sistemas, contratos de equipo de comunicaciones, servicios informáticos, entre otros. La clasificación general de los activos de información se puede visualizar en la figura 7:

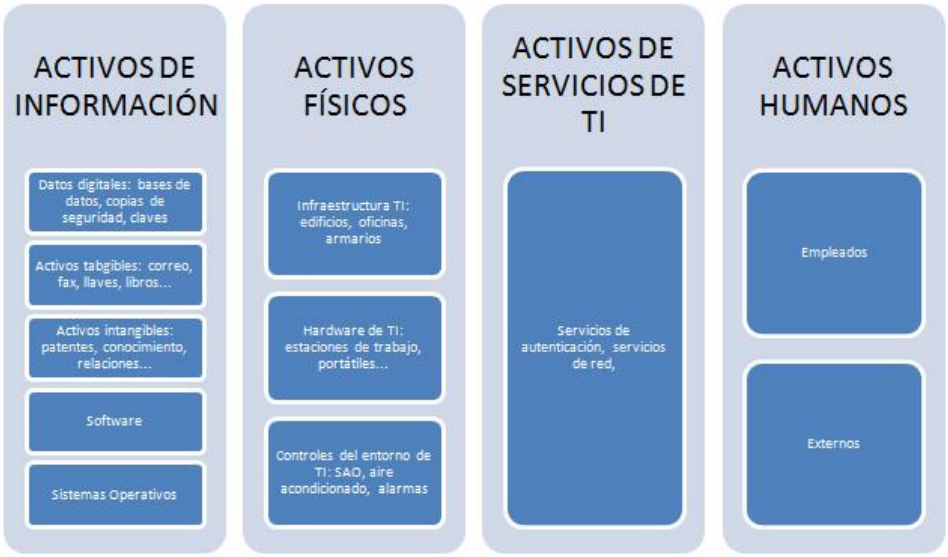


Figura 18. Clasificación de activos de información.

Elaborado por: Investigador

La información de los activos definidos anteriormente debe englobar los siguientes atributos:

- Nombre de activo.
- Descripción de activo.
- Clase a la que pertenece (Equipo, aplicación, servicio, etc.).
- Localización (Espacio físico donde se halla en la organización).
- Propietario (Responsable del activo).

Es fundamental, una vez ejecutado el inventario de activo, considerar los siguientes principios:

- **Amenazas:** Causas de alto grado de un incidente no previsto, por ejemplos daños a los sistemas de información y comunicación de la organización.
- **Vulnerabilidades:** Debilidades de activos que pueden ser aprovechadas por otras amenazas.

Para ejecutar el análisis de amenazas y vulnerabilidades se necesita:

- Elaborar un listado de amenazas que puedan ejecutarse de manera accidental en activos de información.
- Distinguir las amenazas de las vulnerabilidades de activos porque el análisis debe centrarse en las amenazas.
- Determinar riesgos internos y externos de procesos, analizando acciones que se ejecutan como las amenazas determinadas, estableciendo los riesgos originados por personal externo a la organización. (Figura 23).

Tabla 23. Amenazas y Riesgos (Internos y Externos)

Amenaza Interna	Ingreso indebido a aplicaciones	**Riesgo Interno**	Modificación en información, posibilidad de mala aplicación y daños a sistemas
	Robo por parte del personal.		Robo de información y posibilidad de mala aplicación de la misma.
	Modificación de información.		Elaboración de informes fraudulentos por cambios en la información.
	Mal uso de imagen de la organización		Robo de confidencialidad
	Problemas en servidor y sistemas de información y comunicación.		Información no disponible, daños económicos.
Amenaza Externa	Robo de identidad.	**Riesgo Externo**	Modificación de información e ingreso indebido a sistemas.
	Virus o malware.		Ataques a sistemas informáticos.
	Pérdida de información.		Copia de información secreta.
	Ataques externos.		Ingreso a sistemas con malos objetivos..
	Robo por personal ajeno		Robo de imagen y aplicación de información secreta con malos objetivos.

Elaborado por: Investigador

Valorar de Activos de Información: Una vez identificado los activos de información, el siguiente proceso de esta etapa es evaluarlos de acuerdo con su importancia dentro la organización, para permanecer con aquellos que tengan un alto valor, para luego realizar el análisis de riesgos.

La interrogante a evaluar es **¿la gestión inadecuada de estos activos, cómo afectan en la disponibilidad, confidencialidad e integridad de la información de una organización,** para el efecto se usarán el rango de valores de 1 a 5, siendo el 1 de menor afectación y 5 de mayor afectación. El valor final del activo evaluado es el promedio de los valores correspondientes a la disponibilidad, confidencialidad e integridad.

Luego de evaluar el valor por cada activo escogeremos aquellos de valor significativos, el valor umbral queda a moderación de la organización, por ejemplo, serán de consideración los activos con rango de valores igual o mayores a la 3.

A continuación (Tabla 24), se detallan las condiciones de confidencialidad, integridad y disponibilidad que se tiene que asignar a los activos en referencia con el grado de afectación: Alto, Medio y Bajo, acorde a las actividades ejecutadas de este activo en los procesos:

Tabla 24. Condiciones de Confidencialidad, Integridad y Disponibilidad por Activo.

Condición	Grado de Valoración		
	Bajo	**Medio**	**Alto**
Confidencialidad	La información es pública y no tiene impacto sobre el resultado del proceso en caso de ser accedido por personal no autorizado	La información es de uso interno y si es accedida por personas no autorizadas no afectaría el riesgo de la organización.	La información es reservada y si es accedida por personas no autorizadas, el impacto sería grave sobre los proceso de la organización.
Integridad	La modificación no autorizada no es crítica para las aplicaciones internas y el impacto es bajo en la organización	La modificación no autorizada no es crítica, pero si notoria para las aplicaciones internas y el impacto es elocuente en la organización.	La modificación no autorizada es crítica para la organización y el impacto podría sufrir la falta grave del sistema organizacional.
Disponibilidad	Se puede permitir que el activo no esté utilizable por más de un día.	Se puede permitir que el activo no esté utilizable por más de un medio día	No se puede permitir que el activo no esté utilizable por unas cuantas horas.

Elaborado por: Investigador

Identificar Amenazas y Vulnerabilidades: Señalar las amenazas relacionados con la identificación y tasación de activos, además de señalar vulnerabilidades que alterar estos activos definidos en la etapa anterior.

Identificar los impactos: Señalar las actividades que podrían presumir pérdidas de confidencialidad, integridad y disponibilidad de los activos de la organización.

e) Análisis y Evaluación de Riesgos.

El análisis y evaluación de riesgos tiene como finalidad disponer una priorización de los riesgos de procesos y activos implicados en el alcance del SGSI para su tratamiento siguiente. Esta etapa tiene que establecer las amenazas relacionada con:

- Procesos de la organización.
- Activos de información de la organización,
- Probabilidad de ocurrencia de amenazas
- Vulnerabilidades frente a las amenazas.

Todo esto facilitara considerar el efecto de concretar cualquier error de seguridad de información en la organización. Además, para ejecutar estas actividades se debe:

- Medir el efecto en la organización de una resolución de la seguridad que deduzca la falta de confidencialidad, integridad o disponibilidad de un activo de información.

- Medir de manera real la posibilidad de que suceda una resolución de la seguridad en relación a las amenazas, vulnerabilidades e impacto en los activos y los controles ya implementados.

- Estimar el nivel de riesgo.

Luego de definir las amenazas y vulnerabilidades de los activos, se tasará el riesgo, el mismo que se determinará por el mayor valor de cada activo teniendo presente:

Grado de Riesgo = Grado de Amenaza x Grado de Vulnerabilidad x Grado de efecto

El grado de vulnerabilidad como posibilidad de amenaza se puede tasar en un rango de valores que va de 0 a 3:

Tabla 25. Grado de Vulnerabilidad.

Grado	Vulnerabilidad
0	No aplica
1	Bajo
2	Medio
3	Alto

Elaborado por: Investigador

f) Identificar y evaluar las opciones del tratamiento de riesgo.

En esta etapa (Ver Figura 19) se debe tener presente los siguientes lineamientos:

- Aplicar los controles convenientes.
- Asumir el riesgo si se cumple con políticas y criterios establecidos en la aceptación de riesgos.
- Prevenir riesgos.
- Transferir el riesgo a terceros.

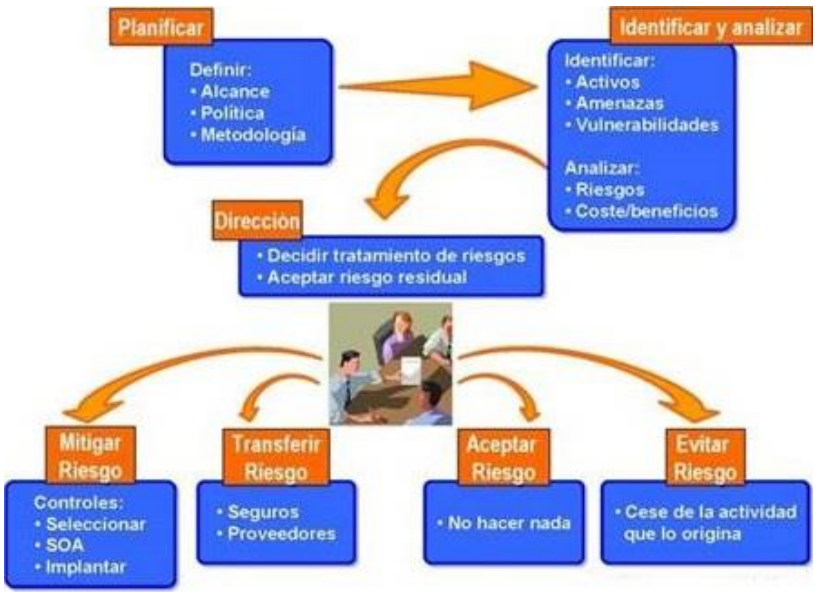


Figura 19. Gestión de Riesgos.

Elaborado por: Investigador

g) Seleccionar controles para el tratamiento del riesgo.

Se debe elegir los objetivos de control y controles del Anexo 3 para el tratamiento del riesgo que ejecutan las condiciones señaladas en el proceso de evaluación del riesgo, además de aprobar por medio la alta dirección de la organización los riesgos residuales, como la implantación y utilización del SGSI.

h) Declaración de aplicabilidad que contenga:

Esta etapa debe incluir los siguientes objetivos a continuación:

- Objetivos de control, controles elegidos y las causas para su para su selección;
- Objetivos de control y controles que ya hallan implantados;
- Objetivos de control y controles del anexo 3 separados y las causas para su separación; esta es una técnica que ayuda a encontrar probables omisiones involuntarias.

Fase 2: Hacer (Implementación y operar el SGSI)

Esta fase contempla las siguientes etapas o actividades (Ver Tabla 26):

Tabla 26. Etapas del Ciclo Hacer.

Fase	Ciclo	Etapa	Actividad
2	Hacer (Implementar y operar el SGSI)	a	Definir plan de tratamiento del riesgo.
		b	Implantar plan de tratamiento de riesgos.
		c	Implementar los controles
		d	Definir un sistema de métricas
		e	Formar y Concientizar.
		f	Gestionar operaciones del SGSI
		g	Gestionar recursos del SGSI
		h	Implantar procedimientos y controles

Elaborado por: Investigador.

a) Plan de tratamiento del riesgo.

La finalidad de esta etapa es elegir los controles y aplicar las reglas apropiadas, luego de haber analizado, cuantificado y determinado el efecto que tienen los riesgos en la organización, con el objetivo de corregir los riesgos y prevenir daños esenciales al factor de riesgo, revisando el grado de conveniencia en caso de aceptar el riesgo.

En el plan de tratamiento del riesgo se determina cómo se implementarán los controles, personal a cargo, fechas de elaboración, presupuesto de la realización, estos lineamientos permitirán:

- Una organización competente con sus funciones.
- Disponer de la efectividad de controles internos.
- Disponer de estatutos válidos y de acuerdo a las normas establecidas.

En el plan de tratamiento de riesgos se tiene que elegir mecanismos de respuesta para los riesgos que posean altas probabilidades de éxito, entre los cuales podemos aplicar los mecanismos detallados a continuación:

- **Transmitir el riesgo a un tercero:** Esta factibilidad permite transportar los resultados de un riesgo a una tercera parte unido con el compromiso de la respuesta.

- **Mitigar el riesgo:** Permite bajar las probabilidades de sucesos contra un límite admitido previo del momento de activación. Es fundamental que los valores de mitigación sean menores a la posibilidad del riesgo y sus resultados. En la ejecución de la mitigación de riesgos se requiere:

  - Elegir los controles
  - Implantar los controles
  - Revisar los controles
  - Definir indicadores.

La elección de estos controles se realiza tomando como referencia la norma ISO/IEC 27002 del anexo 3.

- **Eliminar o evitar el riesgo:** Trata de suprimir la amenaza eliminando la causa que puede ocasionarla.

- **Aceptar o asumir el riesgo:** Aplica cuando se elige no hacer frente al riesgo previa a su activación. La admisión puede ser activa o pasiva, es activa si existe un plan de contingencia que se ejecuta siempre y cuando el riesgo se presenta, o pasiva, cuando la admisión no necesita de alguna acción, solo se lleva a cabo la gestión del riesgo.

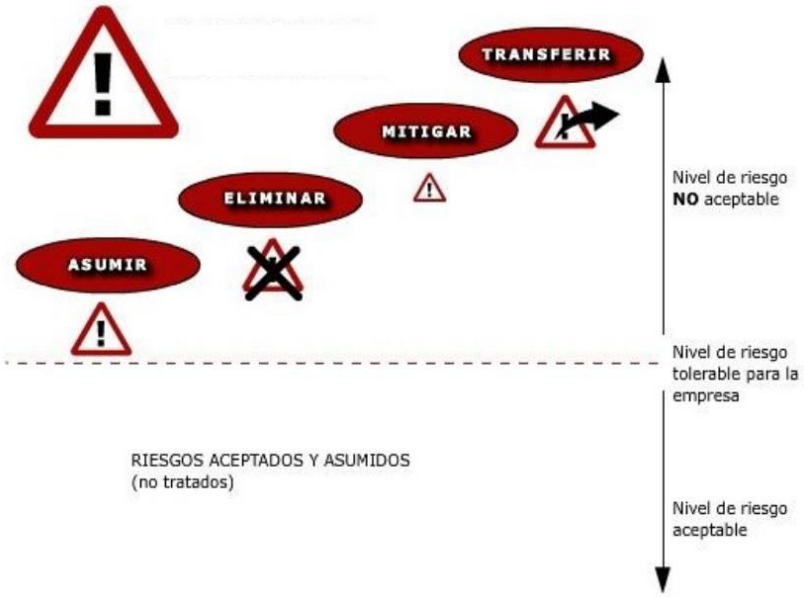


Figura 20. Tratamiento del Riesgo en el SGSI.

Elaborado por: Autor

Además, se debe denominar un responsable de implementar el mecanismo elegido para los riesgos de acuerdo al plan preestablecido. En el resultado de esta implantación pueden surgir riesgos residuales, es decir riesgos que continúan luego de implementar las respuestas al riesgo y riesgos secundarios que surgen como resultado de la implementación de la respuesta a un riesgo.

b) Selección de Controles

La selección adecuada de los controles permite asegurar que cada aspecto de los activos de información de la organización, que se valoraron con algún grado de riesgo, sea

cubierto y auditable. La selección adecuada de controles permite definir el plan de tratamiento de riesgos que estará contenido en los 114 controles de la norma ISO/IEC 27002 del anexo 3.

Los objetivos de control y los controles tienen que seleccionarse como parte del proceso de definición y establecimiento del SGSI, teniendo presente los 14 dominios de la norma ISO 27001 (Ver Figura 21).

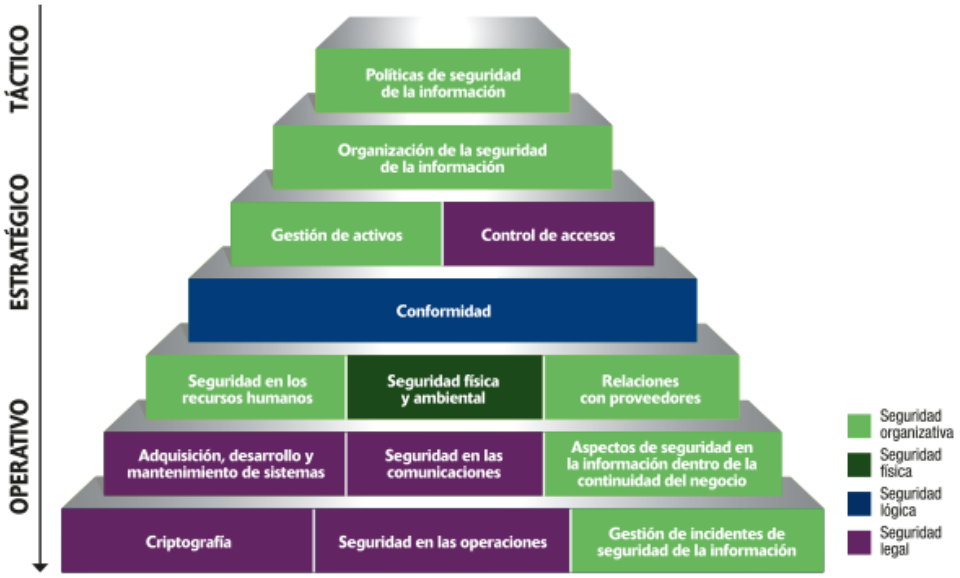


Figura 21. Estructura de dominios ISO 27002.

Elaborado por: Investigador

Para definir los controles la organización debe tener presente:

- El valor del control frente al valor del efecto que tendría el activo a proteger si este fuera afectado por una amenaza.
- Qué los controles estén disponibles.

Además, hay que tener presente la clasificación de controles:

- **Controles Técnicos**. Sistemas de encriptado, copias de seguridad de datos, sistemas anti-phising, actualización de aplicaciones, software de utilidades, etc.

- **Controles Organizativos**. Política de Controles y Seguridad, métodos de aplicación de sistemas de información para usuarios, capacitaciones, proyectos mejora continua.

c) Implementación de controles

Para implementar los controles previamente escogidos en la etapa anterior y que serán aplicados por el SGSI, se deben definir técnicas.
Se sugiere reunir distintos controles para hacer más efectivo el SGSI, a su vez aumenta su operatividad y permitir su implementación.

d) Verificación de controles

Los controles implementados deben pasar por una exhaustiva revisión para corroborar su adecuada ejecución, luego de ser establecidos los controles se tiene que realizar la revisión de su funcionamiento a través de una serie de medidores que aprueban su evaluación y seguimiento.

e) Formación y Concienciación.

El estándar ISO 27001 en esta etapa establece que el personal debe estar comprometido con los procesos asociados al SGSI, es fundamental entrenar y capacitar al personal en temas de seguridad informática, creando una cultura de adecuadas prácticas de seguridad de información, además de reducir las probabilidades de amenazas para la organización.

f) Objetivos de Control e Indicadores

El plan de tratamiento de riesgo debe incorporar actividades que se ejecutarán para gestionar el riesgo, además estas actividades deben contar con medidores que faciliten calcular la eficiencia de los controles definidos previamente, el cálculo se hará teniendo presente los registros del sistema.

Las medidas que se fijen deben tener presente las variables que faciliten el cumplimiento de objetivos y agrupen los siguientes criterios: Pertinente, disponible, confiable y operatividad.

Fase 3: Revisar (Monitorear y Revisar el SGSI)

Esta fase contempla las siguientes etapas o actividades (Ver Tabla 27):

Tabla 27. Etapas del Ciclo Revisar.

Fase	Ciclo	Etapa	Actividad
3	Revisar (Monitorizar y revisar el SGSI)	a	Monitorear y Revisar el SGSI.
		b	Revisar y medir la efectividad de los controles del SGSI (métricas del SGSI)
		c	Revisar los riesgos residuales
		d	Realizar auditorías internas del SGSI.
		e	Revisar el SGSI por parte de la dirección.

Elaborado por: Investigador

a) Monitorear y Revisar el SGSI.

En esta etapa la revisión del SGSI está establecida por la norma ISO/IEC 27001, que sugiere chequear el sistema una vez al año, para determinar su nivel de eficiencia de acuerdo con las metas de la organización. Este chequeo facilita la evaluación del SGSI, además de descubrir fortalezas, debilidades y la toma de medidas respecto a proyectos de mejora continua.

La norma ISO/IEC 27001, determina los siguientes procedimientos que deberá realizar la organización para ejecutar el seguimiento al SGSI:

- Ejecutar métodos de monitoreo y revisión.
- Realizar chequeos regulares del SGSI.
- Calcular el impacto de los controles para corroborar que se hayan cumplido las condiciones de seguridad.

- Chequear el análisis y evaluación del riesgo a intervalos proyectados y chequear el grado de riesgo residual y riesgo admisible identificado.
- Ejecutar auditorías internas al SGSI por etapas de tiempo proyectado.
- Ejecutar una revisión gerencial del SGSI para mantener queel alcance continúe adecuado y se verifiquen las mejoras en el proceso del SGSI.
- Actualizar los planes de seguridad para tener presente los hallazgos de las acciones de monitoreo y chequeo.
- Registrar actividades y sucesos que podrían lograr un efecto sobre el desempeño del SGSI.

Auditorías Internas

En esta etapa se deben establecer las auditorías internas en la organización con el propósito de determinar condiciones necesarias para mantener y mejorar el SGSI, realizando un trabajo de evaluación de la implementación de los términos establecidos en la política de seguridad y los controles asociados con la seguridad informática determinado en el SGSI.

El personal que ejecute las auditorías internas debe poseer un alto entendimiento en la implementación del SGSI y la utilización de normas ISO/IEC 27001 en la organización, ya que este personal ejecutara el servicio de valorar y verificar controles complejos, desarrollando y utilizando metodologías de auditoría.

Para ejecutar las auditorías internas se puede aplicar los siguientes métodos: revisión, estudio, entrevistas, documentación y procedimientos analíticos a los sistemas informáticos de la organización.

Los auditores deben incorporar las siguientes acciones:

- Programar la auditoría.
- Ejecutar labores establecidas en las fases de la auditoría.
- Administrar amenazas y riesgos que pueden aparecer en la auditoría.

- Comunicar a las máximas autoridades de la organización sobre el diseño y funcionamiento de controles implementados, la veracidad de la información facilitada, la suficiencia de las medidas en la que basan las conclusiones de la auditoría.

Fase 4: Actuar (Mantener y Mejorar el SGSI)

Esta fase contempla las siguientes etapas o actividades:

Tabla 28. Etapas del Ciclo Actuar.

Fase	Ciclo	Etapa	Actividad
4	Actuar (Mantener y mejorar el SGSI)	a	Implementar mejoras al SGSI.
		b	Realizar acciones preventivas y correctivas
		c	Evaluar sugerencias y definir la implementación de mejoras.
		d	Comunicar acciones y mejoras del SGSI
		e	Corroborar la efectividad de las acciones.

Elaborado por: Investigador

La fase final cuenta con cuatro etapas donde se implementan medidas correctivas y planes de mejora conseguidos como resultado de la revisión del SGSI. Algunas de las acciones de esta etapa son las siguientes:

- Establecer plan de actividades basado en reglas correctivas, preventivas y planes de contingencia.
- Ejecutar planes de mejoramiento al SGSI, planteados en la fase de verificación.
- Valorar el impacto de los planes de mejora continua del SGSI, teniendo presente los resultados de actividades implementadas previamente.
- Actualizar planes de seguridad en sistemas informáticos en función de las conclusiones.
- Chequear la adecuada implementación de las mejoras propuestas al SGSI.

- Verificar y Mejorar la implementación del SGSI con un instrumento de escaneo de vulnerabilidades y amenazas para la mejora continua de la gestión de la seguridad de la información y evaluar los parámetros de confidencialidad, integridad y disponibilidad de los sistemas de información y comunicación de las instituciones de Educación Superior. Este instrumento ejecuta un análisis, identificación y reporte muy sistemático de las vulnerabilidades en cuestión de seguridad que se tienen en una infraestructura de tecnologías de la información y comunicación. La intención es proteger en el mejor porcentaje posible la seguridad de la información ante el ataque de un ente externo.

  Además, este instrumento permitirá remediar las vulnerabilidades dentro del ambiente TI antes de que un hacker o agresor cibernético logre detectarlas, es cierto, nadie puede proteger una empresa al 100% pues cada segundo nace nuevos virus y es imposible seguirles el paso.

¿Cuáles son los entregables en un Escaneo de Vulnerabilidades?

- Contrato de confidencialidad
- Detección y evaluación de las vulnerabilidades a través del uso de hardware y software
- Análisis del muestreo
- Reporte cuantitativo y cualitativo de los datos obtenidos
- Sugerencias
- Propuesta de Soluciones para robustecer la estrategia de ciberseguridad.

¿Cada que tiempo se debe realizar una ejecución de escaneo de vulnerabilidades?

Se recomienda realizar este escaneo de vulnerabilidades cada 6 meses, de esta forma se da un seguimiento equilibrado y estructurado a la estrategia de la gestión de la Seguridad de la Información en las Instituciones de Educación Superior de la ciudad de Machala.

6.7.2 Modelo Operativo.

Contexto de la Organización (Comprensión de la Organización).

La Universidad Técnica de Machala forma profesionales en diferentes carreras que esta oferta, para este efecto se resguarda con estrategias para la excelente gestión de los sistemas de información y comunicación, brindando servicios de la mejor manera a los usuarios finales. El Departamento de Tecnologías de la Información y Comunicación desempeña un rol fundamental convirtiéndose en un facilitador de herramientas para la mejora continua de la gestión de la seguridad de la información y los procesos.

La Dirección de Tecnología de Información y Comunicación de la Universidad Técnica de Machala cumple con un objetivo que es:

- Gestionar la seguridad de la información,
- Desarrollar, administrar y controlar las diferentes aplicaciones y utilidades informáticas con que trabaja la institución.
- Brindar mantenimiento tanto del hardware como del software institucional
- Dar soporte a los requerimientos técnicos, logísticos.
- Capacitar al personal institucional en el área informática para fortalecer y beneficiar a la comunidad universitaria.

Estructura Organizacional del Departamento de Tecnologías de la Información y Comunicación de la Universidad Técnica de Machala (Figura 22).

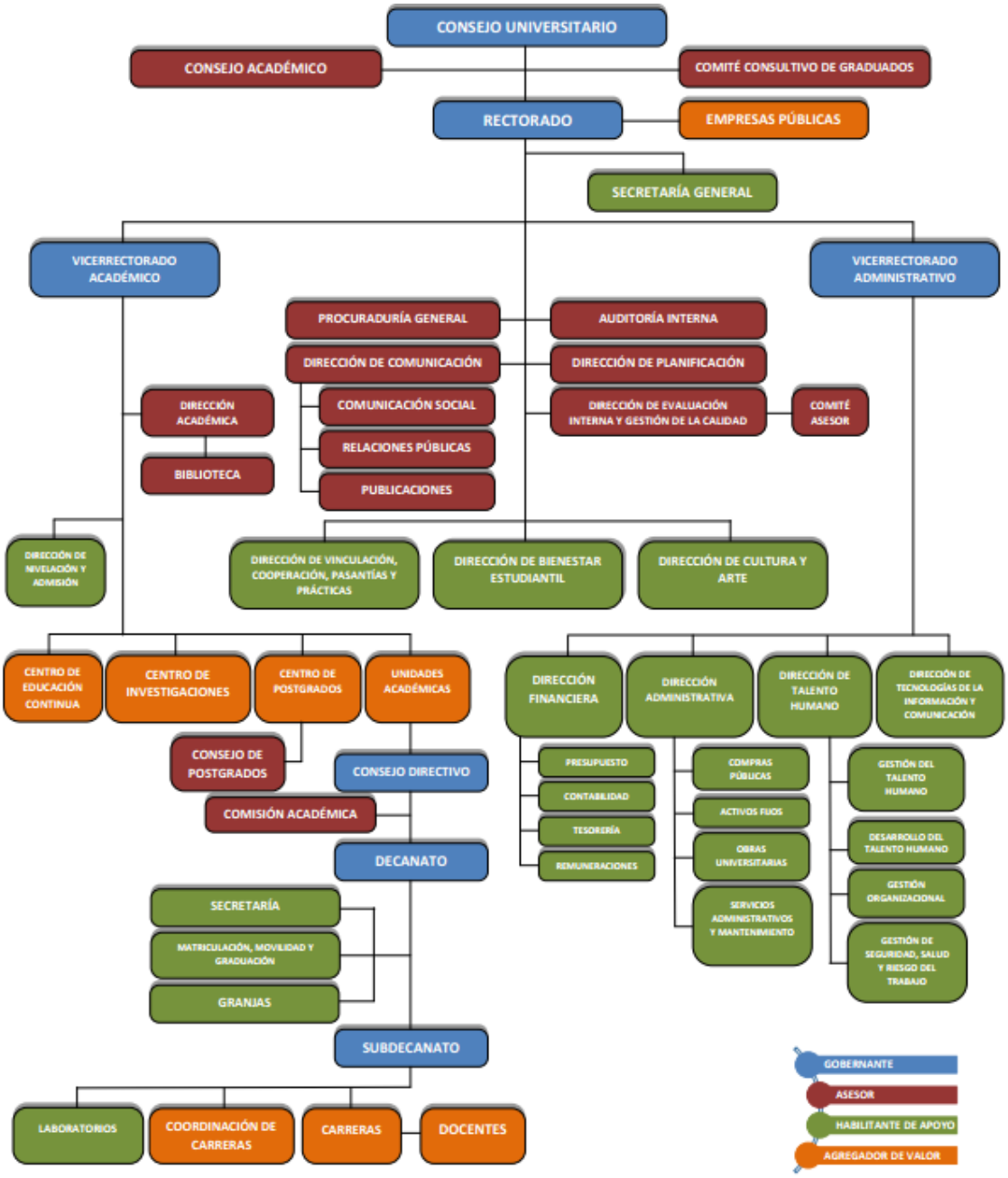


Figura 22. Estructura Organizacional de la UTMACH.

Elaborado por: *Investigador*

Desarrollo de la Implementación.

Para la implementación del Sistema de Gestión de Seguridad de la Información en la Universidad Técnica de Machala, se seguirá el modelo de mejora continua PDCA, donde se aplican las cuatro fases de la metodología para la implementación del Sistema de Gestión de Seguridad de la Información debido a que la institución cuenta con diferentes activos y personal que ejecuta actividades relacionadas con la gestión de la seguridad de la información.

Las fases, etapas y actividades del modelo de mejora continua PDCA para implementar la propuesta en la institución se detalla a continuación (Ver Tabla 29).

Tabla 29. Fases, Etapas y actividades del modelo PDCA.

Fase	Ciclo PDCA	Actividad (Etapas)
1	PLANEAR. (Establecer)	a) Definir alcance del SGSI. b) Definir política de seguridad. c) Metodología para la evaluación y control de riesgos. d) Identificar los riesgos (Inventario y Tasación de Activos) e) Analizar y evaluar los riesgos f) Identificar y evaluar opciones del tratamiento de riesgos. g) Seleccionar controles para el tratamiento del riesgo. h) Declaración de Aplicabilidad
2	HACER. (Implementar y operar el SGSI)	a) Definir plan de tratamiento de riesgos b) Implantar el plan de tratamiento de riesgos. c) Implementar los controles. d) Definir un sistema de métricas e) Formar y concientizar. f) Gestionar recursos del SGSI. g) Implantar procedimientos y controles.
3	VERIFICAR. (Monitorizar y revisar el SGSI)	a) Monitorear y Revisar el SGSI b) Revisar la efectividad de los controles del SGSI (métricas del SGSI) c) Revisar los riesgos residuales d) Realizar auditorías internas del SGSI e) Revisar el SGSI por parte de la dirección
4	ACTUAR. (Mantener y mejorar el SGSI)	f) Implementar mejoras al SGSI. g) Realizar acciones preventivas y correctivas. h) Evaluar sugerencias y definir la implementación de mejoras. i) Comunicar acciones y mejoras del SGSI. j) Asegurar alcanzar los objetivos previstos.

Elaborado por: Investigador

6.7.2.1 FASE 1: Planear: (Establecer el SGSI).

Esta fase está constituida las siguientes etapas:

a) Alcance.
b) Políticas
c) Metodología de evaluación de riesgos.
d) Identificar los riesgos (Identificar y Valorar los activos)
e) Analizar y Evaluar los Riesgos
f) Identificar y evaluar opciones del tratamiento de riesgo.
g) Seleccionar controles para el tratamiento del riesgo.
h) Declaración de Aplicabilidad

a) Alcance.

La definición del alcance del Sistema de Gestión de Seguridad de la Información es responsabilidad del rector de la Universidad Técnica de Machala, respaldado por el grupo de trabajo que gerencia el proyecto, el mismo que esta orientados al área de la seguridad de la información.

El alcance del Sistema de Gestión de Seguridad de la Información será aplicado a procesos que se desarrollan en el departamento de Tics de la Universidad Técnica de Machala los cuales se detallan a continuación:

- Acceso a sistemas de información y comunicación.
- Acceso a los activos informáticos.
- Gestión y desarrollo de software.
- Mantenimiento de hardware y software.
- Revisión de red y servicios a terceros.
- Administración de e-mail.
- Gestión de seguridad.
- Soporte a usuarios.

b) Política.

Para cumplir la política establecida en el departamento de Tics de la Universidad Técnica de Machala se han definido los siguientes objetivos:

- Desarrollar e Implementar un sistema de gestión de seguridad de la información.
- Definir una metodología de evaluación del riesgo adecuada para el SGSI y los requerimientos de la Universidad Técnica de Machala.
- Implantar medidas de seguridad para prevenir las violaciones de seguridad
- Implantar un mecanismo de control de riesgos de la información.
- Implantar criterios de admisión del riesgo
- Implantar niveles de riesgo admitido.

b) Metodología de Evaluación de Riesgo aplicada al departamento de Tics de la Universidad Técnica de Machala.

La metodología aplicada será Magerit, la misma que desarrolla una serie de objetivos que serán aplicados en la Identificación de Riesgos y que se detallan a continuación:

- Identificar activos.
- Valorar activos.
- Identificar amenazas y vulnerabilidades.
- Calcular el impacto.
- Calcular el riesgo.
- Selección apropiada de tratamiento.
- Reducción del riesgo y riesgos residual.

Estos objetivos cumplen un papel fundamental al momento de implementar el SGSI en la Universidad Técnica de Machala, por lo que su normal desarrollo es vital para alcanzar una gran gestión de la seguridad de la información.

d) Identificar los riesgos.

La aplicación de esta etapa se basa en los objetivos de la metodología Magerit.

Identificar activos.

Para la identificación de los activos se utilizaron datos proporcionados por el jefe de sistemas del departamento de Tecnologías de la Información y Comunicación de la Universidad Técnica de Machala, correspondiente al siguiente inventario (Ver Tabla 30).

Tabla 30. Valoración de Activos - Departamento Tics.

No.	Activo	Tipo de Activo
1	Servidores.	Hardware
2	Computadoras de escritorio y portátiles	
3	Impresoras	
4	Sistemas Pegasus y E-volutions	Software
5	Software ACL	
6	Red LAN y WAN	Comunicaciones
7	Sistema de telefonía IP	
8	Servicio de e-mail	Servicios
9	Sitio Web	

Elaborado por: Investigador

Valorar activos.

Para tasar los activos se aplicaron directrices de confiabilidad, integridad y disponibilidad de estos activos:

Tabla 31. Valoración de Activos - Departamento de Tics.

No.	Activo	Confiabilida	Integridad	Disponibilid	Total
1	Servidores	4	5	4	4
2	Computadoras de escritorio y portátiles	2	4	2	3
3	Impresoras	2	4	2	3
4	Sistemas Pegasus y E-volution	3	4	3	3
5	Software ACL	5	4	5	5
6	Red LAN y WAN	3	4	3	3
7	Servicio de Telefonía IP	2	4	3	3
8	Servicio de e-mail	3	4	3	3
9	Sitio Web	2	4	2	3

LEYENDA					
Grado de impacto	Muy poco	Poco	Medio	Alto	Muy alto
Valor	1	2	3	4	5

Elaborado por: Investigador

Identificar amenazas y vulnerabilidades.

A continuación, la figura 37 muestra los activos pertenecientes a la Universidad Técnica de Machala, destacando las amenazas y vulnerabilidad a la que están expuestos estos activos.

Tabla 32. Identificación de Amenazas y Vulnerabilidad.

No.	Activo	Valor de Activo	Amenaza	Vulnerabilidad
1	Servidores	4	Acceso lógico intencional	Debilidad técnica en sistema operativo
			Acceso lógico intencional	Sistema operativo desactualizado
			Acceso lógico intencional	Carencia de plan de licencias de software
			Defectos de causa física	Agotamiento natural de partes
			Defectos de causa física	Piezas deficientes de fábrica
			Defectos de causa física	Presencia de basura
			Catástrofes naturales	Carencia de plan antisísmico del edificio
			Defectos de causa física	Carencia de mantenimientos preventivos.
			Defectos de causa lógica	Contraseña del administrador compartida.
			Defectos de causa lógica	Ingreso indebido
			Caída de sistema por abuso de recursos	Carencia de límites y controles en utilizar recursos
2	Computadoras de escritorio y portátiles	3	Catástrofes naturales	Carencia de plan antisísmico del edificio
			Defectos de causa física	Carencia de mantenimientos preventivos.
			Defectos de causa física	Agotamiento natural de partes
			Defectos de causa física	Partes defectuosas de fábrica
			Defectos de causa física	Presencia de basura
			Defectos de causa física	Contraseña del administrador compartida.
			Defectos de causa física	Ingreso indebido
			Caída de sistema por abuso de recursos	Carencia de límites y controles en utilizar recursos
			Acceso lógico intencional	Debilidad técnica en sistema operativo

No.	Activo	Valor de Activo	Amenaza	Vulnerabilidad
3	Impresoras	3	Defectos de causa física	Agotamiento natural de partes
			Defectos de causa física	Partes defectuosas de fábrica
			Caída, suspensión y negación de servicios y sistemas.	Agotamiento de recursos
			Abuso de privilegios de acceso	Carencia de revisiones continuas de privilegios de ingreso
4	Sistemas Pegasus y E-volution	3	Propagación de programas dañinos	Bases de datos de antivirus no actualizadas.
			Exceso de privilegios de ingresos	Carencia de revisiones continuas de privilegios de ingreso
5	Software ACL	5	Exceso de privilegios de ingresos.	Carencia de revisiones continuas de privilegios de ingreso
6	Red LAN y WAN	3	Defectos de causa física	Desgaste natural de partes
			Defectos de causa física	Partes deficientes de fábrica
			Caída, suspensión y negación de servicios y sistemas.	Agotamiento de recursos
			Exceso de privilegios de ingresos	Carencia de revisiones continuas de privilegios de ingreso
7	Sistema de Telefonía IP	3	Defectos de causa física	Desgaste natural de partes
			Defectos de causa física	Partes deficientes de fábrica
			Caída, suspensión y negación de servicios y sistemas.	Agotamiento de recursos
			Exceso de privilegios de ingresos	Carencia de revisiones continuas de privilegios de ingreso
8	Servicio de e-mail	3	Utilización no prevista	Confusión de usuarios
			Caída, suspensión y negación de servicios y sistemas.	Carencia de límites y controles en utilizar recursos
			Fuga de información	Carencia de control de contenidos transmitidos en la red
			Acceso lógico intencional	Debilidad técnica en el sistema
			Acceso lógico intencional	Sistema desactualizado
			Caída, suspensión y negación de servicios y sistemas.	Agotamiento de recursos
			Exceso de privilegios de ingresos	Carencia de revisiones continuas de privilegios de ingreso
9	Sitio Web	3	Caída, suspensión y negación de servicios y sistemas.	Falta de límites y control en el uso de recursos

Elaborado por: Investigador

e) Analizar y Evaluar el riesgo.

Grado de Admisión del Riesgo		
Valor del	**Grado del riesgo**	**Propósito**
1-4	Admitido	No se aplican controles
5-10	Pesado	Aplica controles para grado admitido
11-15	Grave	No aplica controles de grado pesado
16-25	Maligno	No aplica controles grado grave

Tabla 33. Análisis y Evaluación del Riesgo.

Activo	Amenazas	Posibilidad de ocurrencia de la amenaza	Vulnerabilidades	Posibilidad que la amenaza penetre la vulnerabilidad	Valor de activos en Riesgo	Posibilidad de ocurrencia de amenaza	Total Riesgo
Servidores	Acceso lógico intencional	4	Debilidad técnica en sistema operativo	4	20	20	3,4
	Acceso lógico intencional	4	Sistema operativo desactualizado	4	20	20	3,4
	Acceso lógico intencional	4	Carencia de plan de licencias de software	3	15	20	3,4
	Defectos de causa física	4	Agotamiento natural de partes	3	15	20	3,4
	Defectos de causa física	4	Piezas deficientes de fábrica	3	15	20	3,4
	Defectos de causa física	4	Presencia de basura	3	15	20	3,4
	Catástrofes naturales	4	Carencia de plan antisísmico del edificio	2	10	20	3,4
	Defectos de causa física	4	Carencia de antenimientos preventivos.	2	10	20	3,4
	Defectos de causa lógica	4	Contraseña del administrador compartida.	2	10	20	3,4
	Defectos de causa lógica	4	Ingreso indebido	2	10	20	3,4
	Caída de sistema por abuso de recursos	4	Carencia de límites y controles en utilizar recursos	4	10	20	3,4

.

Activo	Amenazas	Posibilidad de ocurrencia de la amenaza	Vulnerabilidades	Posibilidad que la amenaza penetre la vulnerabilidad	Valor de activos en Riesgo	Posibilidad de ocurrencia de amenaza	Total Riesgo
Computadores de escritorio y portátiles.	Catástrofes naturales	4	Carencia de plan antisísmico del edificio	2	10	15	2,8
	Defectos de causa física	4	Carencia de mantenimientos preventivos.	2	10	15	2,8
	Defectos de causa física	4	Agotamiento natural de partes	3	15	15	2,8
	Defectos de causa física	4	Partes defectuosas de fábrica	3	15	15	2,8
	Defectos de causa física	4	Presencia de basura	3	15	15	2,8
	Defectos de causa física	4	Contraseña del administrador compartida.	2	10	15	2,8
	Defectos de causa física	4	Ingreso indebido	2	10	15	2,8
	Caída de sistema por abuso de recursos	4	Carencia de límites y controles en utilizar recursos	4	10	15	2,8
	Acceso lógico intencional	4	Debilidad técnica en sistema operativo	4	10	15	2,8
Impresoras	Defectos de causa física	3	Agotamiento natural de partes	3	10	10	1,8
	Defectos de causa física	3	Partes defectuosas de fábrica	3	10	10	1,8
	Caída, suspensión y negación de servicios y sistemas.	3	Agotamiento de recursos	3	10	10	1,8
	Abuso de privilegios de acceso	3	Carencia de revisiones continuas de privilegios de ingreso	3	10	10	1,8
Sistemas Pegasus y E-volution	Propagación de programas dañinos	3	Bases de datos de antivirus no actualizadas.	3	12	12	1,8
	Exceso de privilegios de ingresos	3	Carencia de revisiones continuas de privilegios de ingreso	3	12	12	1,8
Software ACL	Exceso de privilegios de ingresos.	3	Carencia de revisiones continuas de privilegios de ingreso	3	14	14	1,8

Activo	Amenazas	Posibilidad de ocurrencia de la amenaza	Vulnerabilidades	Posibilidad que la amenaza penetre la vulnerabilidad	Valor de activos en Riesgo	Posibilidad de ocurrencia de amenaza	Total Riesgo
Red LAN y WAN	Defectos de causa física	3	Desgaste natural de partes	3	13	13	2,4
	Defectos de causa física	3	Partes deficientes de fábrica	3	13	13	2,4
	Caída, suspensión y negación de servicios y sistemas.	3	Agotamiento de recursos	3	13	13	2,4
	Exceso de privilegios de ingresos	3	Carencia de revisiones continuas de privilegios de ingreso	3	13	13	2,4
Sistema de Telefonía IP	Defectos de causa física	3	Desgaste natural de partes	3	7	7	2,8
	Defectos de causa física	3	Partes deficientes de fábrica	3	7	7	2,8
	Caída, suspensión y negación de servicios y sistemas.	3	Agotamiento de recursos	3	7	7	2,8
	Exceso de privilegios de ingresos	3	Carencia de revisiones continuas de privilegios de ingreso	3	7	7	2,8
Servicio de e-mail	Utilización no prevista	4	Confusión de usuarios	4	19	19	2,2
	Caída, suspensión y negación de servicios y sistemas.	4	Carencia de límites y controles en utilizar recursos	4	19	19	2,2
	Fuga de información	4	Carencia de control de contenidos transmitidos en la red	4	19	19	2,2
	Acceso lógico intencional	4	Debilidad técnica en el sistema	4	19	19	2,2
	Acceso lógico intencional	4	Sistema desactualizado	4	19	19	2,2
	Caída, suspensión y negación de servicios y sistemas.	4	Agotamiento de recursos	3	19	19	2,2
	Exceso de privilegios de ingresos	4	Carencia de revisiones continuas de privilegios de ingreso	3	14	19	2,2
Sitio Web	Caída, suspensión y negación de servicios y sistemas.	4	Falta de límites y control en el uso de recursos	4	15	15	2,2

Elaborado por: Investigador

f) Identificar y Evaluar las opciones para el tratamiento del riesgo.

El análisis y evaluación de riesgos de los activos de la Universidad Técnica de Machala brindo una visión real de los riesgos, facilito valorizar las amenazas a las cuales están más expuestos los activos de información, es decir, con este estudio podemos conocer en qué dirección podemos orientar los recursos del Departamento de Tecnologías de la Información y Comunicación de la Universidad Técnica de Machala, para esto se cuenta con cuatro opciones de tratamiento del riesgo que son:

- Reducir el riesgo, con la aplicación de contramedidas establecidas en los controles de la norma ISO/IEC 27002.
- Evitar los riesgos, previniendo llevar a cabo las acciones que originan los riesgos.
- Transferir el riesgo, a un tercero, o sea, a tercerización de servicios.
- Asumir el riego, o sea correr el riesgo.

La alternativa de asumir un riesgo deber ser admitida por el rectorado de la Universidad Técnica de Machala, en mucho de los casos se muestra esta postura cuando el control necesario de establecer un valor monetario que el mismo activo.

Para el estudio de esta investigación la única alterativa de tratamiento que se utilizó fue la de reducción del riesgo.

g) Selección de controles para el tratamiento del riesgo.

Los controles son las contramedidas o salvaguardas especificadas en el Anexo 3 (Norma ISO/IEC 27001:2013), enfocados a los 14 dominios de cobertura de la norma, como son (Ver Tabla 24):

Tabla 34. Dominios de la Norma ISO/IEC 27001.

No.	Dominio
1	Políticas de seguridad
2	Aspectos organizativos de la seguridad de la información.
3	Seguridad ligada a los recursos humanos.
4	Gestión de activos.
5	Control de accesos.
6	Cifrado
7	Seguridad física y ambiental
8	Seguridad en la operatividad
9	Seguridad en las telecomunicaciones
10	Adquisición, desarrollo y mantenimiento de los sistemas de información
11	Relaciones con suministradores.
12	Gestión de incidentes en la seguridad de la información
13	Aspectos de seguridad de la información en la gestión de la continuidad del negocio
14	Cumplimiento

Elaborado por: Investigador

La selección de los controles que la Universidad Técnica de Machala debe implementar se lo hace:

- Del tratamiento del riesgo, enfocados a suprimir vulnerabilidades o reducir los impactos.
- Las condiciones legales (implementación no es discutible).

Se ha considerado como antecedente a la norma ISO/IEC 17799:2005 actualmente ISO/IEC 27002:2013 para un aumento de las prácticas para implementar los controles e incluir los controles sugeridos por el Jefe del Departamento de Tics de la Universidad Técnica de Machala.

Tabla 35. Selección de Controles. Departamento de Tics.

Activo	Amenazas	Vulnerabilidad	Opción de tratamiento de riesgo	Controles o Salvaguardas de norma ISO/IEC 27001 (Control Vulnerabilidad)
Servidores	Acceso lógico intencional	Debilidad técnica en sistema operativo	Reducción	9.1.1 Política de control de accesos. 9.1.2 Control de acceso a las redes y servicios asociados. 9.2.6 Retirada o adaptación de los derechos de acceso. 12.4.2 Protección de los registros de información.
	Acceso lógico intencional	Sistema operativo desactualizado		
	Acceso lógico intencional	Carencia de plan de licencias de software		
	Defectos de causa física	Agotamiento natural de partes		11.1.5 El trabajo en áreas seguras. 11.2.2 Instalaciones de suministro. 11.2.4 Mantenimiento de los equipos 12.3.1 Copias de seguridad de la información. 14.2.3 Revisión técnica de aplicaciones tras efectuar cambios en sistema operativo. 17.1.1 Organización de continuidad de seguridad de información 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información
	Defectos de causa física	Piezas deficientes de fábrica		
	Defectos de causa física	Presencia de basura		
	Defectos de causa física	Carencia de mantenimientos preventivos.		
	Catástrofes naturales	Carencia de plan antisísmico del edificio		11.1.3 Seguridad de oficinas, despachos y recursos. 11.1.4 Protección contra las amenazas externas y ambientales. 17.1.1 Organización de continuidad de seguridad de información. 17.1.2 Fijación de la continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de continuidad de seguridad de la información.
	Defectos de causa lógica	Contraseña del administrador compartida.		11.1.5 El trabajo en áreas seguras. 11.2.2 Instalaciones de suministro. 11.2.4 Mantenimiento de los equipos. 12.3.1 Copias de seguridad de la información. 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información. 17.1.1 Organización de continuidad de seguridad de información. 14.2.3 Revisión técnica de aplicaciones tras efectuar cambios en el sistema operativo.
	Defectos de causa lógica	Ingreso indebido		
	Caída de sistema por abuso de recursos	Carencia de límites y controles en utilizar recursos		11.2.4 Mantenimiento de los equipos. 12.1.2 Gestión de cambios. 12.1.3 Gestión de capacidades. 12.3.1 Copias de seguridad de la información. 15.1.1 Política de seguridad de la información para suministradores

Activo	Amenazas	Vulnerabilidad	Opción de tratamiento de riesgo	Controles o Salvaguardas de norma ISO/IEC 27001 (Control Vulnerabilidad)
Computador de escritorio y laptops	Catástrofes naturales	Carencia de plan antisísmico del edificio	Reducción	11.1.3 Seguridad de oficinas, despachos y recursos. 11.1.4 Protección contra las amenazas externas y ambientales. 17.1.1 Organización de continuidad de seguridad de información. 17.1.2 Fijación de la continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de continuidad de seguridad de la información.
	Defectos de causa física	Carencia de mantenimientos preventivos.		11.1.5 El trabajo en áreas seguras. 11.2.2 Instalaciones de suministro. 11.2.4 Mantenimiento de los equipos 12.3.1 Copias de seguridad de la información. 14.2.3 Revisión técnica de aplicaciones tras efectuar cambios en sistema operativo. 17.1.1 Organización de continuidad de seguridad de información 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información
	Defectos de causa física	Agotamiento natural de partes		
	Defectos de causa física	Partes defectuosas de fábrica		
	Defectos de causa física	Presencia de basura		
	Defectos de causa física	Contraseña del administrador compartida.		
	Defectos de causa física	Ingreso indebido		
	Caída de sistema por abuso de recursos	Carencia de límites y controles en utilizar recursos		11.2.4 Mantenimiento de los equipos. 12.1.2 Gestión de cambios. 12.1.3 Gestión de capacidades. 12.3.1 Copias de seguridad de la información. 15.1.1 Política de seguridad de la información para suministradores
	Acceso lógico intencional	Debilidad técnica en sistema operativo		9.1.1 Política de control de accesos. 9.1.2 Control de acceso a las redes y servicios asociados. 9.2.6 Retirada o adaptación de los derechos de acceso. 12.4.2 Protección de los registros de información.

Activo	Amenazas	Vulnerabilidad	Opción de tratamiento de riesgo	Controles o Salvaguardas de norma ISO/IEC 27001 (Control Vulnerabilidad)
Impresoras	Defectos de causa física	Agotamiento natural de partes	Reducción	11.1.5 El trabajo en áreas seguras. 11.2.2 Instalaciones de suministro. 11.2.4 Mantenimiento de los equipos 12.3.1 Copias de seguridad de la información. 14.2.3 Verificación técnica de aplicaciones luego tras alteración en sistema operativo. 17.1.1 Planificación de la continuidad de la seguridad de la información 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información
	Defectos de causa física	Partes defectuosas de fábrica		
	Caída, suspensión y negació de servicios y sistemas.	Agotamiento de recursos		11.2.4 Mantenimiento de los equipos. 12.1.2 Gestión de cambios. 12.1.3 Gestión de capacidades. 12.3.1 Copias de seguridad de la información. 15.1.1 Política de seguridad de la información para suministradores
	Abuso de privilegios de acceso	Carencia de revisiones continuas de privilegios de ingreso		9.1.1 Política de control de accesos 9.1.2 Control de acceso a las redes y servicios asociados. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 9.2.6 Retirada o adaptación de los derechos de acceso 9.4.1 Restricción del acceso a la información. 16.1.2 Notificación de los eventos de seguridad de la información.
Sistemas Pegasus y E-volution	Propagación de programas dañinos	Bases de datos de antivirus no actualizadas.		14.2.3 Verificación técnica de aplicaciones luego tras alteración en sistema operativo. 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas. 14.2.9 Pruebas de aceptación. 16.1.7 Recopilación de evidencias.
	Exceso de privilegios de ingresos	Carencia de revisiones continuas de privilegios de ingreso		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. 9.3.1 Uso de información confidencial para la autenticación. 9.4.2 Procedimientos seguros de inicio de sesión. 9.4.4 Uso de herramientas de administración de sistemas. 12.4.2 Protección de los registros de información. 16.1.2 Notificación de los eventos de seguridad de la información.

Activo	Amenazas	Vulnerabilidad	Opción de tratamiento de riesgo	Controles o Salvaguardas de norma ISO/IEC 27001 (Control Vulnerabilidad)
Software ACL	Exceso de privilegios de ingresos	Carencia de revisiones continuas de privilegios de ingreso	Reducción	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. 9.3.1 Uso de información confidencial para la autenticación. 9.4.2 Procedimientos seguros de inicio de sesión. 9.4.4 Uso de herramientas de administración de sistemas. 12.4.2 Protección de los registros de información. 16.1.2 Notificación de los eventos de seguridad de la información.
Red LAN Y WAN	Defectos de causa física	Desgaste natural de partes		11.1.5 El trabajo en áreas seguras. 11.2.2 Instalaciones de suministro. 11.2.4 Mantenimiento de los equipos 12.3.1 Copias de seguridad de la información. 14.2.3 Revisión técnica de aplicaciones tras efectuar cambios en sistema operativo. 17.1.1 Organización de continuidad de seguridad de información 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información
	Defectos de causa física	Partes deficientes de fábrica		
	Caída, suspensión y negación de servicios y sistemas.	Agotamiento de recursos		9.1.1 Política de control de accesos. 9.2.4 Gestión de información confidencial de autenticación de usuarios. 12.3.1 Copias de seguridad de la información. 16.1.5 Respuesta a los incidentes de seguridad.
	Exceso de privilegios de ingresos	Carencia de revisiones continuas de privilegios de ingreso		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. 9.3.1 Uso de información confidencial para la autenticación. 9.4.2 Procedimientos seguros de inicio de sesión. 9.4.4 Uso de herramientas de administración de sistemas. 12.4.2 Protección de los registros de información. 16.1.2 Notificación de los eventos de seguridad de la información.

Activo	Amenazas	Vulnerabilidad	Opción de tratamiento de riesgo	Controles o Salvaguardas de norma ISO/IEC 27001 (Control Vulnerabilidad)
Sistema de Telefonía IP	Defectos de causa física	Desgaste natural de partes	Reducción	11.1.5 El trabajo en áreas seguras. 11.2.2 Instalaciones de suministro. 11.2.4 Mantenimiento de los equipos 12.3.1 Copias de seguridad de la información. 14.2.3 Verificación técnica de aplicaciones tras efectuar cambios en sistema operativo. 17.1.1 Organización de continuidad de seguridad de información 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información
	Defectos de causa física	Partes deficientes de fábrica		
	Caída, suspensión y negación de servicios y sistemas.	Agotamiento de recursos		9.1.1 Política de control de accesos. 9.2.4 Gestión de información confidencial de autenticación de usuarios. 12.3.1 Copias de seguridad de la información. 16.1.5 Respuesta a los incidentes de seguridad.
	Exceso de privilegios de ingresos	Carencia de revisiones continuas de privilegios de ingreso		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. 9.3.1 Uso de información confidencial para la autenticación. 9.4.2 Procedimientos seguros de inicio de sesión. 9.4.4 Uso de herramientas de administración de sistemas. 12.4.2 Protección de los registros de información. 16.1.2 Notificación de los eventos de seguridad de la información.

Activo	Amenazas	Vulnerabilidad	Opción de tratamiento de riesgo	Controles o Salvaguardas de norma ISO/IEC 27001 (Control Vulnerabilidad)
Servicio de e-mail	Utilización no prevista	Confusión de usuarios	Reducción	9.1.1 Política de control de accesos.
	Caída, suspensión y negación de servicios y sistemas.	Carencia de límites y controles en utilizar recursos		9.1.1 Política de control de accesos. 9.2.4 Gestión de información confidencial de autenticación de usuarios. 12.3.1 Copias de seguridad de la información. 16.1.5 Respuesta a los incidentes de seguridad.
	Fuga de información	Carencia de control de contenidos transmitidos en la red		9.4.1 Restricción del acceso a la información. 12.4.2 Protección de los registros de información 16.1.2 Notificación de los eventos de seguridad de la información
	Acceso lógico intencional	Debilidad técnica en el sistema		9.1.1 Política de control de accesos. 9.1.2 Control de acceso a las redes y servicios asociados. 9.2.6 Retirada o adaptación de los derechos de acceso. 12.4.2 Protección de los registros de información.
	Acceso lógico intencional	Sistema desactualizado		
	Caída, suspensión y negación de servicios y sistemas.	Agotamiento de recursos		9.1.1 Política de control de accesos. 9.2.4 Gestión de información confidencial de autenticación de usuarios. 12.3.1 Copias de seguridad de la información. 16.1.5 Respuesta a los incidentes de seguridad.
	Exceso de privilegios de ingresos	Carencia de revisiones continuas de privilegios de ingreso		9.1.1 Política de control de accesos. 9.2.4 Gestión de información confidencial de autenticación de usuarios. 12.3.1 Copias de seguridad de la información. 16.1.5 Respuesta a los incidentes de seguridad.
Sitio Web	Caída, suspensión y negación de servicios y sistemas.	Falta de límites y control en el uso de recursos		9.1.1 Política de control de accesos. 9.2.4 Gestión de información confidencial de autenticación de usuarios. 12.3.1 Copias de seguridad de la información. 16.1.5 Respuesta a los incidentes de seguridad.

Elaborado por: Investigador

h) Preparación de la declaración de aplicabilidad

Uno de los requerimientos de la norma ISO/IEC 27001:2013 es que la Universidad Técnica de Machala cuente con una declaración de la aplicabilidad, que consiste en un documento (Políticas de Seguridad-SGSI en Anexo 2) que involucre e identifique los controles del anexo 3 (Norma ISO/IEC 27002:2013) que se implementará y la justificación si está no se procede. Esto expresa que todos los controles predeterminados de la norma son aplicables a la Universidad Técnica de Machala y cualquier excepción debe ser justificada. La declaración de aplicabilidad esta verificada y admitida por el Jefe del Departamento de Tecnologías de la Información y Comunicación.

Tabla 36. Declaración de Aplicabilidad - Departamento de Tics.

Dominio	Objetivos de Control	Controles	Aplicabilidad		Justificación
			Si	No	
9. Control de acceso	9.1 Requisitos del negocio para el control de acceso	9.1.1 Política de control de accesos.	x		Se debe aplicar la seguridad en cuanto al acceso de los usuarios a los sistemas de información. Además, se necesita establecer seguridad en cuanto a la utilización limitada del software que podrían exceder al sistema y controles de aplicación.
		9.1.2 Control de acceso a las redes y servicios asociados.	x		
	9.2 Gestión de acceso a usuarios	9.2.1 Gestión de altas/bajas en el registro de usuarios.	x		
		9.2.2 Gestión de los derechos de acceso asignados a usuarios.	x		
		9.2.3 Gestión de los derechos de acceso con privilegios especiales.	x		
		9.2.4 Gestión de información confidencial de autenticación de usuarios.	x		
		9.2.6 Retirada o adaptación de los derechos de acceso	x		
	9.3 Responsabilidad del usuario	9.3.1 Uso de información confidencial para la autenticación.	x		
	9.4 Control de acceso a sistemas y aplicaciones.	9.4.1 Restricción del acceso a la información	x		
		9.4.2 Procedimientos seguros de inicio de sesión.	x		
		9.4.4 Uso de herramientas de administración de sistemas.	x		
11. Seguridad Física y Ambiental	11.1 Áreas seguras.	11.1.3 Seguridad de oficinas, despachos y recursos.	x		Se necesita llevar un control de seguridad en cuanto al acceso físico indebido, daño e interferencia al local y a la información.
		11.1.4 Protección contra las amenazas externas y ambientales.	x		
		11.1.5 El trabajo en áreas seguras.	x		
	11.2 Seguridad de los equipos.	11.2.2 Instalaciones de suministro.	x		
		11.2.4 Mantenimiento de los equipos	x		
12. Seguridad en la Operatividad	12.1 Responsabilidad y procedimientos de operación	12.1.2 Gestión de cambios.	x		Es fundamental preservar la seguridad de los programas e información del mismo previniendo oportunidades de filtraciones en la información.
		12.1.3 Gestión de capacidades.	x		
	12.3 Copias de seguridad.	12.3.1 Copias de seguridad de la información.	x		
	12.4 Registro de actividades y supervisión.	12.4.2 Protección de los registros de información.	x		

Dominio	Objetivos de Control	Controles	Aplicabilidad		Justificación
			Si	No	
14. Adquisición, desarrollo y mantenimiento de los sistemas.	14.2 Seguridad en los procesos de desarrollo y soporte.	14.2.3 Revisión técnica de aplicación tras efectuar cambios en sistema operativo.	x		Es fundamental preservar la seguridad de los programas e información del mismo previniendo oportunidades de filtraciones en la información
		14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.	x		
		14.2.9 Pruebas de aceptación.	x		
15. Relaciones con suministradores.	15.1 Seguridad de la información con los suministradores	15.1.1 Política de seguridad de la información para suministradores	x		Se sugiere ejecutar medidas de seguridad en cuanto a los medios externos porque a través de ellos se administra y procesa información.
16. Gestión de Incidentes en la seguridad de la información.	16.1 Administración de eventualidad de la seguridad de la información y mejoras.	16.1.2 Aviso de eventos de seguridad de la información.	x		Es fundamental preservar la seguridad de los programas e información del mismo previniendo oportunidades de filtraciones en la información
		16.1.5 Respuesta a los incidentes de seguridad.	x		
		16.1.7 Recopilación de evidencias.	x		
17. Aspectos de la seguridad de la información en la gestión de la continuidad del negocio.	17.1 Continuidad de la seguridad del negocio.	17.1.1 Organización de seguridad de información	x		Se requiere aplicar planes de continuidad comercial, se deben testear y ser actualizables constantemente para validar su efectivos.
		17.1.2 Fijación de continuidad de seguridad de la información	x		
		17.1.3 Verificación, revisión y evaluación de continuidad de seguridad de la información.	x		
	17.2 Redundancias.	17.2.1 Disponibilidad de instalaciones para el procesamiento de la información	x		

Elaborador por: Investigador

Revisado por: Ing. Jairo Jiménez (Jefe del Departamento de Tics)

6.7.2.2 FASE 2: Hacer (Implementar y Operar el SGSI)

Esta fase está constituida las siguientes etapas:

a. Definir plan de tratamiento del riesgo.
b. Implementar plan de tratamiento de riesgos.
c. Implementar los controles.
d. Definir un sistema de métricas.
e. Formar y concienciar.
f. Gestionar recursos del SGSI.
g. Implantar procedimientos y controles.

a) Plan de tratamiento de riesgos.

Un plan de tratamiento de riesgos obliga a la implantación en la Universidad Técnica de Machala de un conjunto de controles de seguridad con la finalidad de mitigar los riesgos no asumidos por el rectorado.

b) Implementar el plan de tratamiento de riesgo, para lograr los objetivos de los controles identificados.

El Departamento de Tics de la Universidad Técnica de Machala es encargado de implantar y velar por el cumplimiento de políticas. Además, se encarga de valorar, adquirir e implantar productos de seguridad informática, y ejecutar acciones para garantizar un entorno informático adecuado. También se preocupa de suministrar ayuda técnica y administrativa en los temas relacionados con seguridad, casos de contagio de virus, ataque de hackers, robos y otros incidentes.

c) Implementar los controles seleccionados (Seleccionados del Anexo 3)

A continuación, detallaremos la implementación de los controles seleccionados, para este caso de investigación resultaron 7 Dominios, 14 objetivos y 34 controles:

Dominio 1:

9. Control de acceso

Las normas de control del acceso y derechos para los usuarios se deben definir en la política de control de acceso. Los controles de acceso son lógicos como físicos.

La política debe incorporar:

- Requerimientos de seguridad de aplicaciones institucionales individuales;
- Identificar la información asociada con aplicaciones institucionales y riesgos que enfrenta la información;
- Consistencia entre controles de acceso y políticas de clasificación de información de diferentes sistemas y redes;
- Perfiles de acceso de usuario para función de trabajo en la Universidad Técnica de Machala;
- Gestionar derechos de acceso en ambiente distribuido y en red que reconoce los tipos de conexiones disponibles;
- Separación de funciones del control del acceso.
- Condicionamiento para autorización de solicitudes de acceso;
- Condicionamiento para revisión de controles de acceso
- Anular derechos de acceso.

Objetivo 1:

9.1 Requisitos del negocio para el control de acceso.

Prevenir violaciones de seguridad como es el caso de claves facilitadas para ingresos críticos a la base de datos o accesibilidad física denegada al área de equipos.

El encargado del ambiente de producción debe ejecutar una revisión mensual de usuarios del sistema, corroborando que hallan solo usuarios necesarios y que sus permisos sean adecuados. Las normas de contraseñas listada van acorde a las condiciones y normativas internacionales.

La confidencialidad no definida de información puede ocasionar vacíos para asignar accesos.

Se tiene que definir contraseñas de acceso a nivel de información.

Contraseñas

La contraseña de chequeo de identidad no debe muy fácil de descifrar, debe incluir parámetros tales como:

- Al menos 8 caracteres de longitud.
- Una unión de caracteres alfabéticos y no alfabéticos.
- No tener un usuario ID como parte de contraseña.
- Sistemas y aplicaciones que tengan información secreta, necesitan modificaciones de contraseña cada 3 meses.

Objetivo 2:

9.2 Gestión de acceso a usuarios

Incluir los siguientes parámetros:

- Condicionar a los usuarios para firmen un documento para asegurar confidenciales las contraseñas secretas.
- Establecer procedimientos para revisar la identidad de usuario antes de suministrar clave secreta nueva;
- Claves secretas temporales deben ser suministradas a usuarios de forma segura.
- Claves secretas temporales deben ser únicas para la persona
- Usuarios deben conocer la recepción de claves secretas;
- Claves secretas nunca deben almacenarse en sistemas de cómputo.
- Claves secretas predefinidas por el vendedor deben ser modificada después de la instalación.

Revisión de los derechos de acceso del usuario

Debe considerar los siguientes parámetros:

- Derechos de ingreso de usuarios deben ser chequeados por unidad de talento humano.
- Derechos de acceso de usuario se deben revisar y re-asignar cuando se traslada de un empleo a otro dentro de la misma Universidad Técnica de Machala;
- Autorizaciones para derechos de acceso privilegiados.
- Revisar la designación de privilegios a intervalos regulares para mantener que no se hayan obtenido privilegios indebidos;
- Registrar cambios en cuentas privilegiadas para un chequeo periódico.

Objetivo 3:

9.3 Responsabilidad del usuario.

Los usuarios deben saber de las condiciones de seguridad y procedimientos para proteger el equipo desatendido, responsabilidades para implementar dicha protección. Se debe comunicar a los usuarios lo siguiente:

- Cerrar sesiones activas cuando se concluye
- Salir de computadoras mainframe, servidores y computadoras de oficina cuando se termina la sesión.
- Asegurar los equipos contra la utilización no autorizado por medio de un seguro con clave

Objetivo 4:

9.4 Control de acceso a sistemas y aplicaciones.

Se debe considerar los siguientes lineamientos:

- Uso de procedimientos de identificación, autenticación y autorización para utilidades del sistema;
- Separación de utilidades del sistema, software de aplicación;

- Limitar el uso de utilidades del sistema a un número mínimo de usuarios.
- Autorizar el uso de facilidades con un propósito concreto.
- Limitar la disponibilidad de utilidades del sistema.
- Registrar uso de utilidades del sistema;
- Definir y documentar niveles de autorización de utilidades del sistema;
- Eliminar las utilidades no necesarias sustentadas en software.

Las denegaciones de acceso deben estar sustentadas en condiciones específicas de la aplicación y consistente con la política de acceso a la información de la Universidad Técnica de Machala.
Se debe considerar lo siguiente para ayudar a los requisitos de restricciones de ingreso:

- Establecer menús para controlar accesos a funciones del sistema de aplicaciones;
- Controlar derechos de acceso de usuarios.
- Controlar derechos de acceso de otras aplicaciones;
- Asegurar las salidas de sistemas de aplicación que procesan información sensible.

Dominio 2:

11. Seguridad Física y Ambiental

Se debe aplicar protección física contra desastres naturales. También hay que considerar los siguientes parámetros para prevenir los desastres naturales:

- Los materiales amenazantes deben ser guardados a una distancia segura.
- Los medios de respaldo tienen que localizarse a una distancia segura.

- Se debe suministrar equipos contra-incendios localizados convenientemente.

Objetivo 5.

11.1 Trabajo en áreas aseguradas

Se tiene que aplicar la protección física y los parámetros para trabajar en áreas aseguradas. Se debe tener en cuenta los siguientes lineamientos:

- El personal debe estar de las acciones dentro del área asegurada sólo conforme las necesite conocer;
- Prevenir el trabajo no-supervisado en el área asegurada para prevenir las ocasiones para acciones maliciosos;
- Las áreas aseguradas deben ser cerradas físicamente.

- No permitir equipos o dispositivos que no estén autorizados;
- Considerar el tema que equipos asegurados con una empresa.

Objetivo 6:

11.2 Seguridad de los equipos.

Protección contra amenazas externas e internas

Se debe aplicar protección física contra desastres naturales.

También hay que considerar los siguientes parámetros para prevenir los desastres naturales:

- Los materiales amenazantes deben ser guardados a una distancia segura.
- Los medios de respaldo tienen que localizarse a una distancia segura.
- Suministrar equipos contra-incendios localizados convenientemente.

Trabajo en áreas aseguradas

Se tiene que aplicar la protección física y los parámetros para trabajar en áreas aseguradas. Se debe tener en cuenta los siguientes lineamientos:

- El personal debe estar de las acciones dentro del área asegurada sólo conforme las necesite conocer;
- Prevenir el trabajo no-supervisado en el área asegurada para prevenir las ocasiones para acciones maliciosos;
- Las áreas aseguradas deben ser cerradas físicamente.
- No permitir equipos o dispositivos que no estén autorizados;
- Considerar el tema que equipos asegurados con una empresa.

Dominio 3:

12. Seguridad en la Operatividad

Incluir los siguientes parámetros:

- Requerir que usuarios firmen un enunciado para mantener confidenciales las claves secretas.
- Establecer procedimientos para revisar la identidad de usuario antes de suministrar clave secreta nueva;
- Claves secretas temporales deben ser suministradas a usuarios de forma segura.
- Claves secretas temporales deben ser únicas para la persona
- Usuarios deben conocer la recepción de claves secretas;
- Claves secretas nunca deben almacenarse en sistemas de cómputo.
- Claves secretas predefinidas por el vendedor deben ser modificada después de la instalación.

Revisión de los derechos de acceso del usuario

Debe considerar los siguientes parámetros:

- Derechos de ingreso de usuarios deben ser chequeados por unidad de talento humano.
- Derechos de acceso de usuario se deben revisar y re-asignar cuando se traslada de un empleo a otro dentro de la misma Universidad Técnica de Machala;
- Autorizaciones para derechos de acceso privilegiados.
- Revisar la designación de privilegios a intervalos regulares para mantener que no se hayan obtenido privilegios indebidos;
- Registrar cambios en cuentas privilegiadas para un chequeo periódico.

Objetivo 7:

12.1 Responsabilidad y procedimientos de operación

Se debe definir procedimientos de manipulación y almacenamiento de información de forma adecuada a su clasificación. Los siguientes parámetros deben ser tomarse en cuenta:

- Etiquetado en administración de los medios;
- Restricción de acceso para identificar personal no autorizado;
- Mantener registros formales de recipientes autorizados de datos;
- Asegurar de los datos de entrada, su proceso y la validación de salida sean completos;
- Proteger los datos que están en cola para su salida de acuerdo con su criticidad;
- Almacenar los medios en un ambiente de acuerdo a las especificaciones del fabricante;
- Reducir distribución de datos;
- Identificar las copias de datos para su atención por el receptor autorizado;

Objetivo 8:

12.3 Copias de seguridad.

Para reducir el riesgo de corrupción se debe tomar en cuenta lo siguiente:

- Actualización del software operacional, aplicaciones y bibliotecas de programas únicamente debe ser realizada por administradores.

- Sistemas operacionales únicamente deben mantener códigos ejecutables aprobados, y no códigos de desarrollo o compiladores;

- No se debe implantar código ejecutable en un sistema operativo mientras no se tenga evidencia del éxito de las pruebas.

- Utilizar un sistema de control de configuración para asegurar un control de todo el software implementado;

- Asegurar un registro de auditoría de las actualizaciones a las librerías de programas en producción;

- Las versiones anteriores de software deben ser archivadas junto con toda la información requerida.

Objetivo 9:

12.4 Registro de actividades y supervisión

Se debe monitorear los sistemas y registrar los sucesos de seguridad de la información. Los registros de operador y actividad de registro de errores se deben usar para asegurar la identificación de problemas del sistema de información. Se sugiere ejecutar el monitoreo del sistema para corroborar la eficiencia de controles adoptados y chequear el cumplimiento de un modelo de política de acceso.

Uso del sistema de monitoreo.

Se necesita el uso de procedimientos de monitoreo para asegurar que los usuarios estén ejecutando acciones para las cuales han sido autorizados.

Las áreas que se deben considerar incorporan:

Acceso autorizado, incorporando pormenores tales como:

- ID de usuario;
- Fecha y hora de sucesos claves;
- Tipos de sucesos;
- Archivo a quienes se acceso;
- Programas/utilidades usados;

Operaciones privilegiadas:

- Uso de cuentas privilegiada.
- Inicio y apagado de sistema;

Intentos de acceso indebidos:

- Ingreso de usuario denegadas;
- Acciones denegadas que implican datos;
- Violaciones a política de acceso y firewalls de la red;
- Alertas de sistemas de detección de intrusiones;

Errores del sistema como:

- Alertas en la consola;
- Alarmas de gestión de la red;
- Alarmas activadas por sistema de control de acceso;
- Cambios en controles del sistema de seguridad.

La continuidad con que se revisan resultados de actividades de monitoreo dependerá de los riesgos implicados. Los factores de riesgo a considerarse incorporan:

- Grado crítico de procesos de aplicación;
- Valor, sensibilidad y grado crítico de información involucrada;
- Antecedentes de infiltración y uso indebido del sistema, y la continuidad con la que se explotan vulnerabilidades;
- Extensión de interconexión del sistema.

Protección del registro de información

Los controles deben tener la finalidad de proteger contra modificaciones indebidas y errores operacionales, y el medio de registro debe incorporar:

- Modificaciones registradas a tipos de mensajes;
- Archivos de registro que se modifiquen;

Registro de fallas

Deben incorporar;

- Hora a la cual sucede un sucedo.
- Información acerca del suceso
- Que procesos están implicados.

Dominio 4:

14. Adquisición, desarrollo y mantenimiento de los sistemas

Objetivo 10:

14.2 Seguridad en los procesos de desarrollo y soporte.

Se debe considerar los siguientes parámetros:

- Escanear el flujo de salida de medios y comunicaciones en busca de información escondida;
- Enmascarar y modular la conducta del sistema y comunicaciones para restar la probabilidad que terceras personas puedan deducir la información a partir de dicha conducta;

- Usar sistemas y software considerados de alta integridad
- Chequeo de actividades del personal y del sistema
- Chequeo del uso de recursos en sistemas de cómputo.

Dominio 5:

15. Relaciones con suministradores

Objetivo 11:

15.1 Seguridad de la información con los suministradores

Para promover la seguridad de información se tiene que mantener recursos el sistema de información de la Universidad Técnica de Machala, y estos sean usados de forma como se planeó.

Haber un compromiso del rectorado con la seguridad de la información, coordinación de la seguridad de información, para medios de procesamiento de información, pactos de confidencialidad, contacto con otras autoridades, y chequeo autónomo de seguridad de la información.

Organización interna.

Objetivo: Manejar la seguridad de información internamente.

Establecer un área referencial de rectorado para empezar y controlar la implementación de seguridad de información dentro de la Universidad Técnica de Machala. El rectorado debe aprobar la política de seguridad de información, designar funciones de seguridad y chequear la implementación de la seguridad en toda la Universidad Técnica de Machala.

Chequeo independiente de seguridad de información.

- Se tiene que chequear la orientación del departamento de Tics para controlar la seguridad de información y su implementación de manera autónoma a intervalos planeados.

- Este chequeo autónomo es necesario para mantener la orientación del departamento de Tics para gestionar la seguridad de la información. El chequeo debe incorporar las oportunidades de evaluación para mejorar y la necesidad de cambios, incorporando políticas y objetivos de control.

- Si el chequeo autónomo señala que la orientación y la implementación del departamento de Tics de la Universidad Técnica de Machala para manejar la seguridad de información no van acorde con la dirección de seguridad de información determinada en el documento de política de seguridad de información, el rectorado debe considerar acciones correctivas.

Instituciones externas

Objetivo: Asegurar la seguridad de información y los medios de procesamiento de información de la Universidad Técnica de Machala que son ingresados, procesados, comunicados y manejados por grupos ajenos a la institución.

La seguridad de información y los medios de procesamiento de información de la Universidad Técnica de Machala no deberían ser disminuidos por el ingreso de productos y servicios de grupos ajenos a la institución.

Se debe monitorear cualquier ingreso a medios de procesamiento de información de la Universidad Técnica de Machala y el procesamiento y comunicación de información ejecutado por grupos ajenos a la institución.

Identificación de los riesgos relacionados con los grupos externos

- Se debe señalar riesgos para la información y los medios de procesamiento de información de la Universidad Técnica de Machala a raíz de procesos institucionales que impliquen a grupos ajenos a la institución. y se deberá implementar controles adecuados antes de otorgarles acceso.

- Donde se requiera la necesidad de permitir que un grupo ajenos a la institución tenga acceso a los medios de procesamiento de información de la Universidad Técnica de Machala, se deberá ejecutar una evaluación del riesgo para identificar cualquier condición de controles determinados.

- No facilitar acceso a grupos ajenos a la institución a la información de la Universidad Técnica de Machala hasta que se hayan implementado los controles adecuados y cuando se haya firmado un acuerdo definiendo términos y requerimientos para el contrato de trabajo.

Se debe asegurar que el grupo ajenos a la institución acepte responsabilidades implicadas en el acceso de los medios de procesamiento de información de la Universidad Técnica de Machala.

Tratamiento de seguridad cuando se trata con personas ajenas a la institución.

- Se debe asumir las condiciones de seguridad señaladas previo a proporcionar a personas ajenos a la institución la información de la Universidad Técnica de Machala.

- Se debe considerar los términos de seguridad previo a facilitar a personas ajenos a la institución ingreso a cualquier activo de la Universidad Técnica de Machala:

1. Protección de activos, incorporando:
    - Procedimientos para proteger activos de la Universidad Técnica de Machala, incorporando información, software y control de vulnerabilidades identificadas;
    - Procedimientos para establecer si ha sucedido aumentos de riesgo de activos;
    - Denegaciones acerca de copias de datos;
2. Los requerimientos y beneficios para el ingreso de usuario;
3. Política de control de acceso;
4. Para el reporte de imprecisiones de información.
5. Derecho a chequear cualquier acción asociada con activos de la UTMACH;
6. Las obligaciones de la UTMACH y los usuarios;
7. Responsabilidades con temas legales y cómo mantener que se lleven a cabo las condiciones legales

Las condiciones de seguridad asociadas al ingreso de usuario a los activos o de la institución pueden cambiar dependiendo de medios de procesamiento de información a la cual se puede acceder.

Dominio 6:

16. Administración de eventualidad de la seguridad de la información y mejoras.

Se debe establecer y documentar funciones y responsabilidades de seguridad de empleados, contratistas y terceros de acuerdo con la política de seguridad de la información. Considerando el manual de funciones existente que detalla las funciones de cada cargo.

Las funciones y responsabilidades deben incorporar condiciones para:

- Implementar y actuar de acuerdo con políticas de seguridad de información del departamento de Tics de la Universidad Técnica de Machala;
- Proteger activos contra el ingreso no autorizado;
- Asegurar que se denomine al responsable por las actividades tomadas.
- Reportar sucesos de seguridad para la Universidad Técnica de Machala.
- Se debe tener en cuenta el asunto de días y horarios de ingresos.

Objetivo 12:

16.1 Gestión de incidentes de la seguridad de la información y mejoras.

El rector debe asegurar que las condiciones y criterios de aceptación de los sistemas nuevos estén establecidos, aceptados, documentados y probados. Los sistemas de información nuevos, las actualizaciones y las versiones nuevas deben migrar a la producción luego de obtener la aceptación. Se debe tomar en cuenta los siguientes elementos previo a la aceptación:

- Condiciones de rendimiento y capacidad de computadores;
- Procedimientos de recuperación de errores y reinicio, planes de contingencia;
- Preparación y prueba de procedimientos operativos de rutina según normas establecidas;
- Conjunto acordado de controles y medidas de seguridad instalados;
- Manual de procedimientos eficiente;
- Arreglos para la continuidad de la Universidad Técnica de Machala;
- Evidencia que la instalación del sistema nuevo no afectará sistemas existentes.
- Evidenciar que se considere el efecto del sistema nuevo en la seguridad general de la Universidad Técnica de Machala;
- Capacitación para la operación o aplicación de los sistemas nuevos;
- Facilidad de utilización, ya que afecta el desempeño del usuario y previene el error humano.

Para los programadores nuevos es importante, la función de operaciones y los usuarios deben ser consultados en todas las etapas del proceso del desarrollo para mantener la eficacia operacional del diseño del sistema propuesto. Se debe realizar los test apropiados para confirmar que se ha cumplido con el criterio de aceptación.

Dominio 7:

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

Las pruebas de planes de continuidad de la Universidad Técnica de Machala deben asegurar que los miembros del equipo de recuperación y otro personal relevante están prevenidos de planes y sus responsabilidades para la continuidad de la Universidad Técnica de Machala y la seguridad de información.

Objetivo 13:

17.1 Continuidad de la seguridad del negocio.

Se debe realizar un calendario de pruebas para plan(es) de continuidad de la Universidad Técnica de Machala, en el cual se debe identificar cómo, cuándo probar cada etapa del plan. Se recomienda probar los componentes individuales del plan con frecuencia.

Se debe usar diversos métodos para suministrar la seguridad que los planes funcionarán en la vida real. Estas deberían incluir:

- Prueba sobre el papel de varios escenarios (evaluando disposiciones de recuperación de la institución con ayuda de ejemplos de interrupciones);
- Simulaciones (para entrenar al personal que gestione la crisis tras la contingencia);
- Pruebas de recuperación técnica (asegurando que los sistemas de información pueden restaurarse con efectividad);
- Pruebas de recuperación en un lugar alternativo (haciendo funcionar los procesos de la U Universidad Técnica de Machala en paralelo con las operaciones de recuperación fuera del lugar principal,
- Las pruebas de recursos y servicios del proveedor.
- Ensayos completos (probando que pueden hacer frente a interrupciones de la Universidad Técnica de Machala, el personal, los recursos y los procesos);
- Documento de pruebas realizadas con conclusiones y recomendaciones.

Objetivo 14:

17.2 Redundancias.

Se debe designar responsabilidades para revisar regularmente cada plan de continuidad. Se debe hacer una actualización apropiada del plan tras la identificación de modificaciones en las características de la Universidad Técnica de Machala no reflejadas en los planes de continuidad. Este proceso de control de cambios debe asegurar que las revisiones del plan completo ayuden a mejorar y distribuir los planes actualizados.

Ejemplos de situaciones que necesitarían la actualización de planes: la adquisición de nuevos equipos o la mejora de los sistemas operativos con cambios en:

- El personal;
- Direcciones o números de teléfono;
- Estrategias de la Universidad Técnica de Machala;
- Lugares, dispositivos y recursos;
- Legislación;
- Contratistas, proveedores y usuarios principales;
- Procesos existentes, nuevos y usuarios principales;
- Riesgos (operativos o financieros).

d) Definir un sistema de métricas (Efectividad de los controles seleccionados)

Tabla 37. Métricas de la ISO 27001 para el departamento de Tics.

Ref.	Objetivo	Actividades	Posibles Métricas
9.	CONTROL DE ACCESO		
9.1	Requisitos del negocio para el control de acceso	• Chequear manual de políticas y procedimientos. • Chequear la utilización y funcionamiento de activos de información	Porcentaje de sistemas y aplicaciones institucionales para los que los "propietarios" adecuados sean: a) Notificados, (mínimo 85% inicialmente) b) Aceptada sus responsabilidades, (mínimo 75% inicialmente) c) Ejecutado – revisar accesos y seguridad de aplicaciones, sustentadas en riesgo y (mínimo 85% inicialmente) d) Establecer normas de control de ingreso sustentada en asignaciones. (mínimo 90% inicialmente)
9.2	Gestión de acceso a usuarios	• Chequear manual de procedimientos y políticas definidos, para asegurar que se cumplan con normalidad. • Chequeos trimestrales acerca de los ingresos privilegiados de usuarios. • Chequear y asegurar el ciclo de vida de acceso de usuarios: - Registro de usuarios - Gestión de privilegios - Gestión de las contraseñas - Chequeo de los derechos. -	Tiempo transcurrido entre petición y ejecución de peticiones de modificación de ingreso 72 horas Número de solicitudes de modificación de ingreso realizadas en el mes, 35 solicitudes de cambio promedio al mes.

Ref.	Objetivo	Actividades	Posibles Métricas
9.	CONTROL DE ACCESO		
9.3	Responsabilidad del usuario	• Chequear el plan de concientización de la información. • Comunicar a usuarios de activos acerca de las responsabilidades que tienen los computadores desatendidos.	Porcentaje de descripciones de funciones de trabajo que incorporan responsabilidades en seguridad de información: Documentada y aceptada. (mínimo 85% de las descripciones de puesto deben involucrar responsabilidades de seguridad)
9.4	Control de acceso a sistemas y aplicaciones.	• Chequear el manual de procedimientos y políticas de seguridades físicas y lógicas. • Chequear archivos logs del sistema biométrico • Definir controles de seguridad informática.	Porcentaje de plataformas conformes con normas de seguridad con anotaciones sobre los sistemas no conformes (mínimo 75% inicialmente)
11.	SEGURIDAD FÍSICA Y AMBIENTAL		
11.1	Áreas seguras.	• Dos chequeos anuales para revisar la seguridad física de instalaciones, incluyendo actualizaciones del estado de medidas correctivas identificadas en inspecciones anteriores que aún estén en espera. • Chequear archivos logs de los medios biométricos.	Datos de inspecciones de seguridad física de instalaciones, incorporando controles correctivos identificados en inspecciones anteriores. Aceptable un 90% mínimo inicialmente
11,2	Seguridad de los equipos.	• Realizar una verificación mensual por muestreo, para revisar el estado y funcionamiento de equipos. • Chequear manual de políticas y procedimientos de seguridades físicas y lógicas. • Ejecutar mantenimiento a equipos de forma trimestral. • Revisar planes de contingencia	Porcentaje de chequeos que demuestren movimientos indebidos de equipos. Máximo un 5% de chequeos con movimientos no autorizados

Ref.	Objetivo	Actividades	Posibles Métricas
12.	SEGURIDAD EN LA OPERATIVIDAD		
12.1.	Responsabilidad y procedimientos de operación	• Chequeo del enfoque del departamento para manejar la seguridad de información y su implementación de forma independiente cada tres meses. • Asignación de funciones y responsabilidades de seguridad de información a empleados del departamento	Porcentaje de asignaciones implantando un mecanismo para asegurar riesgos de seguridad de información. Porcentaje de empleados que han: Asumido funciones y responsabilidades de seguridad de información. Aceptable un 80% mínimo inicialmente
12.3	Copias de seguridad	• Realizar soportes encriptados de backup de información. • Chequeo de privilegios de usuarios de sistemas de información. • Concientizar a los empleados del departamento acerca de seguridad de información	Porcentaje de apoyo de respaldos de datos. 55% de archivos encriptados inicialmente
12.4	Registro de actividades y supervisión	• Chequear las operaciones privilegiadas • Registro de intentos indebidos. • Ejecutar revisiones periódicas y procedimientos de monitorización del uso de sistemas.	Porcentaje de sistemas cuyos logs de seguridad: a) Configurados, (mínimo 65% inicialmente) b) Revisados (mínimo 60% inicialmente)
14.	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS		
14.2	Seguridad en los procesos de desarrollo y soporte.	• Desarrollar procedimiento de control de modificaciones. • Ejecución de revisiones técnicas a aplicaciones después de realizar modificaciones, teniendo presente las aplicaciones críticas. • Documentar las restricciones en los cambios de paquetes de software. • Implementar medidas para prevenir robos de información. • Supervisión y chequeo de desarrollos de software externalizado. • Gestión técnica de vulnerabilidades	"Modo de seguridad en sistemas en proceso", o sea, Datos sobre el estado de seguridad en procesos de desarrollo de software, con informes sobre incidentes actuales, vulnerabilidades de seguridad y pronósticos de riesgos. (Se encuentran establecidas políticas de evaluación de sistemas de desarrollo, se debe evaluar el 90% de sistemas en proceso arrojando incidentes en máximo el 10%)

Ref.	Objetivo	Actividades	Posibles Métricas
15.	RELACIONES CON SUMINISTRADORES		
15.1	Seguridad de la información con los suministradores	• Chequear planes de contingencia para continuidad de la institución • Prueba, mantenimiento y re-valoración de planes de continuidad institucional.	Porcentaje de planes de continuidad de la institución en fases del ciclo de vida. (mínimo 75% de fases del ciclo de vida deben tener planes de contingencia) Porcentaje de unidades organizativas con planes de continuidad de la institución: a) Documentados y (mínimo 70% inicialmente) (b) Admitidas por medio de pruebas en 1 año. (mínimo 70% inicialmente)
16.	GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.		
16.1	Gestión de incidentes de la seguridad de la información y mejoras	• Chequear y determinar incidentes de seguridad de red identificados. • Designar controles para prevenir incidentes de seguridad • Chequear, hallar, registrar, y cumplir políticas de la institución.	Número de imprevistos de seguridad de red identificados en mes previo, dividido por niveles, con análisis y descripción Máximo 8 incidentes leves 3 importantes 0 graves
17.	ASPECTOS DE LA SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.		
17.1	Continuidad de la seguridad del negocio.	• Chequear planes de contingencia para la continuidad del negocio. • Prueba, mantenimiento y re-valoración de planes de continuidad organizacional	Porcentaje de planes de continuidad de la institución en cada una de las fases del ciclo de vida. (mínimo 75% de las fases del ciclo de vida tienen que contener planes de contingencia) Porcentaje de departamentos organizados con planes de continuidad de la institución que han sido convenientemente: a) Documentados y (mínimo 75% inicialmente) b) Admitidos en un año. (mínimo 75% inicialmente)

Ref.	Objetivo	Actividades	Posibles Métricas
17.	ASPECTOS DE LA SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.		
17.2	Redundancias.	• Chequear las condiciones de rendimiento y capacidad de equipos. • Mantener al día los manuales de procedimientos de los sistemas. • Definir controles para monitorear el análisis de riesgos ejecutados y valorar activos y considerar cambios para mantener la seguridad de información. • Desarrollar criterios de asumir nuevos sistemas, y versiones que deban implantarse.	• Chequear las condiciones de rendimiento y capacidad de los equipos. • Mantener al día manuales de procedimientos de sistemas. • Definir controles para chequear análisis de riesgos ejecutado y evaluar activos y considerar mejoras para asegurar la seguridad de información. • Elaborar criterios de admisión de nuevos sistemas que deban ser implantados.

Elaborado por: Investigador

Revisado por: Ing. Jairo Jiménez (Jefe del Departamento de Tics)

e) Formar y Concienciar (Implementar programas de capacitación y conocimiento)

El departamento de Tics de la Universidad Técnica de Machala debe asegurar que todo el personal sea competente para realizar las tareas requeridas para:

- Proporcionar capacitación.
- Evaluar efectividad de las acciones tomadas;
- Mantener registros de educación, capacitación, capacidades, experiencia y calificaciones (Se deben establecer registros para proporcionar evidencia de conformidad con requerimientos y operación efectiva del SGSI.

  El SGSI debe considerar cualquier condición legal. Los registros deben mantenerse legibles, identificables y recuperables. Se debe documentar e implementar controles para proteger y recuperar los registros. Se deben mantener registros del desempeño del proceso y de las ocurrencias de incidentes de seguridad relacionados con el SGSI.).

  El departamento de Tics de la Universidad Técnica de Machala también debe asegurarse que el personal relevante esté consciente sus actividades y cómo ellos pueden contribuir al logro de los objetivos SGSI.

f) Gestionar recursos del SGSI

Los recursos que constituyen el SGSI es el personal del Departamento de Tics de la Universidad Técnica de Machala (Jefe de Sistemas, Programadores, Administrador de Sistemas, y el Ayudante del Administrador de Sistemas) quienes son los responsables de velar por la seguridad de sistemas de información y comunicación que existen en el departamento, de Tics, así como también mantener los servicios que brindan.

g) Implementar procedimientos y controles, capaces de permitir una pronta detección y respuesta a incidentes de seguridad.

Existen varias formas de responder a un incidente de seguridad. Los siguientes pasos han sido formulados en función de cómo reaccionar desde el momento en el que se anuncia un incidente de seguridad, mientras está ocurriendo y una vez ha terminado.

Paso 1: Informar sobre el incidente.

¿Qué ocurre/ha pasado? (intentar concentrarse en los hechos). ¿Dónde y cuándo sucedió? ¿Quién está involucrado? (en caso de determinarlo) ¿La persona o propiedad ha sufrido algún tipo de daño?

Paso 2. Decidir cuándo reaccionar. Hay 3 posibilidades:

- Una reacción inmediata es necesaria cuando hay que atender a personas heridas o frenar un ataque en marcha.
- Reaccionar inmediatamente es necesaria cuando hay que evitar que surjan nuevos.
- Acción de seguimiento, si la situación se ha estabilizado, tal vez no resulte necesaria una reacción ni inmediata ni rápida, sino de seguimiento.

Además, cualquier incidente de seguridad que haya requerido una reacción inmediata o rápida deberá someterse a observación por medio de una actividad de seguimiento para conservar nuestro espacio de trabajo.

Paso 3. Decidir cómo reaccionar y cuáles son tus objetivos.

Si la reacción debe ser inmediata, los objetivos son precisos: Frenar el ataque.

Si la reacción debe ser rápida, los objetivos deberán ser implantados por la persona encargada y deberá centrarse en restaurar la seguridad necesaria para los afectados por el percance.

Las acciones luego se llevarán a cabo siguiendo vías habituales de la UTMACH en la toma de decisiones, con el objetivo de restaurar un ambiente de trabajo seguro, así como de re-establecer procedimientos organizativos internos.

Toda reacción debe también tener la seguridad y protección de otras personas, organizaciones o instituciones con las que mantengamos una relación laboradle trabajo.

Establecer objetivos antes de empezar a actuar. La rapidez de la acción es importante, pero saber por qué llevar a cabo esa actividad es más importante.

6.7.2.3 FASE 3: Verificar (Monitorear y Chequear el SGSI)

Se realizarán de forma trimestral y cuando se realicen cambios a los procesos de institucionales.

Las etapas que componen fase, son:

a) Monitorear y Revisar el SGSI.
b) Revisar y medir la efectividad de los controles del SGSI (Métricas del SGSI).
c) Revisar los riesgos residuales.
d) Realizar auditorías internas del SGSI.
e) Revisar el SGSI por parte de la dirección.

a) Monitorear y Revisar el SGSI.

A efectos de detectar, posibles diferencias entre el estado de seguridad de la Universidad Técnica de Machala (sujeto al alcance definido para el SGSI) y el estado que se pretende alcanzar (objetivos y requerimientos de seguridad), es necesario recolectar datos que permitan posicionar el estado de seguridad en el departamento de Tics.

Entrada:

- Alcance y Política del SGSI.
- Estándares y procedimientos asociados a la seguridad de información.
- Resultado de Evaluación de Riesgos
- Objetivos de Control.
- Controles elegidos.
- Requerimientos de Seguridad de Información.
- Clasificación de Procesos y Activos
- Registros de Incidentes de Seguridad de Información.
- Estado de actividades planificadas y que se ejecutando.

Acción:

Deben realizarse revisiones en forma trimestral de chequear que se están aplicando todos los controles seleccionados. Deben coordinarse las acciones de monitoreo de forma de lograr su cometido reduciendo su impacto en operaciones de la universidad y sin que tenga un impacto en la calidad de los servicios ni en los procesos diarios.

Las actividades de monitoreo deben:

- Detectar problemas de los niveles deseados.
- Tomar acciones correctivas
- Replantearse procedimientos y soluciones técnicas.

Quienes deberían participar:

Personal del departamento de Tics de la Universidad Técnica de Machala.

Salida:

- Registro de actividades de monitoreo e informe en el cual sintetice el resultado de estas acciones.
- Informe con recomendaciones técnicas en función de resultados logrados.

b) Revisar y medir la efectividad de los controles del SGSI (Métricas del SGSI)

De las métricas definidas en el capítulo anterior, revisarlas y analizarlas para ver si cumplen con sus parámetros establecidos.

c) Revisar los riesgos residuales.

Posteriormente a la ejecución de la implementado de las decisiones asociadas con el tratamiento del riesgo en las etapas uno y dos del ciclo de mejora continua PDCA, Planear y Hacer respectivamente, constantemente existirá un residuo del mismo riesgo, este riesgo que permanece, después de haber implementado el plan de tratamiento contra los riesgos, es conocido como el riesgo residual.

Se debe ejecutar decisiones para resolver en el caso de que el riesgo residual se ha presentado como inaceptable, en muchos de los casos no se puede minimizar los riesgos hasta un punto aceptable, debido a muchos factores entre los cuales se puede destacar el factor económico, debido a estas circunstancias existe la alterativa de admitir el riesgo.

d) Auditorías Internas del SGSI.

Según la norma ISO/IEC 27001, deben ejecutarse auditorías internas planificados para establecer si los objetivos de control, controles, procesos y procedimientos cumplen:

- Los controles están implementados y se mantienen de forma eficiente
- Se desempeñan de acuerdo a lo requerido.

Debe documentarse criterios, alcance, frecuencia y técnicas que se ejecutarán.

Quienes deberían participar:

Personal del departamento de Tics de la Universidad Técnica de Machala:

- Planificar auditoría que se llevará a cabo.
- Documentar resultados.
- Proponer actividades correctivas y preventivas.

e) Revisión

Esta etapa debe realizarse de forma trimestral y planificada, y tiene como objetivos:

- Evaluar efectividad del SGSI
- Analizar riesgos residuales
- Actualizar planes de seguridad

Entrada:

- Resultados de etapas de monitoreo en función de métricas.
- Cambios en la realidad de la Universidad Técnica de Machala que afecten el SGSI
- Informes de auditoría interna.
- Posibles nuevas tecnologías aplicables a controles existentes.
- Sugerencias e informes recolectados sobre el SGSI.

Acción:

Revisar vigencia principios y requerimientos bajo cuales se tomaron las decisiones y criterios de definiciones del SGSI.

- ¿El alcance del SGSI es adecuado o conviene redefinirlo de acuerdo a la nueva realidad?
- ¿Los niveles de seguridad establecidos en cuanto a confidencialidad, disponibilidad e integridad son competentes?
- ¿Los controles establecidos e implementados son eficaces?

- ¿Las políticas de seguridad de información están al día?
- ¿Están las condiciones de seguridad de información alineados con contratos con proveedores y usuarios?
- ¿Ha cambiado el alcance y/o política del SGSI de la universidad?

Quienes deberían participar:

Empleados del departamento de Tics de la Universidad Técnica de Machala.

Salida:

- Informe de mejoras para hacer al SGSI más eficaz.
- Redefinir el SGSI para adaptarse a cambios de la realidad para lograr los objetivos de los controles dispuestos.

6.7.2.4 FASE 4: Actuar (Mantener y mejorar el SGSI).

En etapa se debe tener presente:

a) Implementar mejora al SGSI.
b) Realizar acciones preventivas y correctivas.
c) Evaluar sugerencias y definir la implementación de mejoras.
d) Comunicar acciones de mejoras del SGSI.
e) Asegurar alcanzar los objetivos previstos.

Entrada:

- Informes de Auditoría interna.
- Informes de no conformidades que estén dentro del alcance del SGSI en cuestión.
- Informes de conclusiones y sugerencias surgidas de la etapa de revisión.
- Propuestas de mejoras de otras áreas.

Quienes deberían participar:

Personal del departamento de Tics de la Universidad Técnica de Machala.

Acción:

- Identificar no conformidades.
- Identificar acciones correctivas y preventivas.
- Implementar las mejoras.
- Prueba de la obtención de las mejoras esperadas.
- Chequeo.
- Información de cambios y las mejoras.

Salida:

Informe con plan de mejoras, describiendo las conclusiones más relevantes surgidas de la etapa de revisión y especificando objetivos, el impacto de cambios y quienes estarían implicados, así como un plan tentativo para ejecutarlo.

Verificar y Actuar

En esta última fase de Implementación, se añade mejoras al SGSI, procediendo a la implementación de un servidor de escaneo de vulnerabilidades mediante la Herramienta NAGIOS, el cual es un sistema de monitorización de redes ampliamente utilizado, de código abierto, que vigila los equipos (hardware) y servicios (software) que se especifiquen, alertando cuando el comportamiento de los mismos no sea el deseado.

Existen muchas herramientas de escaneos de vulnerabilidades en la Web, pero no todas disponen de complementos y funciones completas en cuanto al monitoreo de la gestión de la seguridad de la información en diversas plataformas, además la Universidad Técnica de Machala está afiliada a la Academia CISCO, empresa que provee las licencia para esta herramienta de monitoreo y escaneo de vulnerabilidades en la web.

Por estas razones se ha seleccionado el instrumento de monitorización de redes NAGIOS, la cual entre sus características principales figuran la monitorización de servicios de red (SMTP, POP3, HTTP, SNMP...), la monitorización de los recursos de sistemas hardware (carga del procesador, uso de los discos, memoria, estado de

los puertos...), independencia de sistemas operativos, posibilidad de monitorización remota mediante túneles SSL cifrados o SSH, y programar plugins específicos para nuevos sistemas.

Se trata de un software que proporciona una gran versatilidad para consultar prácticamente cualquier parámetro de interés de un sistema, y genera alertas, que pueden ser recibidas por los responsables correspondientes mediante (entre otros medios) correo electrónico y mensajes SMS, cuando estos parámetros exceden de los márgenes definidos por el administrador de red.

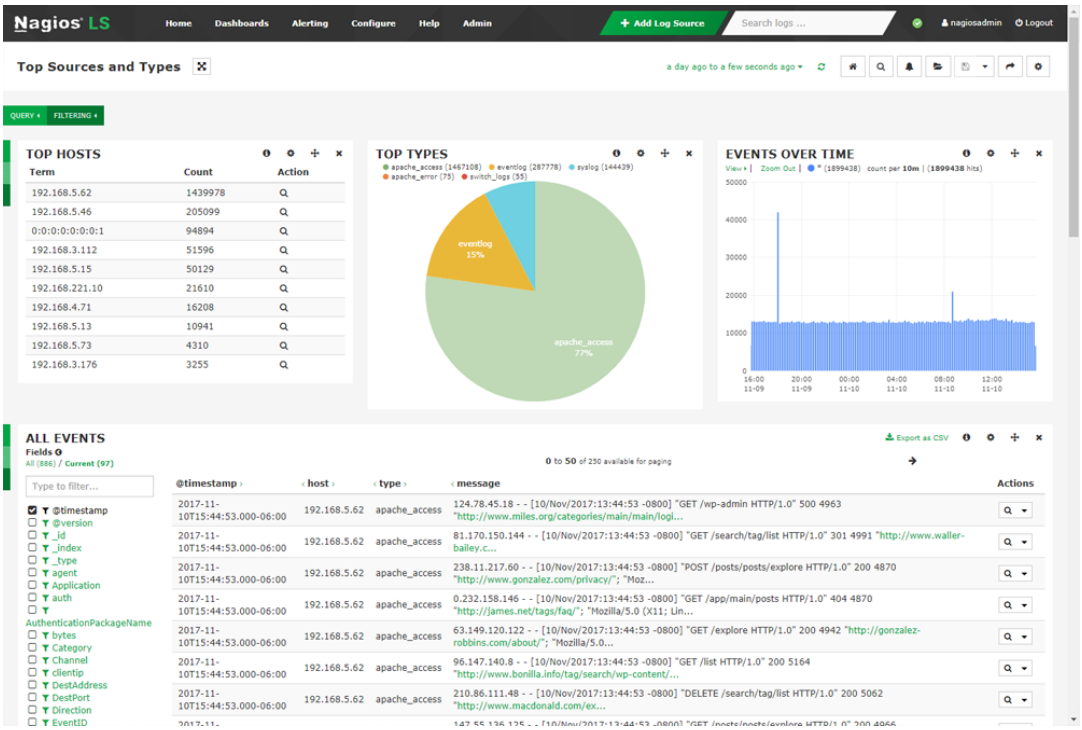


Figura 23. Testeo de Vulnerabilidades NAGIOS LS.

Elaborado por: *Investigador*

Además de la implementación de la herramienta NAGIOS se debe valorar el cumplimiento de las Políticas de Seguridad de la Información que se crearon; se ha establecido una revisión por semestre las cuales luego en reunión del Área de Seguridad de la Información serán evaluadas, monitoreadas y se emitirá un informe del cumplimiento para con ello tomaran medidas correctivas si fuera el caso.

Gracias a la implementación y aplicación de esta herramienta, el personal del Departamento de Tecnologías de la Información y Comunicación puede evaluar los diferentes parámetros de confidencialidad, integridad y disponibilidad de la información que procesan, manejan e intercambian con los diferentes departamentos de sistemas de las cinco facultades y otras dependencias con que cuenta la Universidad Técnica de Machala

De esta manera se da cumplimiento a la adecuada Gestión de la Seguridad de la Información con la Implementación del modelo de Seguridad sustentado en un Sistema de Gestión de Seguridad de la Información en el Departamento de Tecnologías de la Información y Comunicación de la Universidad Técnica de Machala, proporcionando una solvente y eficaz herramienta que cuenta con Dominios, Directivas de Controles y Controles que permiten tener una mejor organización de la institución, distribución de tareas, procesamiento de la información, protección de activos, entrenamiento y capacitación del personal de sistemas y su respectiva gestión de la seguridad de la información de la institución.

Dentro del Anexo A de la Norma ISO 27001 se recomiendo el uso de documentación para los diferentes aportes de seguridad para lo cual se ha creado varios formatos los cuales se utilizan a nivel de todos los departamentos de la institución. (Anexo 11 donde se agrupan 6 Subanexos).

6.8. IMPLEMENTACION DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001 EN EL DEPARTAMENTO DE TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN DE LA UNIVERSIDAD TECNICA DE MACHALA.

CONTENIDO

1. INTRODUCCIÓN.

Con el objetivo de Gestionar la Seguridad de la información de la Universidad Técnica de Machala, surge la necesidad de implementar un modelo base de SGSI que permita alinear los procesos a un mismo objetivo en la gestión de la seguridad de la información.

2. OBJETIVO.

Este documento formaliza el compromiso del rectorado frente a la gestión de la seguridad de la información y presenta de forma escrita a los usuarios de sistemas de información el resumen de actividades con las cuales la Universidad Técnica de Machala establece las normas para proteger de posibles riesgos de daño, pérdida y utilización indebido de la información, los equipos y demás recursos informáticos de la Institución, los cuales están en consecuentes cambios y evolución acorde con el avance de la tecnología y los requerimientos de la organización.

3. REQUISITOS LEGALES Y/O REGLAMENTARIOS.

Para la implementación del SGSI, la Universidad Técnica de Machala deben regirse por lo dispuesto en el marco jurídico y normativo aplicable a las Instituciones de Educación Superior.

4. RESPONSABLE

Compromiso del Departamento de Tics.

El departamento de Tecnologías de la Información y Comunicación de la Universidad Técnica de Machala debe brindar evidencias de su compromiso con el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de los mecanismos para asegurar información:

Se debe programar los objetivos de la seguridad de la información, designando roles para cada funcionario de la institución, quien a su vez es responsable del manejo de algún activo.

Para lograr el propósito de la mejora continua institucional, Los rectores deben estar previamente informados del cumplimiento de los objetivos de la seguridad de la información.

Gestión de los recursos

- Asegurar que las políticas de seguridad de la información brindan apoyo al cumplimiento de la misión y visión de la Universidad Técnica de Machala.
- Identificar y atender los requisitos legales y reglamentarios, así como las obligaciones de seguridad contractuales; o mantener la seguridad suficiente mediante la aplicación correcta de todos los controles implementados;
- Asegurar que todo el personal tiene conciencia de la importancia de la seguridad de la información.

Procedimiento. Comunicación de las políticas de seguridad:

El personal del departamento de Tecnologías de la Información y Comunicación de la Universidad Técnica de Machala, conscientes que los recursos de información son utilizados de manera permanente por los usuarios que acceden a diferentes servicios, definidos en este documento, han considerado oportuno transmitir a los mismos las normas de comportamiento básicas en la utilización de los equipos de cómputo y demás recursos tecnológicos y de información.

4.1 APLICACIÓN DE POLÍTICAS DE SEGURIDAD. (APLICACIÓN DEL SGSI):

Las políticas de seguridad informática(SGSI) se orientan a reducir el riesgo de incidentes de seguridad y minimizar su efecto. Establecen las reglas básicas con las cuales la organización debe operar sus recursos informáticos. El diseño de las políticas de seguridad informática está encaminado a disminuir y eliminar muchos factores de riesgo, principalmente la ocurrencia.

5. POLÍTICAS DE SEGURIDAD.

La Universidad Técnica de Machala reconoce abiertamente la importancia de la gestión de la seguridad de la información, así como la necesidad de su protección para constituir un activo estratégico de la organización y todas las partes interesadas, el no uso adecuado de los activos de información puede poner en peligro la continuidad del negocio o al menos suponer daños muy importantes que afecten el normal funcionamiento de los procesos.

Los funcionarios, terceros y usuarios en general deberán conocer el presente documento, normas, reglas, estándares y procedimientos que apliquen según las funciones que realicen para la organización, el desconocimiento que conlleve a la violación de lo anteriormente mencionado representará para la persona involucrada las sanciones disciplinarias que apliquen según el incidente presentado.

Igualmente se implementarán los controles de seguridad encaminados a garantizar la confidencialidad, integridad y disponibilidad de los activos de información de la institución con el objetivo de lograr un nivel de riesgo aceptable de acuerdo con la visión, misión, planeación y estrategia de la compañía, y dando cumplimiento al marco jurídico aplicable a los estándares nacionales.

5.1 Directrices de la Dirección en Seguridad de la Información.

5.1.1 Conjunto de Políticas para la Seguridad de la Información.

El departamento de Tecnologías de la Información y Comunicación dará seguimiento al cumplimiento de las normativas de la ISO para crear un ambiente de Seguridad de la Información los cuales tendrán las siguientes funciones:

- Cuidar por la seguridad de los activos informáticos.
- Gestión, Administración y Procesamiento de la información.
- Elaboración y Desarrollo de planes de seguridad.

- Mantener capacitados a los usuarios en temas de Seguridad.
- Mantener informados a las máximas autoridades sobre problemas de seguridad.
- Poner especial atención a los usuarios de la red institucional sobre sugerencias o quejas con respecto al funcionamiento de los activos de información.

El departamento de Tecnologías de la Información y Comunicación, a través de su Director deberá elaborar manuales de roles, políticas y responsabilidades para cada uno de los trabajadores de cada departamento, el cual deberá estar documentado y aprobado por Rectorado, tomando en cuenta todos los cargos concernientes a políticas de seguridad de la información. En este manual deben constar todos los cargos, que se encuentran detallados en el organigrama de la Institución.

- El jefe del Departamento dentro de la red institucional es el único responsable de las actividades precedentes a sus acciones.
- El Director de Tics es el encargado de mantener en buen estado los servidores dentro de la red institucional.
- Todo usuario de la red institucional gozara de absoluta privacidad sobre su información, o la información que provenga de sus acciones, salvo en casos en que se vea involucrado en actos ilícitos o contraproducentes para la seguridad de la red institucional.
- Los usuarios tendrán el acceso a Internet previa autorización siempre y cuando se cumplan los requisitos mínimos de seguridad para acceder a este servicio y se acaten las disposiciones de conectividad de la unidad informática.
- Las actividades administrativas tienen la primera prioridad por lo que a cualquier usuario utilizando otro servicio (por ejemplo: juegos, chat), sin estos fines, se le podrá solicitar salir o desconectar automáticamente los servicios si, así fuera necesario.

5.1.2 Revisión de las políticas para la seguridad de la información.

- Las revisiones de las políticas de seguridad se realizarán periódicamente, por los encargados del departamento de Tecnologías de la Información y Comunicación.

- El departamento de Tecnologías de la Información y Comunicación tendrá a cargo la revisión de manuales y documentos que se realizaren sobre políticas de seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE SEGURIDAD DE LA INFORMACIÓN.

6.1. Organización interna

6.1.1 Asignación de responsabilidades para la seguridad de la información.

- Con el cumplimiento de este control el Director del departamento de Tecnologías de la Información y Comunicación asignará a un compañero dentro del área que será responsable de elaborar manuales de políticas y procedimientos para el área de tecnologías de la información y comunicación.

- Los miembros del departamento de Tecnologías de la Información y Comunicación, así como también un comité de Seguridad integrado por: Gestor de Seguridad, Responsable de Activos, Departamento de Sistemas serán los encargados de generar planes de contingencia anti desastres, etc.

6.1.2 Segregación de tareas.

El Director del Departamento de Tecnologías de la Información y Comunicación, capacitará a los demás trabajadores del departamento asignado a su responsabilidad, en cuanto al uso de los sistemas de información.

En caso de ocurrir algún problema interno el servidor público encargado del área deberá solucionarlo en el caso que sea extremo acudir con el encargado del Departamento de Tecnologías de la Información y Comunicación.

Si un incidente ocurre en relación con el control de acceso, protección contra amenazas externas y de medio ambiente que el encargado del Departamento de Tecnologías de la Información y Comunicación no pueda solucionarlo deben notificar al encargado de Seguridad de la Información de la Universidad Técnica de Machala.

6.1.3 Contacto con las autoridades.

Deberá existir una constante comunicación con el Director del departamento de Departamento de Tecnologías de la Información y Comunicación, para que en el caso de realizar alguna actualización en las políticas de uso de la información darle a conocer sobre el caso.

6.1.4 Contacto con grupos de interés especial.

El Director del Departamento de Tecnologías de la Información y Comunicación se mantendrá al tanto sobre el tema de la seguridad de la información, tomando información de foros o grupos de seguridad externos, de la información acerca de cambios o actualizaciones de las políticas a nivel general.

6.1.5 Seguridad de la información en la gestión de proyectos.

Cuando se desarrollen proyectos en el Departamento de Tecnologías de la Información y Comunicación, sin importar la índole del proyecto, cada trabajo deberá ser informado al departamento de Tecnologías de la Información y Comunicación que determinara las políticas que se aplicaran en dicho proyecto.

6.2 Dispositivos para movilidad y teletrabajo.

Dispositivos móviles: En la institución se reconoce el alto grado de exposición que presenta la información y los datos de la institución almacenados en dispositivos móviles (computadores portátiles, tabletas, teléfonos inteligentes, entre otros.).

Corresponde a la dirección administrativa y funcionarios gestores de los recursos tecnológicos, elaborar, mantener e implementar planes de capacitación que propendan por la formación y mantenimiento de la conciencia en cuestión de seguridad de la información.

Las redes inalámbricas potencialmente introducen nuevos riesgos de seguridad que deben ser identificados, valorados y tratados de acuerdo a los lineamientos de la Política de Seguridad de la información en materia de redes.

- Los usuarios necesitaran permiso para instalar o desinstalar aplicaciones en los dispositivos móviles. Que sean de propiedad de la institución, no se les permite acceder al sistema y a las aplicaciones virtuales de las computadoras.

- No acceder a los enlaces solicitados a través de SMS/MMS/Email podría ser código malicioso.

- La configuración, modificación o eliminación de software aplicativo sobre los dispositivos móviles es responsabilidad exclusiva del área asignada para tal fin.

Computación en la nube: La información producida por los procesos de la institución, no debe ser alojada en dispositivos de almacenamiento en la nube, ya que se podría verse afectada la integridad, confidencialidad y disponibilidad de los datos, en caso tal de contratarse un servicio de cloud computing para la institución, podrán alojarse los archivos que requieran copias de seguridad, almacenamiento y difusión masiva.

6.2.1. Política de uso de portátiles.

- Protección de la información
- El antivirus siempre debe estar activo y actualizado
- No permitir que personas extrañas lo observen mientras trabaja en el equipo portátil, especialmente si esta fuera de las instalaciones de la institución.
- Seguir las políticas de acceso remoto
- Toda la información que es confidencial debe estar cifrada.
- No dejar el computador portátil en lugares públicos
- Cuando viaje el computador portátil no debe ir dentro de su maletero siempre debe llevarse en su equipaje mano.
- No es permitido que el computador portátil sea utilizado por familiares y/o amigos.

6.2.2 Teletrabajo.

- La modalidad de Teletrabajo no está disponible en el Departamento de Tecnologías de la Información y Comunicación de la Universidad Técnica de Machala.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.

Se debe considerar como recurso humano a todo el personal interno, externo, temporal en el aseguramiento de las responsabilidades que son asignadas a cada uno, asociadas con sus respectivos roles, para reducir el riesgo de hurto, fraude, sabotaje o uso inadecuado de los activos de información.

Cuando un usuario inicie su relación laboral con la institución se debe diligenciar el documento de entrega de inventario.

Cuando un funcionario de la institución inicie su relación laboral se debe diligenciar el documento de entrega de inventario.

7.1 Antes de la contratación. Para toda persona que ingrese a la laborar en la institución, la Dirección de Talento Humano debe asegurar las responsabilidades sobre seguridad de la información de manera previa a la contratación. Así mismo incluir un acuerdo de confidencialidad, esta tarea debe reflejarse en una adecuada descripción del cargo, funciones, investigación de antecedentes y en los términos y condiciones de la contratación.

7.1.1 Investigación de antecedentes.

- Se realizarán concursos de méritos que deberán ser aprobados.
- Se solicitará referencias personales, laborares, para asegurarse de no tener problemas de índole legal al momento de contratar nuevo personal.

7.1.2 Términos y condiciones de contratación.

Luego de la selección del nuevo empleado para la institución, existirá un contrato legalizado, el que incluirá cláusulas de confidencialidad, las que el nuevo empleado debe cumplir ya sea persona natural o jurídica.

En el contrato se incluirá sobre la aceptación de los términos y condiciones, que le obligan al funcionario a declararse como responsable de dar cumplimento a las políticas de seguridad que estén vigentes dentro del Departamento de Tecnologías de la Información y Comunicación.

En el ANEXO 4 se encuentra el formulario de “Acuerdo de Confidencialidad”.

Acuerdo de confidencialidad. Para el uso de los recursos tecnológicos de la institución, todo usuario debe firmar un acuerdo de confidencialidad y un acuerdo de Seguridad de los sistemas de información (Anexo 5) antes de que le sea otorgado una cuenta de usuario y contraseña de acceso a la red y sus respectivos privilegios o medios de instalación de las soluciones de autenticación biométrica.

- Los usuarios no deben utilizar los dispositivos electrónicos propios de la institución para su uso personal, es por ello que no deberán acceder desde estos a redes sociales ni correos electrónicos personales.
- Todos los usuarios deben realizar el envío de información únicamente a través del correo institucional.
- Cada usuario que se denomine como personal interno será responsable por el mal uso del equipo de cómputo en el cual realiza sus tareas, incluyendo infecciones de virus.
- Los usuarios no deben bajo ninguna circunstancia descargar de internet archivos, que pudiera ser considerado pornográfico, difamatoria, racista, videos, música, entre otros. o que atente contra las buenas costumbres o principios, excepto que su función administrativa así lo amerite.

Responsabilidades de usuarios externos. Personal que es parte de organizaciones externas que tengan convenios o relaciones con la institución. Los usuarios externos o terceros y personal de empresas externas, deben estar autorizados por un miembro del personal de la organización, quien será responsable del control y vigilancia del uso adecuado de la información y de los recursos tecnológicos institucionales, del uso que estos tengan; ellos deben acatar los siguientes reglamentos:

– **Registro de las compañías que reciben información privada.**

  El personal de la institución que facilito información privada a terceros debe mantener un registro de toda divulgación y este debe contener qué información fue revelada, a quién fue revelada y la fecha de divulgación.

– **Transferencia de la custodia de información de un funcionario que deja la Universidad Técnica de Machala.**

  Cuando un empleado se retira de la institución, su jefe inmediato debe revisar tanto los archivos magnéticos, correo electrónico como documentos impresos para determinar quién se encargará de dicha información o para ejecutar los métodos para la destrucción de la información.

7.2 Durante la contratación.

Definición de responsabilidades de la Dirección de Talento Humano para garantizar que la seguridad se aplica en todos los puestos de trabajo de los empleados de la institución.

A los usuarios empleados, contratistas y terceras personas se les proporcionará un adecuado nivel de concienciación, educación y capacitación en procedimientos de seguridad de la información y en el uso correcto de los medios disponibles para el procesamiento de la información con objeto de mitigar los posibles riesgos de seguridad.

7.2.1. Responsabilidades de gestión.

- Sera obligatorio que los términos y condiciones resalten en el contrato, estableciendo las diversas responsabilidades del empleado en cuanto a la seguridad de la información donde va a laborar.
- Los diferentes departamentos de las otras facultades de la institución deberán estar informados sobre las responsabilidades de seguridad informática, además de sanciones por incumplimiento de las mismas.

7.2.2 Concienciación, educación y capacitación de seguridad de la información.

Realizar capacitaciones y requerimientos de seguridad, al asignar responsabilidades a cada encargado de departamento en su área. El encargado de organizar este tipo de actividades será el departamento de Tecnologías de la Información y Comunicación para difundir las políticas de seguridad.

El departamento de Tecnologías de la Información y Comunicación tendrá la responsabilidad de proporcionar el material necesario para la actividad, este material debe ser actualizado cada cierto tiempo que se vea necesario para estar claro en relación con el tema y cambios que hayan surgido.

7.2.3 Proceso disciplinario.

El proceso debe pronosticar una respuesta gradual, tomando en consideración la gravedad del acto, su impacto en la institución, si el trabajador fue capacitado correctamente, la sanción se tomará en cuenta según el acuerdo de confidencial firmado en el contrato.

Si el acto realizado tiene un nivel de gravedad perjudicial para la Institución, el proceso permitirá la terminación inmediata de los derechos de acceso y privilegios otorgados, o la separación inmediata del cargo empleado dentro de la Institución.

7.3 Cese o cambio de puesto de trabajo. La Dirección de Talento Humano debe asegurar que los funcionarios, contratistas, terceras partes, que no laboren más en la empresa o cambien de puesto de trabajo, hayan firmado un acuerdo de confidencialidad, cuyo cumplimiento será vigente hasta que la institución lo considere conveniente, incluso después de la finalización del puesto de trabajo o del contrato; también que se devuelve todo el equipamiento y se eliminan todos los derechos de acceso.

8. GESTIÓN DE ACTIVOS.

Control sobre los activos.

- Identificar los propietarios para todos los activos y asignar la responsabilidad para el mantenimiento de los controles. La implementación de los controles específicos puede ser delegada por el propietario según el caso, pero él sigue siendo responsable de la protección adecuada de los activos.

- Los recursos informáticos de la institución, dispuestos para la operación registral, solo deben ser usados para fines laborales, entre los cuales, se resalta la prestación del servicio de autenticación biométrica a los usuarios de la institución. El producto del uso de dichos recursos tecnológicos será de propiedad de la institución y estará catalogado como lo consagran las políticas de la institución. Cualquier otro uso está sujeto a previa autorización del rectorado.

- El uso del computador personal y demás recursos informáticos por parte del empleado, trabajadores o usuarios del sistema de autenticación biométrica, debe someterse a todas las instrucciones técnicas que imparta el departamento de Tecnologías de la Información y Comunicación.

Clasificación de la Información

- La información se debe clasificar para indicar la necesidad.
- Se deben asignar responsabilidades en cuanto a la propiedad de los activos de información a usuarios encargados de mantener la integridad de la información. Es responsabilidad del administrador de la información asignar los respectivos controles de acceso a la información.

Eliminación segura de la información en medios informáticos

Todo medio informático reutilizable de terceros como equipos rentados, discos externos, memorias USB, etc. utilizados por la institución, antes de su entrega se les realizara un proceso de borrado seguro en la información.

Eliminación segura de la información en medios físicos

Cualquier documento físico que haya sido considerado y clasificado de carácter confidencial y que necesite ser destruido, debe realizarse en la respectiva máquina destruye papel o cualquier otro método seguro de destrucción aprobado por el departamento de Tecnologías de la Información y Comunicación.

Manejo de los soportes de almacenamiento.

- Está terminantemente prohibido compartir los discos duros o las carpetas de los computadores de escritorio, aunque estén protegidos por contraseña. Cuando exista la necesidad de compartir recursos esto se debe hacer con autorización previa y restringir por dominio.
- Asegure los soportes y la información en tránsito no solo físico sino electrónico (a través de las redes). Encripte todos los datos sensibles o valiosos antes de ser transportados.

8.1 Responsabilidad sobre los activos.

8.1.1 Inventario de Activos.

El Departamento de Tecnologías de la Información y Comunicación tendrá identificado todos los activos de información, en relación con los sistemas de información que maneja la institución, así como sus respectivas ubicaciones físicas de cada activo.

El inventario permanentemente será actualizado, en caso de que exista alguna modificación administrativa o de estado del activo, en caso de que sucediera un cambio en el activo y este no se notificaría, la responsabilidad recaerá sobre el encargado del que las custodia.

8.1.2 Propiedad de los Activos.

En cuanto a propiedad de activos, el punto es que toda la información que pertenezca a la institución está sujeta a revisiones periódicas por parte del Departamento de Tecnologías de la Información y Comunicación encargada de la seguridad de la información.

8.1.3 Uso aceptable de los activos.

La política se rige en que los activos de información de la Universidad Técnica de Machala son de propiedad de la misma, por tal motivo debe serutilizada únicamente para fines laborales.

Lineamientos de seguridad de la información:

- Los recursos de servicio internet, correo electrónico y sistemas de información, serán utilizados para fines laborales, y con el permiso respectivo del departamento de sistemas.

- Cada encargado de sus departamentos identificará la labor que realizará los empleados a su cargo concediendo el debido acceso a la información mediante una asignación de roles que va a desempeñar el trabajador.

- Se prohíbe la divulgación de la información almacenada, creada o transmitida por los sistemas de Información de la Universidad Técnica de Machala.

- Las aplicaciones, software y sistemas de información que se utiliza dentro de la Universidad Técnica de Machala. deberán estar con su respectiva licencia o lo que es recomendable utilizar software libre, esto será instalado por el personal del departamento de Tecnologías de la Información y Comunicación.

- El Departamento de Tecnologías de la Información y Comunicación será el encargado de establecer las cuentas a los usuarios de todos los departamentos, incluyendo acceso al control de los servidores en el caso que se necesite la información, auditorias de base de datos, monitoreo de uso de los sistemas.

- No se permite la compartición de acceso entre usuarios e información confidencial a terceras personas o entidades externas, vía mensaje de texto, transferencias vía correo electrónico o almacenamiento físico.

- Los sistemas de información estarán sujetos a ser auditadas por personal del Departamento de Tecnologías de la Información y Comunicación las veces que sea necesario o estableciendo un determinado tiempo por el mismo encargado.

- El Departamento de Tecnologías de la Información y Comunicación implementara controles de seguridad de la información como firewall, antivirus, DMZ, etc. para asegurar que la información almacenada se encuentre respaldada.

- La Universidad Técnica de Machala podrá revocar los privilegios de uso de activos de la información, emisión de sanciones e incluso trámites legales al empleado que ponga en riesgo la integridad, confiabilidad y disponibilidad de la información de la institución.
- Se establecen restricciones de acceso a redes inalámbricas, de acuerdo con las necesidades de cada departamento dentro de la Universidad Técnica de Machala.

- Para crear cuentas de correo electrónico se debe evitar utilizar caracteres especiales, la dirección de correo debe ser representativo al usuario, se asignará un tamaño de almacenamiento para el buzón de correo.

8.1.4 Devolución de activos.

Con la aplicación de este control el encargado de los activos cumplirá los lineamientos siguientes:

- Si el empleado saliente trabajo con información sobre tecnología o de administración relacionadas con su labor dentro de la Universidad Técnica de Machala deberá dejar en conocimiento a través de documentos al departamento donde laboro.

- Toda la información de la Universidad Técnica de Machala que este en el equipo informático del empleado será removida del mismo.

- Devolución de equipos en general.

En el ANEXO 6 se encuentra el formulario de "Inventario de Hardware y Software de los computadores".

8.2 Clasificación de la información.

8.2.1 Directrices de clasificación.

Con la aplicación de este control se debe clasificar la confidencialidad, integridad y disponibilidad.

Confidencialidad:

- Acceso privado e interno.
- La divulgación de la información traería consecuencias significativas a la Institución.
- La información se considera estrictamente confidencial.
- La información no tendrá acceso al público.

Integridad:

- La información se podrá modificar y rectificada con facilidad.
- La información se podrá modificar y rectificar ocasionando pérdidas mínimas en la Institución.
- La información se podrá modificar, pero será más complicada para corregirla y podría existir pérdidas para la Institución.
- La información se podrá modificar, pero no podría ser corregida y existirán pérdidas importantes para la Institución.

Disponibilidad:

- La información no afectara las operaciones de la Institución.
- La información que no esté habilitada por un tiempo de 5 días, podría afectar las operaciones de la Institución.
- La información que no esté disponible por un día podría afectar severamente las operaciones de la Institución.
- La información que no esté disponible durante una hora puede afectar significativamente las operaciones de la Institución.

8.2.2 Etiquetado y manipulado de la información.

Se tendrá que identificar la información y los activos, que serán manipulados de mejor manera evitando daños o perdidas de la información, se manejará a través de código de colores según el nivel de riesgo.

- Para definir los controles de seguridad que se debe dar a cada una se identificara la información con los colores respetivos.

8.2.3 Manipulación de activos.

Los empleados deben tener los conocimientos de los niveles de riesgos para que puedan ser manipuladas sin ningún problema todo tipo de información en sus departamentos.

8.3 Manejo de los soportes de almacenamiento.

8.3.1 Gestión de soporte extraíbles.

Los encargados de cada departamento de la Universidad Técnica de Machala, deberán controlar los dispositivos extraíbles que pertenezca a su área de trabajo, estos estarán destinados a los procesos que se ejecuten dentro del departamento o de la misma manera si son utilizados para almacenar la información únicamente en el área de trabajo.

8.3.2 Eliminación de soportes.

Se eliminará los dispositivos de almacenamiento, todo tipo de copias y/o clonaciones de la información, esto lo deberá realizar el servidor público encargado de su departamento.

8.3.3 Soportes físicos en tránsito.

Los datos almacenada en los dispositivos extraíbles que salen del área de la Institución, deberá ser encriptados para evitar plagio o copias no autorizadas dentro del departamento ya que puede ser información interna de la institución.

9. CONTROL DE ACCESOS.

9.1 Requisitos de negocio para el control de acceso.

9.1.1 Política de control de acceso. Los usuarios tendrán una identificación única en los sistemas que tenga acceso (usuario), acompañado de un elemento para su autenticación (contraseña) de carácter personal y confidencial para el uso de recursos tecnológicos necesarios en sus labores. Esta política abarca aplicativos implementados hasta la fecha de liberación de este documento. Los funcionarios contarán con una identificación única personal y su respectiva contraseña asignada por el encargado del departamento de tecnologías de la información y comunicación.

- Los usuarios son responsables de los mecanismos de control de acceso que les sean proporcionados; es decir, nombre de usuario y contraseña necesarios para acceder al sistema, grupo de trabajo y/o dominio de red.

9.1.2 Control de Acceso a las redes y servicios asociados. Las contraseñas asignadas a los usuarios para acceder a los sistemas de información, debe ser personal, confidencial e intransferible. Los usuarios deben velar para que sus contraseñas no sean copiadas por otras personas.

- Los usuarios deben cambiar su contraseña por lo menos una vez cada 30 días.
- Para impedir el compromiso de múltiples recursos informáticos, los usuarios deberán utilizar diferentes contraseñas para los recursos a los que tienen acceso. Esto implica equipos de comunicación (firewall, routers, servidores de control de acceso) y a administradores.
- No se debe revela la contraseña en ningún cuestionario o formulario, independientemente de la confianza que le inspire el mismo.
- No se debe usar la característica de "Recordar o guardar Contraseña".
- Se debe evitar compartir la contraseña en respuesta a un ejemplo de petición por correo electrónico o por teléfono, para verificar su identidad, incluso si parece ser de una compañía o persona de confianza.

9.2 Gestión de acceso de usuario.

9.2.1. Gestión de altas/bajas en el registro de usuarios.

Con la aplicación de este control para la cancelación y registro del usuario se realizará de manera individual dando de baja o el acceso a la información que utilizara en su área de trabajo, él encargado del departamento de sistemas será el responsable y tomara en cuenta los lineamientos siguientes:

Identificar con el nombre a los usuarios que los identificará de manera segura para el departamento en el que labore, el usuario y el nivel de acceso asignado al empleado le permitirá realizar sus labores dentro de su área de trabajo.

Verificación de los usuarios que acceden a los servidores, sistemas de información y redes de datos, verificando que sean los autorizados por Departamento de Tecnologías de la Información y Comunicación ya que podría existir algún tipo de infiltración.

En el caso que el empleado termine sus funciones laborales dentro de la Universidad Técnica de Machala, deberá ser notificado de inmediato al Departamento de Tecnologías de la Información y Comunicación para darle de baja.

9.2.2 Gestión de los derechos de acceso asignados a usuarios.

- Se utilizará procedimientos para controlar los usuarios dentro del servidor que permitirán otorgar o quitar los permisos establecidos para las actividades que realizaran dentro de los diferentes departamentos.

9.2.3 Gestión de los derechos de acceso con privilegios especiales.

Se utilizará las políticas de seguridad y privilegios otorgados para filtrar usuarios que necesiten permisos especiales dentro de los servidores o redes de información siguiendo los requerimientos necesarios por parte del Departamento de Tecnologías de la Información y Comunicación:

- Asignar privilegios de acceso y modificación únicamente a los módulos que sean necesarios para el cumplimiento de las funciones del empleado.
- Se deberá realizar revisiones continuas de todas las tareas que realice el empleado, que se encargará el Departamento de Tecnologías de la Información y Comunicación.
- Pasar un informe a cada departamento detallando sobre los privilegios de acceso para los servidores que deberán cumplir y de la misma manera para los sistemas de información y redes, etc.

9.2.4 Gestión de información confidencial de autenticación de usuarios.

Con la aplicación de este control al momento de otorgar una contraseña de acceso a los usuarios se cumplirá unos requerimientos necesarios para mejorar la dificultad de ataques maliciosos:

Un formulario de creación de usuario y responsabilidad de contraseñas.

Se asignará una clave temporal al usuario de modo que el usuario sea quien cree la clave pasando a ser confidencial e intransferible, en el primer ingreso al sistema.
Para la asignación de una clave a un usuario se debe tener la autorización del encargado del departamento donde va a laborar el mismo.

El acceso de encriptación a los de servidores y sistemas se deben almacenar únicamente en el Departamento de Tecnologías de la Información y Comunicación en lugares seguros de poco acceso al personal.

En el ANEXO 7 se encuentra el formulario de "Creación de usuario y responsabilidad de contraseñas".

En el ANEXO 5 se encuentra el formulario de "Formulario de Listado de servidores y contraseñas".

9.2.5 Revisión de los derechos de acceso de los usuarios.

Control que permite realizar revisiones de niveles de acceso que se concedió a usuarios de los departamentos de la Universidad Técnica de Machala tomando en cuenta los siguientes criterios:

- El acceso de los encargados del Departamento de Tecnologías de la Información y Comunicación y otros responsables de sus departamentos respectivos deberán pasar por revisión cada 3 meses.

- Para los usuarios en general se tendrá en cuenta cada mes la revisión respectiva o cada termino laborar de un empleado de la Institución.

- Los empleados que tenga permisos o privilegios especiales en su departamento deberán pasar por revisiones constantes especialmente si poseen acceso total de los sistemas de la Institución.

9.2.6 Retirada o adaptación de los derechos de acceso.

Cuando un servidor público termine sus funciones en la Institución se dará de baja los permisos y derechos concedidos en los sistemas y servicios de la institución, por lo tanto, el encargado de cada departamento deberá notificar de manera inmediata la finalización del contrato del empleado para que el encargado del Departamento de Tecnologías de la Información y Comunicación pueda tomar cartas en el asunto y eliminar el usuario del mismo.

9.3. Responsabilidad del usuario.

9.3.1. Uso de información confidencial para la autenticación.

Con la aplicación de este control los empleados de todos los departamentos deberán tener en cuenta los siguientes requerimientos para la seguridad de la información:

El usuario deberá cambiar la clave provisionalmente otorgada por una personal al momento de ingresar por primera vez al sistema.

Las claves de ingreso a los sistemas de información y servidores deberán ser confidenciales y por seguridad encriptadas en un formato más seguro para evitar robo de información.

En el caso que un usuario olvide su contraseña deberá notificar de manera inmediata al Departamento de Tecnologías de la Información y Comunicación

9.4 Control de acceso a sistemas y aplicaciones

9.4.1 Restricciones de acceso a la información.

Con la realización de este control se tendrá que tomar en cuentas los siguientes requerimientos.

El sistema deberá contener la página de inicio de login para que el usuario pueda colocar su id y contraseña respectiva e ingresar a sus funciones dentro del mismo, por lo tanto, el usuario tendrá limitada sus funciones dentro de la plataforma.

El sistema debe permitir el acceso a la información autorizada y requerida, es decir se debe controlar los permisos de lectura, escritura y ejecución, para cada usuario.

Se tomará en cuenta aplicar auditorías del sistema en cuanto a la información que maneja los usuarios verificando que sean las que debe manipular el mismo.

9.4.2 Procedimientos seguros de inicio de sesión.

Los sistemas establecidos en cada departamento solo podrán tener acceso los usuarios registrados en las bases de datos que maneja el Departamento de Tecnologías de la Información y Comunicación como seguridad de ingreso a la información de la Institución permitiendo solamente el ingreso al usuario autorizado por dicho departamento.

9.4.3 Gestión de contraseñas de usuario.

Las contraseñas que manejen los usuarios deberán tener un grado de complejidad para protegerlas y evitar un acceso no autorizado, por lo tanto, las contraseñas deberán ser de un formato mínimo de 16 caracteres entre número, letras e incluso caracteres especiales.

El usuario deberá estar consciente de los problemas de seguridad que acarrea la irresponsabilidad en la salvaguarda y uso de su contraseña.

La práctica de guardar contraseñas en papel adherido al monitor o áreas cercanas al equipo de trabajo es una falta grave y sancionable.

9.4.4 Uso de herramientas de administración de sistemas.

Los parámetros que tenga las aplicaciones que maneja el Departamento de Tecnologías de la Información y Comunicación deberán tener restricción, solamente los encargados de los departamentos tendrían acceso total respectivo a su área de trabajo.

Solo los encargados de los departamentos tendrían acceso para modificar acceso dentro de su área debido a las restricciones aplicadas a cada usuario.

9.4.5 Control de acceso al código fuente de los programas.

Se restringirá el acceso al código fuente del sistema a los usuarios no a autorizados, para evitar alguna modificación o robo de información del sistema, en el caso que el desarrollador del sistema termine su contrato deberá dejar toda información del sistema

y se mantendrá suspendido su equipo de trabajo por el tiempo que no esté en su lugar de trabajo.

Antes de ser puestas en ejecución las aplicaciones recibirán una auditoria sobre fallos o información errónea que puedan procesar.

10. CIFRADO.

Proteger la confidencialidad, autenticidad o integridad de la información que se envía y se recibe, aplicando controles criptográficos.

- Si se transporta información sensible en medios legibles por el computador (DVD, CD, memorias USB), la información deberá ser encriptada, siempre y cuando el receptor acepte el intercambio de datos cifrados. Para las computadoras portátiles esta clase de información es mantenida por una aplicación de cifrado.

- Si se ha de transmitir datos sensibles a través de cualquier canal de comunicación externo, dichos datos deben ser enviados en forma encriptada, siempre y cuando el receptor tenga los recursos necesarios y acepte el intercambio de datos cifrados.

10. SEGURIDAD FÍSICA Y AMBIENTAL.

11.1 Áreas Seguras.

Todos los elementos o activos que de una u otra forma colaboran con el servicio de procesamiento de la información institucional deben contar con la seguridad adecuada del caso, es decir, con el establecimiento de zonas seguras y los protocoles respectivos de la protección del acceso a estos elementos, además estas zonas seguras, deben estar protegidas físicamente contra acceso no autorizado, daño e interferencia.
La protección suministrada debe estar acorde con los riesgos identificados.

11.1.1 Perímetro de seguridad física.

La restricción del acceso a recursos o activos de tecnología se tendrá en cuenta para la confidencialidad de la información de la Universidad Técnica de Machala, por lo tanto:

Se deberán tener controles biométricos en departamentos que tenga información importante para que puedan restringir esas áreas limitando el acceso a los usuarios que no requirieran esta información.

En la Institución se deberá contar con cámaras de seguridad, vigilancia y alarmas para tener en cuenta quien ingresa al departamento y tener respaldos físicos en caso de alguna anomalía dentro del área.

Sistema de vigilancia con cámaras de seguridad.

Este sistema deberá desarrollarse por las personas naturales o jurídicas, tendientes a prevenir o detener perturbaciones a la seguridad y tranquilidad en lo relacionado con la vida y los bienes propios o de terceros y la fabricación, comercialización, instalación y utilización de equipos para la vigilancia y seguridad privada, blindajes y transporte con este mismo fin.

- El sistema de video vigilancia se empleará únicamente a efectos de protección y seguridad. El sistema contribuye a garantizar la seguridad tanto de los edificios de la institución, su personal y visitantes como de los bienes contenidos en sus instalaciones y la información allí almacenada.

- En caso de necesidad, se recomienda contemplar y complementar con otros sistemas de seguridad físicos, por ejemplo, sistemas de control de acceso y sistemas de detección de intrusiones.

11.1.2 Controles físicos de entrada.

Se contará con un registro de cada persona que ingrese a un área determinada con los datos personales, cedula hora de ingreso y salida.

Se deberán utilizar acceso biométrico, credenciales con foto actualizada, de esta manera se tendrá clasificada el ingreso a los departamentos de la institución la cual se deberá tener revisiones constantes para mantener actualizada la información de los usuarios.

11.1.3 Seguridad de oficinas, despachos y recursos.

Con la aplicación de este control se tendrá la seguridad de los departamentos en especial el Departamento de Tecnologías de la Información y Comunicación ya que en él se encuentra los servidores e información clasificada de la Institución para ello se deberán aplicar los parámetros siguientes:

- Restringir acceso al personal no autorizado en los departamentos.
- Asegurar puertas y ventanas de los departamentos en caso de ser necesario se podría presentar un ingreso no autorizado fuera de horas de trabajo de terceras personas.
- Tener el equipamiento necesario dentro de cada departamento.
- Respaldar la información en servidores y disco externos y evitar que tenga contacto con personal no autorizado.

11.1.4 Protección contra las amenazas externas y ambientales.

Si la Institución debe atender procesos de contabilidad, tesorería, administrativo-académicos, documentarios; actividades que no podrían dejar de funcionar por la importancia estratégica. La recuperación y puesta en marcha de los servidores que alojan dichos sistemas, es fundamental.

- Evitar que suministros de papelería se encuentren al alcance de materiales inflamables.
- Disponer un plan de contingencia en caso de una catástrofe natural de la misma manera contar con equipos contra incendios.
- Disponer de un servidor especial de contingencia ubicado en otro sector para tener respaldos necesarios.
- Tramitar la garantía de los equipos dañados o comprar los equipos indispensables para la continuidad de las operaciones. Responsable encargado de Soporte y Mantenimiento.
- Se recoge los respaldos de datos, programas, manuales y claves. Responsable encargado de Redes.
- Revisar y probar la integridad de los datos. Responsable encargado de Desarrollo.

11.1.5 El trabajo en áreas seguras.

Con la ejecución de este control se aplicarán los siguientes procesos para ser aplicado en la institución:

- Para el área restringida solo los usuarios que laboren dentro de él tendrán acceso concedido y la ubicación del lugar.
- El usuario externo tendrá limitaciones de existir el caso que sea requerido en esta área y tendrá que ser documentado su ingreso previo a una autorización otorgada por el encargado.
- No se podrá acceder con teléfonos, cámaras fotográficas, bebidas y alimentos.

11.1.6 Áreas de acceso público, carga y descarga.

Con la ejecución de este control se cumplir con los siguientes parámetros:

- El personal que entrega los suministros no podrá acceder a áreas restringidas.
- Las áreas de carga y descarga deben estar alejadas del área de procesamiento de información.
- Mantener un listado de los suministros recibidos y ser revisados, para evitar algún material peligro y poder trasladar de manera segura la encomienda sin problemas al departamento destino.
- Auditoria de los suministros obtenidos y que sean los pedidos por los departamentos y se tenga constancia que son las requeridas.

11.2 Seguridad de los equipos.

11.2.1 Emplazamiento y protección de equipos.

- Los equipos informáticos que tenga como objetivo el procesamiento de la información no se ubicarán en lugares que tenga acceso el público en general, estos deberán resguardados por cámaras y vigilancia autorizada y de limitado acceso de personas.

11.2.2 Instalaciones de suministro.

Con la realización de este control la energía eléctrica se deberá regular adecuadamente, para evitar bajas de electricidad o fallas en los sistemas, debido que ocurra algún inconveniente se deberá contar con equipos UPS que permitirán controlar los sistemas de manera segura en un tiempo limitado dependiendo de la característica del mismo que se encargara de proporcionar el cierre seguro de los sistemas cuando exista problemas de cortes de energía eléctrica.

11.2.3 Seguridad del cableado.

El cableado de red interna de los departamentos contara con las categorías establecidas por el departamento de sistemas y estas deberán pasar por canaletas de plástico para evitar contacto con cables de electricidad que provocarían ruidos y cortes en la transmisión de los datos o paquetes, de la misma manera cada uno estará identificado hacia el patch panel de su departamento y por último se tendría un esquema graficado de cómo está estructurado la red del Departamento de Tecnologías de la Información y Comunicación.

Todos los equipos conectados en la red de la Institución tendrán que seguir una auditoria para tener en cuenta que no tengan algún malware o gusano que pueda ser una amenaza para la información almacenada en los servidores.

11.2.4 Mantenimiento de los equipos.

Con la aplicación de este control se tendrá mantenimiento a las Tecnologías de la Información y Comunicación que manejen información dentro de la Institución según los parámetros establecidos:

- Se realizará una auditoria del manteamiento dando a conocer los posibles daños o cambios realizados a las Tecnologías de la Información y Comunicación de piezas y posibles fallas de cada uno de ellos
- El personal de sistemas se les prohibirá la divulgación de la información almacenada en los equipos que pasen por sus manos al momento de realizarle el mantenimiento.

11.2.5 Salida de activos fuera de las dependencias de la Universidad Técnica de Machala.

El equipo informático de la Universidad Técnica de Machala estará en su área establecido únicamente para cumplir con las labores del usuario.

Si un equipo informático es necesitado fuera de su ubicación de trabajo se deberá pedir una autorización para poder trasladar el equipo, siempre tenerlo a la vista para que no ocurra nada durante su movilización.

El equipo tendrá su encriptación respectiva para la información almacenada y en carpetas ocultas.

11.2.6 Seguridad de los equipos.

Los equipos que hacen parte de la infraestructura tecnológica de la Universidad Técnica de Machala, tales como, servidores, equipos de comunicaciones y seguridad electrónica, centros de cableado, UPS, subestaciones eléctricas, aires acondicionados, plantas telefónicas, así como estaciones de trabajo y dispositivos de almacenamiento y/o comunicación móvil que contengan y/o brinden servicios de soporte a la información crítica de las dependencias, deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, hurto o acceso no autorizado a los mismos.

Los equipos servidores, dispositivos activos de red que contengan información y servicios de carácter institucional, deben ser mantenidos en un ambiente seguro y protegido por los menos con:

- No se deben introducir dispositivos extraíbles como memorias USB, cámaras, entre otros. ya que pueden ser portadores de software malicioso y además se pueden utilizar para copiar información sensible
- Controles de acceso y seguridad física.
- Detección de incendio y sistemas de extinción de conflagraciones.
- Controles de humedad y temperatura.

11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.

Cuando se termine de utilizar un dispositivo de almacenamiento dentro de los departamentos, evitar que se contenga información del departamento de categoría sensible o licencias que puedan servir a futuro, por lo tanto, deberá pasar por el encargado del departamento para realizar una revisión esto servirá para que el dispositivo que contenga la información pueda ser reutilizado nuevamente.

Bajo ninguna circunstancia se dejarán desatendidos los medios de almacenamiento, o copias de seguridad de los sistemas.

La ubicación de los medios de almacenamiento deberá estar alejada de polvo, humedad, o cualquier contacto con material o químicos corrosibles.

11.2.8 Equipo informático de usuario desatendido.

El encargado del Departamento de Tecnologías de la Información y Comunicación realizara auditorias semestrales de los equipos y verificar que cada uno posea su contraseña respectiva, en el caso que el equipo se encuentre mal ubicado es decir en lugares húmedos se deberá realizar el cambio a un lugar seguro que no afecte al equipo.

Del mismo modo el sistema deberá contar con su seguridad de antivirus al día.

11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

Se bloqueará el equipo informático cuando este en inactividad y volverá a requerir el usuario y contraseña del usuario el tiempo recomendado para inactividad seria de 10 min.

El usuario deberá tener en cuenta que si sale de su lugar de trabajo donde se encuentra el equipo deberá bloquear el mismo para evitar que otros usuarios corrompan en su equipo.

En los equipos de procesamiento de información solamente se utilizará medios de almacenamiento extraíbles que sean parten de la Institución con previa revisión y autorización del Departamento de Tecnologías de la Información y Comunicación para evitar fugas de información.

12. SEGURIDAD EN LA OPERATIVA.

La institución, establece que todos los recursos informáticos deben estar protegidos mediante herramientas y software de seguridad como antivirus, antispam, antispyware y otras aplicaciones que brindan protección contra código malicioso y prevención del ingreso del mismo a la red institucional, en donde se cuente con los controles adecuados para detectar, prevenir y recuperar posibles fallos causados por código móvil y malicioso.

Será responsabilidad de la Dirección de Talento Humano autorizar el uso de las herramientas y asegurar que el software de seguridad no sea deshabilitado bajo ninguna circunstancia, así como de su actualización permanente.

Sobre el particular se establece los siguientes lineamientos:

- No se permite la desinstalación y/o desactivación de software y herramientas de seguridad.
- No se permite utilizar medios de almacenamiento físico o virtual que no sean de carácter corporativo o avalado por la administración de la institución.

Recursos compartidos.

Está terminantemente prohibido compartir los discos duros o las carpetas de los computadores de escritorio, aunque estén protegidos por contraseña. Cuando exista la necesidad de compartir recursos esto se debe hacer con autorización previa y restringir por dominio.

- Todo monitoreo debe ser registrado e informado al jefe inmediato del usuario.
- Un usuario puede ser monitoreado bajo previa autorización del comité de seguridad.
- Cuando un funcionario de la institución inicie su relación laboral se debe diligenciar el documento de entrega de inventario.

Prueba por parte del área encargada.

Incorporación de contraseñas en el software. Ninguna contraseña deberá ser incorporada en el código de un software desarrollado o modificado por la institución o sus proveedores, para permitir que las contraseñas sean cambiadas con la regularidad establecida en la política "Cambios periódicos de contraseñas".

Acceso del usuario a los comandos del sistema operativo. Después de haber iniciado una sesión, el usuario debe mantenerse en menús que muestren solo las opciones habilitadas para dicho usuario y de esta manera impedir la ejecución de comandos del sistema operativo y la divulgación de las capacidades del sistema.

Todo sistema que maneje información sensible para la institución debe generar registros de auditoria que guarden toda modificación, adición y eliminación de dicha información.

Diseño de seguridad para aplicaciones. El esquema de seguridad de aplicación, debe elaborarse de acuerdo con las definiciones establecidas para la institución.

Políticas para administradores de sistemas

Soporte para usuarios con privilegios especiales. Todos los sistemas y computadores multiusuarios deben soportar un usuario con privilegios superiores a un usuario normal con el fin de poder ejercer las correspondientes labores administrativas y por lo cual estos privilegios deben ser asignados únicamente a los administradores.

Los privilegios de acceso a los sistemas de información otorgados a un usuario terminan cuando el usuario finaliza su vínculo contractual con la Entidad.

Todos los privilegios sobre los recursos informáticos de la institución otorgados a un usuario deben eliminarse en el momento que éste abandone la institución y la información almacenada queda en manos de su jefe inmediato para aplicar los procedimientos de retención o destrucción de información.

Brindar acceso a personal externo. El ingeniero de soporte y web master velará porque individuos que no sean empleados, contratistas o consultores de la Universidad Técnica de Machala no tengan privilegio alguno sobre los recursos tecnológicos de uso interno de la institución a menos que exista una aprobación escrita por el rectorado.

Acceso a terceros a los sistemas de la institución requiere de un contrato firmado. Antes de otorgarle acceso a un tercero a los recursos tecnológicos de la institución se requiere la firma de un formato, acuerdo o autorización del rectorado. Es obligatoria la firma del acuerdo de confidencialidad.

Privilegios por defecto de usuarios y necesidad de aprobación explícita por escrito.

Sin autorización escrita el personal del departamento de Tecnologías de la Información y Comunicación de la institución, los administradores no deben otorgarle privilegios de administración a ningún usuario.

Manejo administrativo de seguridad para todos los componentes de la red. Los parámetros de configuración de todos los dispositivos conectados a la red deben cumplir con las políticas y estándares internos de seguridad.

Sincronización de relojes para un registro exacto de eventos en la red. Los dispositivos multiusuario conectados a la red interna de la institución deben tener sus relojes sincronizados con la hora oficial.

Monitoreo de Sistemas. Se debe mantener una adecuada aplicación de monitoreo configurada que identifique el mal funcionamiento de los sistemas controlados.

Mantenimiento de los Sistemas. Realizar periódicamente el mantenimiento en las bases de datos, antivirus, servidores de correo y servicios de la institución.

Copias de seguridad. Se deben elaborar más de una copia de seguridad con el fin de minimizar el riesgo por daño del medio de almacenamiento en discos duros, según procedimiento de copias de respaldo.

Tipo de datos a los que se les debe hacer copias de respaldo y con qué frecuencia.
A toda información sensible y software crítico de la institución, residente en los recursos informáticos, se le debe hacer copias de respaldos con la frecuencia necesaria soportada por el procedimiento de copias de respaldo. Se deben hacer pruebas periódicas para garantizar el buen estado de la información almacenada.

12.1 Responsabilidades y procedimientos de operación

12.1.1 Documentación de procedimientos de operación.

- Los procedimientos operativos, instalación, cambios en los servicios que presta la Institución, procedimientos de reinicio de sistemas serán documentados para establecer la calidad y confianza de los servicios de la Institución.

- El Monitoreo de los servidores que amacena la información, correos enviados y la información de errores o problemas operativos ubicados en el Departamento de Tecnologías de la Información y Comunicación deberán ser documentados o archivados para tener un respaldo físico de cada trabajo información obtenida.

12.1.2 Gestión de cambios.

- Se evaluará las posibles implicaciones, estos cambios deben ser requeridos por los usuarios de la información, evaluados y aprobados por el encargado del departamento, los registros de cambios en la infraestructura, implicaciones, aprobación y planificación deberán ser documentadas.

- De la misma manera los cambios que sea realizados en la infraestructura de la Institución deberán ser documentadas.

12.1.3 Notificación de puntos débiles de la seguridad.

- Se implementará una cuenta de correo para soporte, en la que los usuarios podrán reportar vulnerabilidades sospechosas o algún evento fuera de lo común, con toda la información posible para ser analizada.

- La administración de este correo lo deberá realizar los encargados del departamento donde este laborando, en un caso que este fuera de sus manos por una fuerte gravedad, se deberá contactarse con la persona encargada en el departamento de sistemas en un plazo máximo de 48 horas, para recopilar la información necesaria para el análisis del problema.

  En el ANEXO 9 se encuentra el formulario de "Tratamiento y valoración de incidentes".

12.1.4 Separación de entornos de desarrollo, prueba y producción.

El entorno de ambiente para el desarrollo será en lugares de acceso restringido para evitar que el código fuente de los sistemas en proceso de desarrollo sean de libre acceso, de la misma manera los encargados de desarrollar las plataformas deberán documentar sus accesos en cada proyecto para evitar personas no autorizadas ingresen a los mismo y ocasionen perdidas de información.

12.2 Protección contra código malicioso.

Los departamentos y usuarios no deben instalar software no autorizado por el departamento de sistemas, ya que este puede ser ilegal o el peor de los casos malicioso y podría causar inconvenientes en los equipos donde se realice la instalación incluso a los servidores de la Institución.

Para evitar todo tipo de inconveniente con se deberá optar por la lista de software previamente identificado por el departamento de sistemas que se encargaría de revisar si contiene algún código malicioso.

El Departamento de Tecnologías de la Información y Comunicación es el encargado de realizar el monitoreo y actualización de los programas y los usuarios deberán reportar a este departamento sobre cualquier problema.

El software que venga de empresas no reconocidas o acreditadas como no confiables, no tendrá ningún valor alguno para la Institución siempre que sea en formato ejecutable.

12.3 Copia de seguridad

12.3.1 Copias de seguridad de la información.

- Las copias de seguridad de la información y los respaldos deben estar correctas y sin errores, la cual se designará a un encargado del departamento de sistemas para llevar acabo la tarea.

Para llevar acabo los respaldos de la información se lo realizara en un lugar adecuado y acondicionado tomando en cuenta los parámetros siguientes:

- Asignar un manual de procedimientos para definir el tipo de respaldo que se requiere para cada sistema y como volver a restaurarlos dependiendo del nivel de criticidad o confidencialidad de información que contenga tendrá su respectivo grado de encriptación.

- Los respaldos se obtendrán en dispositivos grandes de almacenamientos, ejemplo: Discos duros extraíbles, servidores, etc.

Es por esto que se realizaran los Backups a los sistemas de información aplicado por una referencia:

- Respaldo de información de movimiento entre los periodos que no se sacan backups es decir en días no laborales, feriados, etc.
- Uso obligatorio de un formulario de control de ejecución del programa de backups diarios, semanales y mensuales.
- Sistemas desarrollados en el Departamento de Tecnologías de la Información y Comunicación.
- Sistema de control Biométrico de recursos humanos (cada 15 días en el computador del analista informático y cada mes a recursos humanos).

En el ANEXO 8 se encuentra el formulario de “registro de Backups”.

12.4 Registro de actividad y supervisión

12.4.1 Registro y gestión de eventos de actividad.

Dentro de las bases de datos se crearán consultas que permita al usuario en el momento de crear, editar o eliminar se actualicen las auditorias automáticamente, estas deberán estar bien desarrolladas evitando fallas que puedan producirse en el sistema.

12.4.2 Protección de los registros de información.

Los usuarios deben tener definidos sus actividades y los permisos otorgados para la manipulación de información y asignación de roles dependiendo de la labor del empleado, adicional el sistema deberá proporcionar el acceso a varios usuarios simultáneamente.

12.4.3 Registros de actividad del administrador y operador del sistema.

Los encargados del departamento de tecnología de la información y Comunicación llevarán un registro de las actividades en donde reflejara la hora, la actividad realizada, usuarios y adicionales en caso de ser necesario es necesario que dentro de las bases de datos se agregue una tabla para los procedimientos de auditoria.

12.4.4 Sincronización de relojes.

Tener un reloj principal con la hora exacta según la zona horaria para la región continental de Ecuador, el que no se debe cambiar por ningún motivo, esto permitirá que las transacciones realizadas en los sistemas de información y bases de datos se realicen a la hora exacta.

12.5 Control del software en explotación.

12.5.1 Instalación del software en sistemas en producción.

Los usuarios involucrados serán notificados con anterioridad del cambio el mismo, y asegurar que el cambio no afecte las funcionalidades de los sistemas de información, es decir que para realizar un cambio en los equipos de los empleados o encargado por parte del departamento de sistema se deberá avisar con anticipación a los mismos para que estos puedan respaldar su información por seguridad.

12.6 Gestión de vulnerabilidad técnicas.

12.6.1 Gestión de las vulnerabilidades técnicas.

Se asignará un responsable en el Departamento de Tecnologías de la Información y Comunicación que se encargará de monitorear y explorar vulnerabilidades que puedan transcurrir en los departamentos de la Institución, para poder evitar problemas en los equipos y sistemas instalados.

En el momento que se detecte una vulnerabilidad se tomara acciones y se realizara un análisis para poder evitar que exista ese túnel de acceso, para esto se deberá actualizar parchar o configurar de mejor manera los servicios que presenten este inconveniente.

12.6.2 Restricciones en la instalación de software.

Se permanecerá en constante observación el monitoreo de las Tecnologías de la Información y Comunicación de la Institución desde el Departamento de Tecnologías de la Información y Comunicación, también se verificará que los equipos cuenten con el sistema autorizado por el departamento incluso el software que deberán ocupar para su labor de trabajo, se manejara bloqueos de juegos o material inapropiado que distraiga al usuario.

12.7 Consideraciones de las auditorías de los sistemas de información.

12.7.1 Controles de auditoria de los sistemas de información.

Con el cumplimiento de este control punto de seguridad de la información se considera necesario la auditoria interna y externa para optimizar su funcionamiento.
Las auditorias deben tener los siguientes registros (Ver Tabla 38)

Tabla 38. Control de Auditoria

a	Id de Usuario
b	Hora y fecha de ingreso y salida
c	Hora y fecha de actualización
d	Dirección Ip
e	Nombre del equipo donde se realizó la sesión
f	Obtener un registro de accesos fallidos y de ingresos.
g	Monitoreo de los accesos a utilidades, aplicaciones y departamentos.
h	Protección de anti-malware, anti-virus y firewall.

Elaborado por: *Investigador*

13 SEGURIDAD EN LAS TELECOMUNICACIONES.

Se debe garantizar que el servicio de red utilizado por la institución se encuentre disponible y operando adecuadamente, el administrador del sistema o una persona autorizada por el jefe de sistemas puede efectuar escaneos de la red con la finalidad de: resolver problemas de servicio, como parte de las operaciones normales del sistema y del mantenimiento, para mejorar la seguridad de los sistemas o para investigar incidentes de seguridad.

Revisión de accesos de usuarios. Se debe realizar por control de auditoría la revisión de accesos de usuarios a las aplicaciones utilizadas, por lo menos dos veces por año.

Gestión de la seguridad en las redes. La configuración de los dispositivos activos de red, debe estar siempre documentada, se deberá tener copia de respaldo de las configuraciones. Todos los equipos de tecnología deben estar registrados y aplicarles permanentemente mantenimientos preventivos.

Para el fin pertinente se deben cumplir las siguientes premisas:

- Los mensajes y la información contenida en los buzones del correo electrónico son propiedad de la institución, y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.

- No se permite la utilización de la dirección de correo electrónico de la institución, como punto de contacto en comunidades interactivas, redes sociales, tales como Facebook, twitter, entre otras, o cualquier otro sitio que no tenga que ver con las actividades institucionales.

- Se deberá realizar segmentación de dominios de broadcast, para separar cada instancia de la institución, fraccionando un segmento para funcionarios, docentes, estudiantes, invitados; esto deberá aplicar para la red cableada e inalámbrica y un segmento para teléfonos inteligentes.

Recursos tecnológicos: la instalación o desinstalación de cualquier elemento software o hardware en los equipos de cómputo de la institución, es responsabilidad del funcionario encargado del manejo de los elementos tecnológicos, y por tanto será el único autorizado para realizar esta labor. Así mismo, los medios de instalación de software deben ser los proporcionados por la institución a través del departamento de Tecnologías de la Información y Comunicación.

- Los usuarios no deberán realizar modificaciones en los dispositivos de cómputo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales del dispositivo, fondo de escritorio y protector de pantalla institucional, entre otros. Estos cambios pueden ser realizados únicamente por el funcionario encargado de los recursos de Tecnología.

- Sólo usuarios autorizados pueden realizar actividades de administración remota de dispositivos de red, equipos de cómputo o servidores de la infraestructura de procesamiento de información; las conexiones establecidas para este fin, deben utilizar los esquemas y herramientas de seguridad y administración que garanticen los principios básicos de seguridad de la información.

Políticas de uso de firewall.

Detección de intrusos. Los segmentos de red accesible desde Internet deben tener un sistema de detección de intrusos (IDS) para tomar acción oportuna frente a ataques.

Toda conexión externa debe estar protegida por el firewall. Toda conexión a los servidores de la institución proveniente del exterior, sea internet, acceso telefónico o redes externas debe pasar primero por el firewall. Esto con el fin de limitar y controlar las puertas de entrada a la organización.

Filtrado de contenido activo en el proxy. El departamento de Tecnologías de la Información y Comunicación debe asegurar que, dentro de las definiciones de políticas de proxy, se filtre todo contenido activo como applets de java, adobe flash player, controles de ActiveX debido a que estos tipos de datos pueden comprometer la seguridad de los sistemas de información de la Universidad Técnica de Machala.

Sincronización de relojes para un registro exacto de eventos en la red. Los dispositivos multiusuario conectados a la red interna deben tener sus relojes sincronizados con la hora oficial.

Reglas de uso de la Intranet. La institución utiliza la intranet como un recurso de publicación de los documentos que rigen la relación entre ésta y el empleado o trabajador. Por lo tanto, el empleado debe consultar la intranet permanentemente, así como todos los documentos que en ella se encuentran publicados.

Prohibición de publicitar la imagen de la Universidad Técnica de Machala en sitios diferentes a los institucionales. La publicación de logos, marcas o cualquier tipo de información sobre la institución o sus actividades en internet solo podrá ser realizada a través de las páginas institucionales de la misma y previa autorización del rectorado. En consecuencia, se encuentra terminantemente prohibido el manejo de esta información en páginas personales de los empleados.

Prohibición para establecer conexiones a los sitios web de la Universidad Técnica de Machala.

Está prohibido igualmente establecer enlaces o cualquier otro tipo de conexión a cualquiera de los sitios web de la institución por parte de los empleados y de sus sitios web o páginas particulares, salvo previa autorización del rectorado, dependiendo del caso. Particularmente se encuentra prohibido el establecimiento de links o marcos electrónicos, y la utilización de nombres comerciales o marcas de propiedad de la Entidad en sitios diferentes a los institucionales o como meta-etiquetas.

Prohibición de anuncios en sitios web particulares.

Está terminantemente prohibido anunciarse en los sitios web particulares como empleados de la Universidad institución o como sus representantes, o incluir dibujos o crear diseños en los mismos que lleven al visitante del sitio web a pensar que existe algún vínculo con la institución.

13.1. Gestión de la seguridad en las redes

13.1.1 Controles de red.

Con la aplicación de este control el departamento de sistemas se encargará de monitorear las redes y administrarlas, garantizando que la información transmitida sea segura para los usuarios y evadir los accesos no permitidos.

Para ello debemos cumplir con los siguientes requerimientos:

- Tener un registro de acceso a la red para controlar las actividades realizadas.
- Para los equipos de conectividad hay que cambiar las configuraciones por defecto. Además,
- Se deberá cerrar la sesión durante 30 segundos de inactividad.
- Guardar registros de auditoria.
- Sacar respaldos de configuración de los switchs y routers en el caso de ser inalámbricos que se utilicen en los departamentos de la Institución.

13.1.2 Mecanismos de seguridad asociados a servicios en red.

- El encargado del Departamento de Tecnologías de la Información y Comunicación tendrá que cumplir la tarea de monitoreo en el rendimiento y capacidad de los servicios que tienen contratados por proveedores, los servicios deberán incluir VPN, firewall, anti intrusos que se desarrollaran dentro de la Institución o serán adquiridos de manera externa.

- Los servicios de red deben tener controles de autentificación, acceso, cifrado y requerimientos para una conexión segura establecida.

13.1.3 Segregación de redes.

Los segmentos utilizados en la red dentro de la Institución serán documentados con un perímetro de seguridad, adicional se deberá configurar redes virtuales, políticas de control de acceso complementadas con puertas de enlace y firewall.

Al segregar las redes a través de enrutamiento y switching se tendrá como resultado un mejor manejo del tráfico entre los segmentos y sus configuraciones del mismo. Dentro de la Institución se podrá segregar las redes por Vlan para todos los departamentos que la conformen.

13.2 Intercambio de información con partes externas

13.2.1 Políticas y procedimientos de intercambio de información.

Se tendrá el medio de transmisión de la información al momento de transferirla a organismos externos, si es de manera manual se entregará personalmente al destinatario en un sobre sellado.

Si el intercambio es vía email se realizará por el correo de la plataforma de la Institución y la información enviada debe contener una advertencia en cuanto al uso y autorizaciones de uso de la información, quedando la responsabilidad de cuidado y resguardo de la información sobre el receptor.

Si el intercambio es por otro medio cumplirá la política de control de acceso y seguridad de red.

Si el intercambio de información es entre sistemas se debe realizar decretos externos este documento aprueba y define la prestación de servicios mutuos para su cumplimiento de las obligaciones, costos, incumplimientos y responsabilidades, este representada como un documento público que aprueba el convenio de cooperación o de interoperabilidad.

13.2.2 Acuerdos de intercambio.

La información que se va a transferir pasará por una previa autorización, y esta deberá transmitir solo la información requerida.

Si la trasmisión es vía email será encriptada establecida con acuerdos de confidencialidad de la información entre departamentos externos e internos.

13.2.3 Mensajería electrónica.

Se implantará el correo institucional para la institución para poder enviar y recibir información donde el Departamento de Tecnologías de la Información y Comunicación mantendrá el monitoreo del servidor de correo, se verán obligados todos los empleados a utilizar este medio de comunicación dentro de su lugar de trabajo.

13.2.4 Acuerdos de confidencialidad y secreto.

El encargado del Departamento de Tecnologías de la Información y Comunicación designará la responsabilidad que permitirá la revisión continua de los acuerdos de confidencialidad a los encargados de cada departamento de la institución, la cual podrá revisar, analizar y podrán realizar los cambios en los acuerdos.

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.

14.1 Requisitos de Seguridad de los Sistemas de Información.

El software de aplicaciones y software de base sólo debe ser puesto en producción después de ser probado; se deben incluir pruebas sobre la funcionalidad, la seguridad, los efectos sobre otros sistemas y las facilidades de usuario, y deben ser realizadas en ambiente de pruebas. Requisitos de seguridad de los sistemas de información.

14.1.1 Análisis y especificación de los requisitos de seguridad.

El análisis y diseño de los sistemas que funcionan en la institución, deberán contar con mecanismos de seguridad de la información cumpliendo además de los requerimientos del usuario final. Se deberá analizar los riesgos posibles antes de la implementación definiendo así los procedimientos apropiados de seguridad.

14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.

Se protegerá la información que pasa a través de las aplicaciones que utilizan redes públicas para transferirla, mediante la encriptación evitando el ingreso no autorizado, el departamento de sistemas analizara los servicios de redes públicas para evaluar los riesgos y vulnerabilidades, dando la mejor solución para proteger la información.

14.1.3 Protección de las transacciones por redes telemáticas.

Se realizará revisiones continuas de los sistemas verificando su correcto funcionamiento y el almacenamiento de la información, obteniendo los resultados del almacenamiento correcto evitando errores, clonación de la información.

14.2 Seguridad de los procesos de desarrollo y soporte

14.2.1 Política de desarrollo seguro de software.

Se tendrá un estándar del desarrollo del software a través de ciclos, dependiendo de la metodología, estándares de seguridad y calidad aplicada en la institución donde todas estas políticas estarán documentadas y autorizadas por el departamento de sistemas.

Los programadores serán responsables de la seguridad del proyecto o del entorno de soporte y deben garantizar que todas las propuestas de cambio en los sistemas serán revisadas para verificar que no comprometan la seguridad del sistema y exista fuga de información.

14.2.2 Procedimientos de control de cambios en los sistemas.

Los cambios deben ser pasados por escrito al personal del Departamento de Tecnologías de la Información y Comunicación en el caso que se necesite modificar datos, se deberá tener en cuenta la autorización e identificación de los elementos que se modificaran como base de datos, hardware o software.

Se tendrá una auditoria sobre encargados en realizar este tipo de labor dentro del Departamento de Tecnologías de la Información y Comunicación ya que solo en este lugar se llevaría a cabo donde serán aprobados y probados.

En el momento de realizar los cambios se debe garantizar que no sea interrumpida la labor de los servicios que operan en los departamentos, adicional se comunicara con anticipación cobre los cambios a todo el personal del departamento donde se lo realizara.

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

Se realizará pruebas de funcionamiento a la vez serán monitoreados donde sea necesario de actualizaciones o modificaciones, esto se deberá realizar sin interrupciones en el sistema.

14.2.4 Restricciones a los cambios en los paquetes de software.

El encargado del Departamento de Tecnologías de la Información y Comunicación evaluara las modificaciones de los paquetes que necesiten cambios si son necesario, esto no afectaran la integridad, confidencialidad y disponibilidad de la información, los cambios realizados serán autorizados por el encargado del departamento de sistema.

14.2.5 Uso de principios de ingeniería en protección de sistemas.

El encargado del Departamento de Tecnologías de la Información y Comunicación asignará al responsable para la investigación e implementación de los principios de seguridad este deberá analizar previamente los sistemas de información para su implementación.

14.2.6 Seguridad en entornos de desarrollo.

Se creará un entorno para el desarrollo de software adecuado, según las políticas de control de acceso y seguridades físicas y ambientales para los equipos que se utilizaran para el desarrollo, además el ambiente deberá ser confortable para realizar la labor siendo del agrado de los desarrolladores.

14.2.7 Externalización del desarrollo de software.

El responsable del monitoreo de las actividades de desarrollo estará al pendiente de las actividades del desarrollo del software externas, es importante que los involucrados en el proyecto tengan en cuenta la creación, innovación, producto u objeto que se desarrolló dentro de la Institución será propiedad exclusiva de la misma.

Todo los productos o programas externalizados deberán ser entregados en el tiempo acordado, incluyendo manuales, descripción técnica y documentación respectiva.

14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.

Se tendrá una lista de planificación de pruebas con usuarios que pertenezca a los departamentos en el caso que sea el sistema para el correspondiente, donde se evaluará los niveles de seguridad en los sistemas y se podrá tomar decisiones a través de los criterios para proteger la información, y se deberá documentar todo lo realizado con sus fechas respectivas y observaciones que hayan manifestado los usuarios.

14.2.9 Pruebas de aceptación.

Se coordinará un responsable para elaborar un plan de pruebas que deberá ser autorizado y aprobado por el encargado del Departamento de Tecnologías de la Información y Comunicación, en el proceso de las pruebas estas deberán dar las incidencias, mejoras, detección de vulnerabilidades y serán registras en un documento o acta.

En el ANEXO 7 se encuentra el formulario de “los sistemas de información”.

14.3 Datos de prueba

14.3.1 Protección de los datos utilizados en pruebas.

- El acceso a la base de datos formal será restringido para hacer pruebas, en el caso de requerir una base de datos generar una con una herramienta que sea prueba o de la misma manera realizar un backup de la misma y notificar que será utilizada para un proyecto en desarrollo

15. RELACIONES CON LOS SUMINISTRADORES.

Acceso a terceros a los sistemas de la institución requiere de un contrato firmado. Antes de otorgarle acceso a un tercero a los recursos tecnológicos se requiere la firma de un formato, acuerdo o autorización del rectorado. Es obligatoria la firma del acuerdo de confidencialidad.

Acuerdos con terceros que manejan información o cualquier recurso informático de la institución. Todos los acuerdos relacionados con el manejo de información o de recursos de informática de la institución por parte de terceros, deben incluir una cláusula especial que involucre confidencialidad y derechos reservados. Esta cláusula debe permitirle a la institución ejercer auditoría sobre los controles usados para el manejo de la información y específicamente de cómo será protegida la información.

Definición clara de las responsabilidades de seguridad informática de terceros. Socios de convenios, proveedores, docentes y otros asociados a los procesos de la institución deben tener conocimiento de sus responsabilidades relacionadas con la seguridad informática y esta responsabilidad se debe ver reflejada en los contratos con la institución y verificada por el rectorado, el responsable del manejo de estos terceros deberá realizar un acompañamiento controlado durante su estadía en las instalaciones de la institución, y de esta manera podrá verificar la calidad en la entrega de los servicios contratados.

Uso del aplicativo entregado. La Universidad Técnica de Machala ha suscrito con el investigador un contrato de "LICENCIA DE USO" para los aplicativos que utiliza. Está terminantemente prohibido copiar cualquiera de los aplicativos que se aloja en los computadores de la institución, esto se asegura con la firma del Acuerdo de Confidencialidad para los usuarios y con la firma del contrato realizado con los proveedores que maneje información de uso restringido a la institución, adicional a esto cada usuario, dependiendo de las actividades que realice sobre las aplicaciones maneja un perfil limitado, de esta forma es controlado el acceso.

El usuario es responsable por toda actividad que involucre su identificación personal o recursos informáticos asignados. Todo usuario es responsable por todas las actividades relacionadas con su identificación. La identificación no puede ser usada por otro individuo diferente a quien esta le fue otorgada. Los usuarios no deben permitir que ninguna otra persona realice labores bajo su identidad.

De forma similar, los usuarios no deben realizar actividades bajo la identidad de alguien más. La utilización de los recursos informáticos por parte de terceras personas con conocimiento o consentimiento del usuario, o por su descuido o negligencia, lo hace responsable de los posibles daños que estas personas ocasionen a los equipos o a la propiedad de la Universidad Técnica de Machala.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN

Personal del Departamento de Tics. El personal del departamento de Tics de la Universidad Técnica de Machala está conformado por un equipo de trabajo interdisciplinario encargado de garantizar una dirección clara y brindar apoyo visible al rectorado con respecto al programa de seguridad de la información dentro de la institución.

Las siguientes son las principales responsabilidades a cargo del personal del departamento de Tics, dentro de la institución:

- Revisión y seguimiento al modelo de seguridad (SGSI) a implementar en la institución. Revisión y valoración de la Política de Seguridad de la Información.
- Alineación e integración de la seguridad a los objetivos de la institución.
- Reportar, a través de reuniones semestrales al rectorado el estado de la seguridad y protección de la información en la institución y la necesidad de nuevos proyectos en temas de seguridad de la información.
- Evaluar la adecuación, coordinación y la implementación de los controles de seguridad específicos para nuevos servicios o sistemas de información.

Adicionalmente, el personal del departamento de Tecnologías de la Información y Comunicación de la Institución tiene la responsabilidad de tratar los siguientes temas (por demanda):

- Mejoras en las actividades inherentes a la seguridad de la Universidad Técnica de Machala y sus procesos.
- Seguimiento a la aplicación de las políticas, programas y planes adoptados para la protección de los sistemas, recursos informáticos y servidores de la red interna y centros de cómputo de la institución.
- Decisiones de carácter preventivo y proactivo que apunten a la optimización de la seguridad de los procesos y sus procedimientos.

Cambio en los roles del ciclo de certificación.

- Participación activa en la revisión, evaluación, mantenimiento, recomendaciones, mejoras y actualizaciones de la presente política de la Universidad Técnica de Machala, el rector convoca al Director del Departamento de Tics con el propósito de evaluar los cambios a la presente política y autorizar su publicación. Con el Director de Tics se deja acta como constancia de su evaluación y aprobación.

- Las actas del personal del departamento de departamento de Tecnologías de la Información y Comunicación podrán ser anuladas por rectorado mediante el uso de un Acta que invalide el contenido siempre y cuando no se haya(n) ejecutado la(s) acción(es) relacionadas.

16.1 Gestión de incidentes de seguridad de la información y mejoras.

16.1.1 Responsabilidades y procedimientos.

Se capacitará a todos los empleados de los departamentos de la Institución, sobre la funcionalidad de los sistemas de información para que puedan informar sobre un evento o vulnerabilidad que sea encuentre y que pueda afectar a la seguridad de la información de su área de trabajo o a nivel general.

El encargado del Departamento de Tecnologías de la Información y Comunicación será el responsable de aplicar los procedimientos necesarios para gestionar los incidentes de la información de todo tipo en todo el palacio municipal.

16.1.2 Notificación de los eventos de seguridad de la información.

El encargado del Departamento de Tecnologías de la Información y Comunicación debe notificar a los encargados de los diferentes departamentos acerca de los eventos de seguridad de la información implementados o que serán actualizados para evitar errores al manipular la información.

Se notificará a través de vía correo electrónico de la institución o grupos creados en las redes sociales en el caso que los empleados no tengan conocimientos sobre cómo utilizar estos medios se debe realizar capacitaciones para la sociabilización.

16.2.3 Notificación de puntos débiles de la seguridad.

Se implementará una cuenta de correo para soporte, en la que los usuarios podrán reportar vulnerabilidades sospechosas o algún evento fuera de lo común, con toda la información posible para ser analizada.

La administración de este correo lo deberá realizar los encargados del departamento donde este laborando, en un caso que este fuera de sus manos por una fuerte gravedad, se deberá contactarse con la persona encargada en el departamento de sistemas en un plazo máximo de 48 horas, para recopilar la información necesaria para el análisis del problema.

En el ANEXO 8 se encuentra el formulario de “Tratamiento y valoración de incidentes”.

Luego de la recolección de la información del inconveniente el encargado del Departamento de Tecnologías de la Información y Comunicación deberá analizar los recopilados.

16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.

Con la realización de este control es obligatorio aplicar la política de notificación de puntos vulnerables de la seguridad, el siguiente paso será el análisis y podemos clasificarla de la siguiente manera:
Se trata de una amenaza: se informa y reporta sobre una amenaza y se cierra el registro.

Se trata de una debilidad: se realiza los procedimientos necesarios con el área o departamento y activos comprometidos, dejando constancia mediante el registro de la plantilla para el tratamiento y valoración de incidentes.

Se Produjo y debe ser clasificado como un incidente: se activa el proceso de gestión de incidentes.

16.1.5 Respuesta a los incidentes de seguridad.

Con el cumplimiento de este control el encargado de cada departamento deberá notificar sobre los inconvenientes el cual tendrá un periodo de 48 horas para comunicarse con el empleado que lo notifico y seguir con los procedimientos para su análisis y deberá desarrollar acciones inmediatas como:

Iniciar los procedimientos para evitar que se propaguen los daños o efectos del inconveniente.

Reclasificar los inconvenientes de acuerdo a la política de valoración de eventos de seguridad de la información.

Tener el registro recopiladas durante su gestión a través de evidencias.

Documentar todo sobre el problema ocurrido para tomar decisiones en caso de que vuelva a ocurrir.

16.1.6 Aprendizaje de los incidentes de seguridad de la información.

El encargado del Departamento de Tecnologías de la Información y Comunicación deberá hacer una revisión periódica de los problemas atendidos en un periodo de tiempo, teniendo en cuenta los inconvenientes que han ocurrido con frecuencia en la información, teniendo en cuenta el resultado obtenido, solución y tratamiento dependiendo del tipo, volumen y costo de los incidentes.

16.1.7 Recopilación de evidencias.

Es obligatorio documentar los incidentes de acuerdo a la plantilla para el tratamiento y valoración del inconveniente, el documento original deberá ser documentado y crear una bitácora digital de los incidentes y su solución para facilitar el acceso a la información y la búsqueda.

17. ASPECTOS DE LA SEGURIDAD DE LA INFORMACIÓN EN LA GESTION DE LA CONTINUIDAD DEL NEGOCIO.

17.1 Continuidad de Gestión institucional: La gestión continua de la información es un factor preponderante, porque los procesos que se desarrollan dentro de una organización no puede detenerse, salvo algunos casos excepcionales, pero se debe enfrentar los elementos que ocasionan las suspensión de las acciones, entre los cuales se destacan los problemas de sistemas ocasionados por usuarios o ataques, catástrofes de origen natural y cualquier otro elemento que atente con los sistemas de información y comunicación.

- Procedimientos de contingencia. Los cuales describen las acciones a tomar cuando ocurre un incidente que interrumpe las operaciones de la institución, proporcionando mecanismos alternos y temporales para continuar con el procesamiento.

- Procedimientos de retorno. Los cuales describen las acciones a seguir para regresar las operaciones normales a las instalaciones originales.

- Procedimientos de recuperación. Los cuales describen las acciones a seguir para trasladar las actividades de la institución a un centro alterno de recuperación.

Políticas Generales de la Presidencia

Evaluación y tratamiento del riesgo. La evaluación de riesgos debe identificar, cuantificar y priorizar los riesgos frente a los criterios de aceptación del riesgo y los objetivos pertinentes para la institución. Los resultados deben guiar y determinar la acción de gestión adecuada y las prioridades tanto para la gestión de los riesgos de seguridad de la información como para implementar los controles seleccionados para la protección contra estos riesgos.

Se debe realizar una evaluación de riesgos a los recursos informáticos de la Universidad Técnica de Machala por lo menos una vez al año utilizando el procedimiento Interno: “Análisis de riesgos”

Entrenamiento compartido para labores técnicas críticas. Al menos dos personas deben tener la misma capacidad técnica para la adecuada administración de los sistemas de información críticos de la institución.

Preparación y mantenimiento de planes para la recuperación de desastres y para respuesta a emergencias. Los sistema o recurso informático deben definir un plan de contingencia para la restauración de la operación. Se debe preparar, actualizar y probar periódicamente un plan para la recuperación de desastres que permita que sistemas y computadores críticos puedan estar operativos en la eventualidad de un desastre.

De igual forma se debe crear planes de respuesta a emergencia con el fin de que se pueda dar una pronta notificación de problemas y solución a los mismos en la eventualidad de emergencias informáticas.

Chequeo de virus en archivos recibidos en correo electrónico. la institución debe procurar y disponer de los medios para que todos los archivos descargados de internet sean chequeados por un software de detección de virus informático, antes de ser transferidos a los computadores de los usuarios.

17.1.1 Planificación de la continuidad de la seguridad de la información.

El encargado del Departamento de Tecnologías de la Información y Comunicación se compromete a continuar con el plan de seguridad de la información, identificando y comprendiendo las vulnerabilidades que pueda estar expuesta la Institución, la misma tendrá en cuenta las interrupciones en el funcionamiento correcto de los sistemas de información, en tal caso, que un incidente ocurra se tomara en cuenta las precauciones de gestión de riesgos.

17.1.2 Implantación de la continuidad de la seguridad de la información.

Se identificará los recursos humanos, tecnológicos ambientales y financieros para garantizar los recursos mencionados estos deberán ser archivados para garantizar el nivel de seguridad de la información, este se detallará en responsabilidades, funcionalidades y actividades en caso de situaciones adversas a todos los trabajadores que participe en el sistema de seguridad de la información.

17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

Se verificará los controles cada 6 meses, se debe ejecutar pruebas que involucren a los empleados de todos los departamentos y garantizar que estén capacitados con los conocimientos ante una situación advera.

Para ponerlo en práctica se podrá realizar un simulacro con las consecuencias reales, para verificar la eficacia y realidad de los controles y se la conclusión de la prueba será registrada para seguir mejorando con nuevas acciones.

17.2 Redundancias.

17.2.1 Disponibilidad de instalaciones para el procesamiento de información.

Se planificará y se realizará los planos necesarios para la construcción de un área de procesamiento de información donde se verá involucrada nuevas tecnologías y la implementación de nuevos equipos, estas instalaciones de procesamiento de información deben estar aptas para la implementación de controles de seguridad.

18. CUMPLIMIENTO.

Todo uso y seguimiento a los recursos del departamento de Tecnologías de la Información y Comunicación, debe estar de acuerdo a las normas y estatutos internos, así como a la legislación nacional en materia.

Cumplimiento con la seguridad de la información. Todos los colaboradores de la institución, así como los contratistas, deben cumplir y acatar el manual de políticas y los procedimientos en materia de protección y seguridad de la información. Corresponde velar por su estricto cumplimiento al rectorado y al jefe de sistemas.

Medidas disciplinarias por incumplimiento de políticas de seguridad. Todo incumplimiento de una política de seguridad de la información por parte de un funcionario o contratista, así como de cualquier estándar o procedimiento es causa para iniciar acciones disciplinarias, las cuales de acuerdo a su gravedad pueden suponer la terminación de la vinculación laboral del empleado o contratista.

Si el incumplimiento se origina en alguna sede de la institución, esta podrá suspender la prestación de cualquier servicio de información.

Protección por Defecto de Copyright. Todos los colaboradores de la institución deben revisar, e investigar los derechos de propiedad intelectual para todo material como libros, artículos, informes, imágenes, software y/o sitio web encontrado en internet antes de ser usado para cualquier propósito con el fin de asegurar el cumplimiento de las leyes que aplican para este tipo de información.

Actualización, mantenimiento y divulgación de políticas de seguridad de la información.

El presente modelo de seguridad (SGSI) debe ser constantemente analizado y evaluado en periodos programados para corroborar que está cumpliendo con las funciones para el cual fue implementado, de esta manera se garantiza la excelente gestión de la seguridad de información de la institución.

Las siguientes son las principales responsabilidades a cargo del personal del departamento de Tecnologías de la Información y Comunicación:

Revisión y seguimiento al modelo de seguridad (SGSI) a implementar en la Universidad Técnica de Machala. Revisión y valoración de la Política de Seguridad de la Información.

Alineación e integración de la seguridad a los objetivos de la Universidad Técnica de Machala.

Garantizar que la gestión de la seguridad de la información forma parte integral del proceso de planeación estratégica de la institución. Establecer las funciones y responsabilidades específicas de seguridad de la información para la institución.

Promover explícitamente el apoyo de la institución a la seguridad de la información en toda la institución.

Analizar y autorizar cualquier tipo de movimiento o traslado de equipos de misión crítica para la institución.

Mejoras en las actividades inherentes a la seguridad de la institución y sus procesos.
Seguimiento a la aplicación de las políticas, programas y planes adoptados para la protección de los sistemas, recursos informáticos y servidores de la red interna y

departamento de Tecnologías de la Información y Comunicación.

Cambio en los roles del ciclo de certificación.

Participación activa en la revisión, evaluación, mantenimiento, recomendaciones, mejoras y actualizaciones de la presente política de la Universidad Técnica de Machala, el rector convoca al jefe de sistemas con el propósito de evaluar los cambios a la presente política y autorizar su publicación. De esta reunión se deja acta como constancia de su evaluación y aprobación.

Las decisiones del jefe de sistemas son protocolizadas mediante un acta firmada por todos los miembros del departamento de Tic de la institución.

Oficial de Seguridad de la Información.

Identificar y satisfacer las necesidades de capacitación en temas de seguridad de la información a los funcionarios de la institución.

Actualización y seguimiento periódico al mapa de riesgos de la institución, validando con cada proyecto que se implemente como afecta el mapa de riesgos y tomando siempre como base este mapa para cualquier proyecto nuevo que se implemente.

Crear y establecer una metodología de clasificación de la información según su importancia e impacto dentro de la institución. Igualmente debe informarla a la institución y validar que se cumpla. La metodología debe establecer niveles de acceso a la información.

Crear y mantener un programa de concientización en seguridad de la información.
Evaluar en forma continua la efectividad de la seguridad de la información de la institución con el propósito de identificar oportunidades de mejoramiento y necesidades de capacitación.

Documento que certifica la entrega del Plan de Políticas (SGSI) a la Universidad Técnica de Machala (Anexo 10).

18.1 Cumplimiento de los requisitos legales y contractuales.

18.1.1 Identificación de la legislación aplicable.

Uno de los encargados del departamento de Tecnologías de la Información y Comunicación mantendrá actualizada y adaptara las normas y estatutos legales que rigen en el país en especial las que involucran tratamiento de información y/o tengan relación con la tecnología de la información.

18.1.2 Derechos de propiedad intelectual (DPI).

Una de las personas encargadas del departamento de Tecnologías de la Información y Comunicación y las normas y estatutos también tendrá conocimiento de los requisitos legislativos, normativos y contractuales de la propiedad intelectual que permitirán el desarrollo y/o creación, implementaciones de software.

18.1.3 Protección de los registros de la organización.

Los reglamentos, normas y estatutos de la Institución serán actualizados, a través del personal encargada de este ámbito que se encuentre al tanto de esta información, y deberá mantener una capacitación de los reglamentos pertinentes.

18.1.3 Protección de datos y privacidad de la información personal.

Las bases de datos de la Institución contarán con protección para los usuarios que permitirán asegurar los datos. Adicional todos los equipos de cómputo pertenecientes a los diferentes departamentos de la institución y que son utilizados por el personal estarán protegidos contra accesos no autorizados.

18.1.4 Regulación de los controles criptográficos.

Se diseñarán políticas de seguridad que involucren controles criptográficos que permitan salvaguardar la información ante manipulación no autorizada, utilizando un algoritmo de encriptación.

18.2 Revisiones de la seguridad de la información

18.2.1 Revisión independiente de la seguridad de la información.

Se realizará un análisis de las políticas que dará como resultado preservar los niveles de seguridad de la información. Este análisis debe ser realizado por el Departamento de Tecnologías de la Información y Comunicación de la Universidad Técnica de Machala y que se obtendrá las políticas de seguridad que se deben aplicar dentro de la organización, partiendo de los niveles de criticidad acceso y la ubicación física de las Tecnologías de la Información y Comunicación.

18.2.2 Cumplimiento de las políticas y normas de seguridad.

El encargado del Departamento de Tecnologías de la Información y Comunicación y encargados de cada departamento, realizar una auditoría para el cumplimiento de los procedimientos en cuanto a las políticas de seguridad de la información, normas o estatutos que rigen dentro de la Universidad Técnica de Machala.

18.2.3 Comprobación del cumplimiento.

Se realizarán simulacros en los sistemas de información para verificar que se cumplan las políticas de seguridad, que se aplican dentro de la Universidad Técnica de Machala. Donde se tiene que cumplir la confiabilidad, disponibilidad de la información y la integridad de la misma.

Compromiso de la Universidad Técnica de Machala.

El cumplimento de la norma ISO establecida depende de la partición activa y compromiso que asuma la Institución respecto al cumplimiento de continuidad de su ejecución.

6.9 CONCLUSIONES Y RECOMENDACIONES.

6.9.1 CONCLUSIONES.

- El contenido de la norma ISO 27001 está orientado a la gestión de la seguridad de la información mediante la evaluación y tratamiento de riesgos, peligros y vulnerabilidades a la que está expuesta la información de las Instituciones de Educación Superior, ya que esta norma describe paso a paso la manera adecuada de gestionar la seguridad de los activos de información de la Universidad Técnica de Machala.

- Para garantizar la gestión de la seguridad de la información del Departamento de Tecnologías de la Información y Comunicación de la Universidad Técnica de Machala en cuanto a preservar la confiabilidad, disponibilidad e integridad se ha implementado un Sistema de Gestión de Seguridad de la Información, en donde se ha determinado que algunos activos se encuentran desprotegidos por ende se han definido políticas de seguridad y controles que aseguren la protección de la información.

- Al tener implementado un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001 en el Departamento de Tecnologías de la Información y Comunicación no significa contar con seguridad máxima en la información de la Universidad Técnica de Machala, sino que esto significa que la institución cumpla con requerimientos y mejores prácticas establecidas en la norma ISO/IEC 27001 para que la implementación del Sistema de Gestión de Seguridad de la Información funcione de forma exitosa.

6.9.2 RECOMENDACIONES.

- Se recomienda al Director de Tics junto con su personal extender el modelo de políticas de seguridad informática desde el departamento de Tecnologías de la Información y Comunicación a las demás dependencias de la Universidad Técnica de Machala, para que los encargados de los departamentos sistemas de las otras facultades se actualicen en cuanto a temas y normas de seguridad de la información.

- Se recomienda revisar continuamente o por lo menos cada seis meses el sistema de gestión de seguridad de la información por parte del Rectorado y del Director del Departamento de Tecnologías de la Información y Comunicación, ya que el Sistema de Gestión de Seguridad de la Información siempre debe estar mejorándose y actualizándose acorde a los cambios de tecnologías.

- Se recomienda que Rectorado y sus respectivas máximas autoridades capaciten al personal del Departamento de Tecnologías de la Información y Comunicación referente a la norma de seguridad de información ISO/IEC 27001 y no verlo como un gasto sino como una inversión, ya que son muchos los beneficios obtenidos gracias a la aplicación de esta norma en la gestión de la seguridad de la información en la Universidad Técnica de Machala.

BIBLIOGRAFÍA.

Aguirre Bautista, J. (15 de Mayo de 2018). *Auditoria Informática.* Obtenido de http://fcasua.contad.unam.mx: http://fcasua.contad.unam.mx/apuntes/interiores/docs/98/8/audi_infor.pdf

Albornoz, M., Barrere, R., Castro Martínez, E., & Fernández de Lucio, I. (2016). Programa iberoamericano. *Ciencia, tecnología e innovación para el desarrollo y la cohesión social*, 9-14.

Bustamante Maldonado, G., & Osorio Cano, J. A. (2014). Metodología de la seguridad de la información como medida. *Cuaderno Activa*, 74-75.

Bustamante Maldonado, G., & Osorio Cano, J. A. (2017). Metodología de la seguridad de la información como medida. *Cuaderno Activa*, 74-75.

Buxarrais Estrada, M. R., & Ovide, E. (2011). El impacto de las nuevas tecnologías en la educación en valores del siglo XXI. *Scielo*, 1-5.

Campos, P. G., & Burgos Salazar, J. (2017). Modelo Para Seguridad de la Información en TIC. *CEUR Workshop Proceedings*, 240-241.

Cárdenas, F., & Solares, P. (2016). SGSI en las sociedades de información crediticia. *Ciencias de los Sistemas de Información y Seguridad*, 68-69.

Casino, G. (2015). Seguridad en la industria. La era posindustrial trae nuevos riesgos la ciberseguridad, asignatura pendiente en muchas empresas. *Revista Ténica Industrial 311*, 28-30.

Cienciasfera. (15 de junio de 1012). *2. Seguridad de la información*. Obtenido de Actividad: http://www.cienciasfera.com/materiales/informatica/tecnologiainformacion/tema12/2_seguridad_de_la_informacin.html

Comunicación, V. d. (2018). Plan de la Sociedad de la Información el Conocimiento. *Ministerio de Telecomunicaciones y Sociedad de la Información*, 3-4.

Comunicaciones, P. (15 de Enero de 2018). *Sistemas Informáticos*. Obtenido de Las aplicaciones informáticas: https://www.gestion.org/las-aplicaciones-informaticas/

Conceptodefincion. (27 de Agosto de 2017). *Conceptos y Definiciones.* Obtenido de Definición de Dato: https://conceptodefinicion.de/datos/

Congreso , N. (20 de octubre de 2017). *LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS.* Obtenido de LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS: https://www.oas.org/juridico/spanish/cyb_ecu_ley_comelectronico.pdf

Cordova, M. C., Viñas, M., & Coria, M. K. (2017). Gestión del riesgo tecnológico y bibliotecas: una mirada transdisciplinar para su abordaje. *Gestión de la información: dilemas y perspectivas*, 4-6.

Cruz Micán, E. O., Perea Sandoval, J. A., & Ruiz López, J. (2018). Análisis de riesgos en la gestión de proyectos. *Aplicación de las TIC en los sectores económicos (Productivo, Comercial y Servicios) TOMO I*, 21-28.

Cybersecurity, T. (12 de agosto de 2018). *Sistema de Gestión de la Seguridad de la Información.* Obtenido de Implantación de SGSI: https://www.tecnek.com/servicios-de-ciberseguridad/implantacion-de-sgsi.html

Deloitte. (2017). *Seguridad de la Información en Ecuador 2017.* Quito: Deloitte.

Díaz, J. (29 de agosto de 2010). *Negocios y Emprendimiento.* Obtenido de Plantilla para aplicar el ciclo PHVA de la calidad: https://www.negociosyemprendimiento.org/2010/08/plantilla-para-aplicar-el-ciclo-phva-de.html

equipoteccelaya. (7 de febrero de 2018). *calidaddesoftwareteccelaya.* Obtenido de Norma, Estándar, Modelo: http://equipoteccelaya.blogspot.es/1234029360/norma-estandar-modelo/

Excellence, I. (16 de Febrero de 2016). *IsoTools Blog Calidad y Excelencia.* Obtenido de Descubre qué es un SGSI y cuáles son sus elementos esenciale: https://www.isotools.org/2016/02/16/descubre-que-es-un-sgsi-y-cuales-son-sus-elementos-esenciales/

Excellence, I. (Lues de Marzo de 2016). *Software ISO Riesgos y Seguridad.* Obtenido de Sistemas de Gestión de Riesgos y Seguridad: https://www.isotools.org/pdfs-pro/iso-27001-sistema-gestion-seguridad-informacion.pdf

Excellence, I. (28 de julio de 2017). *SGSI.* Obtenido de Blog especializado en Sistemas de Gestión: https://www.pmg-ssi.com/2015/07/que-es-sgsi/

Firma-e. (14 de noviembre de 2017). *El portal de ISO 27001 en Español.* Obtenido de ISO 27000.es: http://www.iso27000.es/sgsi.html

Garbayo Sánchez, J. A., & Sanz Ureta, J. (2013). La Seguridad, condidencialidad y disponibilidad de la información clínica. En J. C. Giménez de Azcárate, *Mecanismo de Seguridad* (págs. 258-259). Madrid: Microsoft Ibérica.

Garcés Suárez, E., Garcés Suárez, E., & Alcívar Fajardo, O. (2016). Las tecnologías de la información en el cambio de la educación superior en el siglo xxi: reflexiones para la práctica. *Universidad y Sociedad*, 171-177.

Gobierno del Estado, B. C. (16 de agosto de 2016). *Organización Internacional para la Estandarización (ISO).* Obtenido de ¿Qué es ISO?:: http://www.bajacalifornia.gob.mx/registrocivilbc/iso_informa2.htm

Heinekn. (15 de Agosto de 2016). *Infodir.* Obtenido de Revista de Información a Directivos: http://www.sld.cu/sitios/infodir/temas.php?idv=1346

Hermoso Ruiz, F. (2017). Sociedad de la Información y Educación. *Consejería de Educación, Ciencia y Tecnología, Dirección General de Ordenación, Renovación y Centros*, 13-29.

Hernández Figueroa, C. (20 de Julio de 2018). *Políticas de Seguridad.* Obtenido de http://www.spi1.nisu.org: http://www.spi1.nisu.org/recop/al01/javier/part4.html

Informática, S. (24 de abril de 2019). *Significados.com*. Obtenido de Significado de Seguridad informática: https://www.significados.com/seguridad-informatica/

iso27000. (10 de noviembre de 2017). *http://www.iso27000.es.* Obtenido de ISO 27001: http://www.iso27000.es/download/doc_iso27000_all.pdf

iso27000.es. (15 de Octubre de 2012). *ISO 27000.es*. Obtenido de El portal de ISO 27001 en Español: http://www.iso27000.es/sgsi.html

Isotools. (24 de mayo de 2018). *Blog Calidad y Excelencia.* Obtenido de 9 pasos para implementar la norma ISO 27001: https://www.isotools.org/2018/05/24/9-pasos-implementar-norma-iso-27001/

Javier Solarte, F. N., Enriquez Rosero, E. R., & Benavides Ruano, M. d. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica ESPOL – RTE,* 493-498.

Martinez Acuña, A. (26 de Mayo de 2018). *Control y Prevención de Riesgos.* Obtenido de https://psicologiayempresa.com: https://psicologiayempresa.com/control-y-prevencion-de-riesgos.html

Pearson. (15 de Abril de 2016). *El valor de la gestión de datos.* Obtenido de Una mala gestión y análisis de datos, "la mayor amenaza" para las ONG: https://blog.powerdata.es/el-valor-de-la-gestion-de-datos/bid/381763/Una-mala-gesti-n-y-an-lisis-de-datos-la-mayor-amenaza-para-las-ONG

Pérez Alonso, R., & Piedras Feria, E. (1012). *Una Agenda Digital: Telecomunicaciones y Tecnologías de la Información en México.* México: Consejo Editorial Camara de Diputados.

Piñeira Alonso, C. (14 de Abril de 2018). *Marco para la Buena Dirección.* Obtenido de http://www.gestionyliderazgoeducativo.cl: http://www.gestionyliderazgoeducativo.cl/gestioncalidad/buenadireccion/recursos.php

Ramírez Castro , A., & Ortíz Bayona , Z. (2017). Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. *Ingenieria, 16*(2), 11. Recuperado el mayo de 2011, de https://dialnet.unirioja.es/descarga/articulo/4797252.pdf

Rodriguez Velez, L. A. (15 de Abril de 2017). *Ecured*. Obtenido de Redes de Datos: https://www.ecured.cu/Redes_de_datos

Senescyt. (15 de abril de 2018). *Secretaria nacional de educación superior, ciencia, tecnologia e innovación*. Obtenido de ¿Qué es una Institución de Educación Superior (IES): http://servicios.senescyt.gob.ec/pregunta-frecuente/que-es-una-institucion-de-educacion-superior-ies/

Serrano Antón, J. C. (15 de Enero de 2017). *Food Defense Solutions.* Obtenido de ISO 27001 “Seguridad de la Información”: https://www.fooddefense-soluciones.com/es/iso-27001-seguridad-de-la-informacion

Sevillano, M. (7 de Mayo de 2016). *SGSIBlog especializado en Sistemas de Gestión.* Obtenido de ¿Por qué implantar un SGSI basado en la norma ISO 27001?: https://www.pmg-ssi.com/2015/05/por-que-implantar-un-sgsi-basado-en-la-norma-iso-27001/

Silva, R., Cruz, E., Méndez, I., & Hernández, J. Á. (2016). Sistema de Gestión Digital para mejorar los procesos administrativos de instituciones de educación superior. *Perspectiva Educacional*, 105-108.

Solarte Solarte, F. N., Enriquez Rosero, E. R., & Benavides Ruano, M. d. (2016). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica ESPOL – RTE, Vol. 28, N. 5, 492-507*, 494-499.

Soluciones para tu empresa. (19 de julio de 2013). Obtenido de SGSI.- Sistema de Gestión de Seguridad de la Información: http://www.madaryconsulting.es/sgsi-sistema-de-gesti-n-de-seguridad-de-la-informaci-n

Sullivan, B. (2016). *Tendencias de seguridad cibernética en américa latina y el caribe.* Washington: Symantec. Obtenido de https://www.symantec.com/content/es/mx/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf

Thompson, I. (12 de Agosto de 2018). *Qué es la Información*. Obtenido de https://www.promonegocios.net: https://www.promonegocios.net/mercadotecnia/que-es-informacion.html

Unam. (20 de febrero de 2018). *Las Tics para aprender*. Obtenido de ¿Qué son las TIC?: http://tutorial.cch.unam.mx/bloque4/lasTIC

Utmach. (2016). *Politica General de Seguridad de la Información de la Universidad Técnica de Machala.* Machala: UTMACH.

Van Der Horst, J. (25 de diciembre de 2017). *Departamento Aeroportuario*. Obtenido de DEPARTAMENTO DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN TIC: http://da.gob.do/?page_id=967

Vera-Cruz, C. (20 de noviembre de 2016). *Gestión de la Seguridad*. Obtenido de Claves para resguardar la seguridad de la información en las empresas: https://searchdatacenter.techtarget.com/es/cronica/Claves-para-resguardar-la-seguridad-de-la-informacion-en-las-empresas

ANEXO 1: MODELO DE ENCUESTA

UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

MAESTRÍA EN GERENCIA DE SISTEMAS DE INFORMACIÓN

Objetivo: Recolectar información para determinar las condiciones de la gestión de la seguridad de la información de los departamentos de Tecnologías de Información y Comunicación de las Instituciones de Educación Superior de la Ciudad de Machala.

Instrucciones: Marque con una X la opción que considere más adecuada.

Cuestionario

No.	Preguntas	SI	NO
1	¿Existen políticas, controles o normas que garanticen la gestión de la seguridad de la información en las Instituciones de Educación Superior?		
2	¿Se aplican políticas de gestión de seguridad de la información en el procesamiento de información de las Instituciones de Educación Superior?		
3	¿El personal tienen conocimiento sobre los Sistema de Gestión de seguridad de la información (SGSI)?		
4	¿Considera necesario que se implemente una normativa de Gestión de Seguridad de la información?		
5	¿Existe alguna política, controles o restricciones de seguridad para evitar el acceso a sitios no autorizados, uso de navegadores y correo electrónico en internet?		
6	¿Firmó usted un certificado de confidencialidad y buen uso de las claves de acceso a diferentes sistemas de gestión de procesos de la información?		
7	¿La información que usted gestiona para el desempeño de sus actividades se respalda frecuentemente?		

8	¿Se aplican en la institución mantenimientos preventivos periódicos a los equipos de cómputo establecidos para la ejecución de sus actividades?		
9	¿Ha constatado que el personal al no utilizar un SGSI que ayuda a la gestión de seguridad de la información ha originado una mala toma de decisiones?		
10	¿Considera necesario contar un SGSI para la gestión de la seguridad de la información en las Instituciones de Educación Superior?		

ANEXO 2: ESQUEMA DE LA NORMA ISO 27001 – CLÁUSULAS (ANEXO SL)

Cláusula 4: Contexto de la organización

La cláusula 4 consta de cuatro sub-cláusulas::

4.1 Conocimiento de la organización y de su contexto

4.2 Comprensión de las necesidades y expectativas de las partes interesadas

4.3 Determinación del alcance del sistema de gestión de la calidad

4.4 Sistema de gestión

Como punto de partida y referencia del sistema de gestión, la cláusula 4 determina por qué la organización está donde está. Como parte de la respuesta a esta pregunta, la organización debe identificar las cuestiones internas y externas que pueden influir en los resultados esperados, así como a todas las partes interesadas y sus necesidades. También debe documentar su alcance y establecer los límites del sistema de gestión - todo en línea con los objetivos de negocio.

Cláusula 5: Liderazgo

La cláusula 5 consta de tres sub-cláusulas:

5.1 Liderazgo y compromiso

5.2 Política

5.3 Roles, responsabilidades y autoridades en la organización

La nueva estructura hace especial hincapié en el liderazgo, no sólo a la dirección que figuraba en las normas anteriores. Esto quiere decir que la alta dirección tiene ahora una mayor responsabilidad y participación en el sistema de gestión de la organización. Deben integrar los requisitos del sistema de gestión en los procesos de negocio de la organización, asegurar que el sistema de gestión logra los resultados previstos y asignar los recursos necesarios. La alta dirección es también responsable de comunicar la importancia del sistema de gestión y aumentar la toma de conciencia y la participación de los empleados.

Cláusula 6: Planificación

La cláusula 6 consta de dos sub-cláusulas:

6.1 Acciones para tratar riesgos y oportunidades

6.2 Objetivos del sistema de gestión y planificación para lograrlos

La cláusula 6 nos proporciona la manera directa de tratar el riesgo. Una vez que la organización ha definido los riesgos y oportunidades en la cláusula 4, tiene que establecer cómo van a ser tratados a través de la planificación. Este enfoque proactivo sustituye a la acción preventiva y reduce la necesidad de acciones correctivas posteriormente. Se pone especial atención también en los objetivos del sistema de gestión. Deben ser medibles, ser objeto de seguimiento, comunicados, coherentes con la política del sistema de gestión y actualizados cuando sea necesario.

Cláusula 7: Soporte

La cláusula 7 consta de cinco sub-cláusulas:

7.1 Recursos

7.2 Competencia

7.3 Toma de conciencia

7.4 Comunicación

7.5 Información documentada

Después de abordar el contexto, el compromiso y la planificación, las organizaciones tendrán que analizar el soporte necesario para cumplir con sus metas y objetivos. Esto incluye los recursos, comunicaciones internas y externas, así como la información documentada que reemplaza los términos utilizados anteriormente como documentos, documentación y registros.

Cláusula 8: Operación

La cláusula 8 consta de una sub-cláusula:

8.1 Planificación y control operacional

La mayor parte de los requisitos del sistema de gestión se encuentran dentro de esta cláusula. La cláusula 8 aborda tanto los procesos internos como los contratados externamente, mientras que la gestión del proceso global incluye criterios adecuados para el control de estos procesos así como formas de gestionar el cambio planificado y el no previsto.

Cláusula 9: Evaluación del desempeño

La cláusula 9 consta de tres sub-cláusulas:

9.1 Seguimiento, medición, análisis y evaluación

9.2 Auditoría interna

9.3 Revisión por la dirección

Para dar cumplimiento a éste requisito, las organizaciones deben determinar qué, cómo y cuándo ha de ser supervisado, medido, analizado y evaluado. La auditoría interna también es parte de este proceso para asegurar que el sistema de gestión se ajusta a los requisitos de la organización, así como a los de la norma, y se ha implantado y mantenido con éxito. El último paso, la revisión por la dirección, que analiza si el sistema de gestión es apropiado, adecuado y eficaz.

Cláusula 10: Mejora

Con dos sub-cláusulas, la cláusula 10 analiza cómo se deben tratar las no conformidades y acciones correctivas:

10.1 No conformidad y acción correctiva

10.2 Mejoracontinua

En un mundo empresarial en constante cambio, no todo siempre se lleva a cabo según lo planificado. La cláusula 10 analiza las formas de hacer frente a las no conformidades y acciones correctivas, así como las estrategias de mejora continua.

ANEXO 3. CONTROLES ISO/IEC 27002:2013 (ANEXO A)

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.

ISO27002.es PATROCINADO POR:

GES CONSULTOR
GOBIERNO T.I. - RIESGO - CUMPLIMIENTO

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.

Iso27000.es: Documento sólo para uso didáctico. La norma oficial debe adquirirse en las entidades autorizadas para su venta.

Octubre-2013

ANEXO 4: ACUERDO DE CONFIDENCIALIDAD

Machala, a _____ de _____ 201__

Yo,_____, portador de la C.C:_____, funcionario de la Universidad Técnica de Machala, desempeñando a la fecha el cargo de _____ en el Área de _____ bajo la modalidad de nombramiento/contrato _____ suscribo el presente Acuerdo de Confidencialidad de la Información, asumiendo que:

1. Comprendo que la información no publica asociada con el personal y la institución tienen el carácter de confidencial, por tanto, me comprometo a estar sujeto y utilizarla solo para los fines que mis responsabilidades como funcionario de la Universidad Técnica de Machala lo requiera.

2. Ser consciente de la responsabilidad de no poner en riesgo la confidencialidad, integridad y disponibilidad de la información que gestiona la Universidad Técnica de Machala. A su vez me comprometo a cumplir los procedimientos de gestión de seguridad de la información que concierne a mis funciones descritas en el documento de las POLITICAS DE SEGURIDAD DE LA INFORMACIÓN (SGSI).

3. Cumplir con las disposiciones relacionadas a las POLITICAS DE SEGURIDAD DE LA INFORMACIÓN(SGSI) en lo que se refiere a su utilización y difusión.

4. Comprende que no cumplir con las disposiciones del presente acuerdo podría implicar penalizaciones por parte de la Universidad Técnica de Machala y las leyes vigentes.

Firma del Funcionario	Firma del Responsable de la Seguridad de la Información
_____	_____
NOMBRES Y APELLIDOS CEDULA DE CIUDADANÍA	NOMBRES Y APELLIDOS CEDULA DE CIUDADANÍA

ANEXO 5: FORMULARIO DE LISTADO DE SERVIDORES Y CONTRASEÑAS.

Listado de Servidores y Contraseñas			
Datos Generales			
Departamento**:**			
Datos del Usuario			
Apellido y Nombre del Solicitante:			
Cargo:		Telf.:	
Correo Electrónico:			
Listado de servidores			
HOSTNAME	**DIRECCION IP**	**USUARIO**	**CONTRASEÑA**
Firmantes			
Cargo: **Fecha:** **Solicitante:**		**Cargo:** **Fecha:** **Autoriza:**	
OBSERVACIÓNES:			

ANEXO 6: FORMULARIO DE INVENTARIO DE HARDWARE Y SOFTWARE DE COMPUTADORAS

Nombre del Computador	
Dirección IP	
Mascara de Subred	
Nombre de Dominio	
Localización física del Computador	
Modelo del Micrprocesador	
Marca de Computador	
Modelo de Computador	
Número de procesadores	
Velocidad Procesador	
Sistema Operativo	
Versión de Sistema Operativo	
Memoria RAM	
Capacidad de Almacenamiento	

Lineamientos de uso de los equipos:

- No ingresar con alimentos ni bebidas.
- No fumar.
- Tener el equipo conectado a un UPS para evitar variaciones de voltaje.
- No realizar cambios sobre el software.
- No realizar cambios o mantenimiento sobre el hardware.
- Conservar los equipos en óptimas condiciones.

ANEXO 7: FORMULARIO DE CREACIÓN DE USUARIOS

Y RESPONSABILIDADES DE CONTRASEÑAS

SOLITUD DE ACCESO A SISTEMAS DE INFORMACIÓN	
Datos Generales	
Departamento**:**	
Datos del Usuario	
Apellido y Nombre del Solicitante:	
Cargo: Telf.:	
Correo Electrónico:	
Perfil de usuario a crear	
Sistema de Información:	
Usuario:	
Contraseña:	
Obligaciones del Usuario	
La clave o contraseña es de uso personal y no puede ser otorgada a otro funcionario por ningún motivo. Para realizar cambios de perfiles de usuario se debe comunicar con el Departamento de Tecnologías de la Información y Comunicación de la Universidad Técnica de Machala. En caso de que el funcionario sea suspendido temporal o definitivamente de su cargo, se deberá informar de manera inmediata al administrador de usuarios. El funcionario debe cerrar su sesión de usuario cuando no esté en uso.	
Firmantes	
_____ **Cargo:** **Fecha:** **Solicitante:**	_____ **Cargo:** **Fecha:** **Autoriza:**
Observaciónes:	

ANEXO 8: FORMATO PARA EL REGISTRO DE BACKUPS.

Código:					
Versión:					
Fecha de Actualización:					
Elaborado por:					
Sistema de información	Tipo de Backups	Tiempo del Backups	Medio de Almacenamiento	Lugar de Almacenamiento	Persona que lo genera

ANEXO 9: FORMULARIO PARA EL TRATAMIENTO Y VALORACIÓN DE INCIDENTES

TRATAMIENTO Y VALORACIÓN DE INCIDENTES	
Datos Generales	
Departamento**:**	
Quien lo reporta:	
Nª de incidente:	
Prioridad:	
Usuarios Afectados:	
Datos del Incidente	
Descripción**:**	
Posible Causa:	
Fecha y Hora Aproximada Iniciado el incidente:	
Fecha y hora de detección:	
Fecha y hora de restauración:	
Sistemas Afectados:	
Registros/Datos Afectados:	
Protocolos Atacados (HTTP, POP, etc.):	
Objetivo del Sistema Afectado:	
Costos asociados:	
Actividades de Restauración:	
Resolución:	
Firmantes	
_____ **Cargo:** **Fecha:** **Solicitante:**	_____ **Cargo:** **Fecha:** **Autoriza:**
OBSERVACIÓNES:	

ANEXO 10: OFICIO DE ENTREGA DE POLITICAS(SGSI)

Machala, 10 de mayo de 2019

Ing. Cesar Quezada Abad,
RECTOR UNIVERSIDAD TÉCNICA DE MACHALA.
Ciudad. -

Motivo: Entrega de Políticas de Seguridad (SGSI).

Por medio del presente documento se expresa la necesidad de disponer de un modelo de seguridad de información para proteger los procesos, activos y demás elementos implicados en el tratamiento de la información en el departamento de Tecnologías de la Información y Comunicación de la Universidad Técnica de Machala.

Para cubrir la necesidad antes mencionada, se hace formal la entrega e implementación de un Plan de Políticas (SGSI) para la Universidad Técnica de Machala para garantizar la Gestión de la Seguridad de la Información, además de la calidad de la gerencia informática, servicios y procesos que se ejecutan en el departamento de Tics de la Universidad Técnica de Machala.

Atentamente,

_____
Ing. Wilson Cuenca L.
INVESTIGADOR

C.C.P. Jairo Jiménez, Jefe de Sistemas.
DPTO DE TICS-UTMACH.

ANEXO 11: LISTA DE DOCUMENTOS ISO 27001 OBLIGATORIOS

UNIVERSIDAD TÉCNICA DE MACHALA

FACULTAD DE _____

REQUERIMIENTO DE SOFTWARE

No. Documentos

DATOS GENERALES

Docente Solicitante: Período: Fecha:

N	Carrera	Nivel	Módulo	Software Requerido	Versión	Observación
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						

Coordinador Docente

Formato requerimiento de software para uso de Docentes

UNIVERSIDAD TÉCNICA DE MACHALA

FACULTAD DE _____

ACTA DE CONFORMIDAD DE INSTALACIÓN DE SOFTWARE

No. Documentos

GENERALIDADES

En la ciuda de Machala, a los ____ días del mes de _____ del 201___ siendo las _____ en presencia del _____ _____, Coordinador de la Carrera de_____, se procede a verificar por parte del mismo que se halla instalado y funcionando el siguiente aoftware de acuerdo a las características solicitadas.

N	No. Documento Solicitante	Docente Saliente	Software Instalado	Versión	Lab. No.	Fecha de Instalación	Observación
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							

_____ Coordinador

_____ Administrador de Redes

Acta de revisión de la Instalación del software requerido por Docente.

U N I V E R S I D A D T É C N I C A D E M A C H A L A

DEPARTAMENTO DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIÓN

M A P A D E R I E S G O S

Resposable	
Lugar y Fecha:	
Objetivo del Formulario:	

Numero de Factor de Riesgo	Código de Riesgo	REDACCIÓN DEL RIESGO	VALORACIÓN DEL RIESGO			RESPUESTA AL RIESGO	MEDIDAS DE MITIGACIÓN	CONTROLES
			Probabilidad	Impacto	Priorización			

Mapa De Riesgos

U N I V E R S I D A D T É C N I C A D E M A C H A L A

DEPARTAMENTO DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIÓN

MATRIZ DE RIESGOS ESTRATEGICOS

Identificación de Riesgos, Medidas de Migitación y Controles

Responsable	
Lugar y fecha:	
Objetivo del control	

Tipos de Riesgos		**Identificación**			**Priorización del Riesgo**					**Medidas de mitigación**	**Responsable de la medida de mitigación**	**Descripción del control**	**Responsable de la ejecución del control**	**Observación**
		Factores	**Amenaza/ Vulnerabilidad**	**Impacto (Efecto)**	**Redacción del Riesgo**	**Probabilidad**	**Impacto**	**Valoración**	**Respuesta al riesgo**					
1	Proyectos													
2	Tecnológicos													
3	Seguridad de la Información													
4	Procesos													

Matriz de Riesgos Estratégicos

GESTIÓN DE RIESGO INSTITUCIONAL
MATRIZ DE RIESGO OPERACIONAL
MAPA DE RIESGOS

Responsable (Identificación del riesgo)	
Responsable (Implementar MMC)	
unidad Administrativa	
Lugar y fecha:	
Objetivo del Formularios	

Número de actividad	Código del riesgo	REDACCIÓN DEL RIESGO	VALORACIÓN DEL RIESGO			Tratamiento al riesgo	Descripción General del Control	Tipo de Control
			Probabilidad	Impacto	Priorización			

Matriz de Riesgo Operacional

UNIVERSIDAD TECNICA DE MACHALA
DEPARTAMENTO DE TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN

GESTIÓN DE RIEGOS
PLAN DE ACCIÓN MEDIDAS DE MITIGACIÓN Y CONTROLES

Responsable (Identificación de riesgos)	
Responsable (Implementación MMC)	
Unidad Administrativa (Ejecutora de Implementación)	
Lugar y Fecha	

RIESGO IDENTIFICADO	VALORACIÓN DEL RIESGO

MEDIDA DE MITIGACIÓN	CONTROLES

PLAN DE ACCIÓN					
ACTIVIDADES	M/C	FECHA INICIO	FECHA FINAL	RESPONSABLE	ENTREGABLE

Plan de Acción de Medidas de Mitigación y Controles

Universidad Técnica de Machala
Departamento de Tecnologias de la Información y Comunicación

Plan de Continuidad Institucional
Registro de Acciones ante una Interrupción

Responsable	
Responsable	
Unidad Administrativa	
Lugar y Fecha:	

RIESGO IDENTIFICADO	VALORES DEL RIESGO

MEDIDAS DE MITIGACIÓN	CONTROLES

PLAN DE ACCION ANTE UNA INTERRUPCIÓN

Funciones Afectadas	Sistemas Informáticos de apoyo	TMI(Tiempo máximo de recuperación	TR(Tiempo de Recuperación)	TMIR(Tiempo máximo de interrupción real	Criticidad

Registro de Acciones Ante una Interrupción