FACULTAD DE ARQUITECTURA E INGENIERÍAS

Trabajo de fin de carrera titulado

DISEÑO DE UNA POLÍTICA DE SEGURIDAD PARA LA INFRAESTRUCTURA DE RED DE LA UNIVERSIDAD CENTRAL DEL ECUADOR BASADA EN LA ISO / IEC 27002:2013

Realizado por:

Ing. Alfonso Fabián Portilla Hernández

Director del proyecto:

Msc. Christian David Pazmiño Flores

Como requisito para la obtención del título de:

MÁSTER EN CIBERSEGURIDAD

Quito, agosto de 2020

DECLARACIÓN JURAMENTADA

Yo, Alfonso Fabián Portilla Hernández, ecuatoriano, con Cédula de ciudadanía N° 1002034435, declaro bajo juramento que el trabajo aquí desarrollado es de mi autoría, que no ha sido presentado anteriormente para ningún grado o calificación profesional, y se basa en las referencias bibliográficas descritas en este documento.

A través de esta declaración, cedo los derechos de propiedad intelectual a la Universidad Internacional SEK, según lo establecido en la Ley de Propiedad Intelectual, reglamento y normativa institucional vigente.

_____

ALFONSO FABIÁN PORTILLA HERNÁNDEZ

CC: 1002034435

DECLARACIÓN DEL DIRECTOR DE TESIS

Declaro que el presente trabajo de investigación titulado:

DISEÑO DE UNA POLÍTICA DE SEGURIDAD PARA LA INFRAESTRUCTURA DE RED DE LA UNIVERSIDAD CENTRAL DEL ECUADOR BASADA EN LA ISO / IEC 27002:2013

Realizado por:

ALFONSO FABIÁN PORTILLA HERNÁNDEZ

Como requisito para la obtención del título:

MASTER EN CIBERSEGURIDAD

Ha sido dirigido por el ingeniero:

Msc. Christian David Pazmiño Flores

Quien considera que constituye un trabajo original de su autor.

_____

Msc. Christian David Pazmiño Flores

DIRECTOR DEL PROYECTO

CC: 1719252049

LOS PROFESORES INFORMANTES:

VERÓNICA RODRÍGUEZ ARBOLEDA

LUIS FABIÁN HURTADO VARGAS

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

Ing. Verónica Rodríguez, MBA	**Ing. Fabián Hurtado, Msc.**

Quito, agosto de 2020

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su desarrollo se respetaron las disposiciones legales que protegen los derechos de autor vigentes.

_____

ALFONSO FABIÁN PORTILLA HERNÁNDEZ

CC: 1002034435

AGRADECIMIENTOS

A la Universidad Internacional SEK, a sus autoridades, personal docente y administrativo que forman parte de la primera Maestría en Ciberseguridad, por su dedicación y compromiso en la formación académica.

Al Msc. Christian David Pazmiño Flores, por su valioso aporte y predisposición para el desarrollo del presente proyecto.

Ing. Verónica Rodríguez., MBA, por su dedicación y tiempo en la revisión de este proyecto.

A la Universidad Central del Ecuador, a la cual pertenezco, por permitirme desarrollar este trabajo de investigación y poder agregar valor a la institución. A su Director de Tecnologías de la Información y Comunicación el Ing. César Morales e Ing. Paúl Tutillo por su apoyo y aporte.

DEDICATORIA

A las personas más importantes en mi vida:

Mis queridas hijas Alicia Fabiana y Alejandra Valentina, quienes serán siempre la inspiración y motivación para mi superación profesional y personal.

A mi esposa Lucia por su confianza y apoyo incondicional, por el impulso en la consecución de este y nuevos objetivos.

A mis padres Jaime Rene y Ruth Alicia (+) por su ejemplo y por haberme inculcado siempre ser perseverante, a mi madre que, a pesar de no estar entre nosotros, este logro también es suyo.

A mis hermanos Jaime Eduardo y Pablo Mauricio, mis amigos de toda la vida.

RESUMEN

El presente proyecto tiene como finalidad el Diseño de una Política de Seguridad para la infraestructura de red de la Universidad Central del Ecuador basada en la Norma ISO/IEC/27002:2013 que actualice la política existente con el propósito de reducir los riesgos de seguridad encontrados para salvaguardar la integridad, confidencialidad y disponibilidad de la información, académica, de investigación, y financiera.

Para la gestión de riesgos se utilizó la metodología Magerit para evaluar todos los activos de la infraestructura tecnológica institucional. Mediante la matriz de riesgos igualmente se valoró las amenazas y el impacto que determinó el riesgo a que se encuentra expuesta la información.

Luego del análisis realizado se procedió a seleccionar las salvaguardas y controles de la norma ISO/IEC/27002:2013 con los que se desarrolló la presente política, se recomienda sea aprobada y socializada dentro de todos los estamentos universitarios.

Palabras clave: Universidad Central de Ecuador, Seguridad de la información, Magerit, Norma ISO/IEC/27002:2013

ABSTRACT

The goal of this project is to design a Security Policy for the network infrastructure of the Universidad Central del Ecuador based on ISO / IEC / 27002: 2013 that updates the existing policy in order to reduce the found security risks and thereby safeguarding the integrity, confidentiality, and availability of academic, financial, and research information.

For the purpose of risk management, the Magerit methodology was used, where all the assets of the technological infrastructure of the institution are evaluated. The risk matrix evaluates threats and the impact, which determine the risk as to which the information is exposed.

After the analysis is carried out, the types of protection and controls of the ISO / IEC / 27002: 2013 standard were selected. The present policy was developed according to this process, it is recommended to be approved, explained, and distributed within all the levels of the institution.

Keywords: Universidad Central del Ecuador, Information Security, Magerit, ISO / IEC / 27002: 2013 Standard

Tabla de contenido

Índice de tablas

Índice de figuras

CAPÍTULO I

INTRODUCCIÓN

1.1. El problema de investigación

1.1.1. Planteamiento del problema

La Universidad Central del Ecuador es una institución pública integrada por tres estamentos, docentes, estudiantes, personal administrativo y de servicios, con personalidad jurídica, autonomía, de derecho público, sin fines de lucro, domiciliada en la ciudad de Quito, capital de la República del Ecuador.

En el Estatuto Universitario aprobado en octubre 2019, en el capítulo 3 página 8, en las bases estratégicas de la Universidad Central del Ecuador se mencionan:

> **Artículo 7**.- **Misión**: Promover acceso a la cultura universal y generar conocimiento a través de la investigación de excelencia para contribuir al desarrollo humano y al buen vivir del Ecuador, esta misión la cumple a través de la formación de grado y posgrado, de la práctica de la investigación social y experimental y de la vinculación con la sociedad, mediante una proyección de la universidad en el contexto internacional. (Estatuto Universitario, 2019, pág. 8).

> **Artículo 8.- Visión:** La Universidad Central del Ecuador será la mejor Universidad pública del país y de la región, con carreras y programas pertinentes en todas las áreas del conocimiento, con sólidas bases de internacionalización, con una significativa incidencia en el desarrollo humano y del buen vivir, a través de sus

programas de formación profesional, investigación y vinculación social. (Estatuto Universitario, 2019, pág. 8).

Artículo 9.- Objetivos: Son objetivos de la Universidad Central del Ecuador:

a. Formar profesionales integrales en grado y posgrado con un carácter de excelencia, con carreras y programas pertinentes en todas las áreas del conocimiento;
b. Generar investigación como un proceso que brinda respuestas a las necesidades del país y de la región y con una fuerte articulación con la docencia, con una sólida producción científica e innovación, para mejorar el conocimiento y aportar al desarrollo humano;
c. Alcanzar significativa incidencia en el desarrollo humano y en el buen vivir, a través de sus programas de vinculación con la sociedad, a su vez articulados a la docencia y a la investigación;
d. Lograr una universidad con sólidas bases de internacionalización expresadas en Vínculos institucionales y presencia internacional;
e. Implementar una gestión institucional por procesos para la mejora continua en lo académico, investigativo, vinculación, administrativo-financiero, tecnológico y comunicacional. (Estatuto Universitario, 2019, pág. 8).

La Universidad Central del Ecuador es una de las instituciones de educación superior con mayor prestigio, más antiguas y reconocidas del país, cuenta con alrededor de 40000 estudiantes, una planta docente de 2500 profesores y con personal administrativo y de servicios 1300 aproximadamente (Transparencia UCE, 2019).

Debido a la cantidad de alumnos, personal administrativo y docente que laboran en la UCE, no se puede llevar un control adecuado del tráfico de red, por lo que se ha hecho

imprescindible la evaluación y actualización de la política de seguridad existente y que se encuentre definida bajo estándares internacionales.

La mayoría de equipos tecnológicos que se conectan a la red de la Universidad navegan en internet por lo que se encuentran expuestos a constantes amenazas y riesgos que podrían ser descubiertas oportunamente evitando problemas en la infraestructura de red.

De acuerdo a la indagación realizada en la Dirección de Tecnologías de la Información de la Universidad Central (DTIC) en donde se concentra toda la información académica, investigación, financiera, convirtiéndose en un punto neurálgico sensible y confidencial que, por falta de controles, procedimientos actualizados lo que conlleva a dejar vulnerabilidades ante amenazas como la pérdida de información. En la figura 1, se muestra cómo se encuentra la infraestructura de red de la UCE:

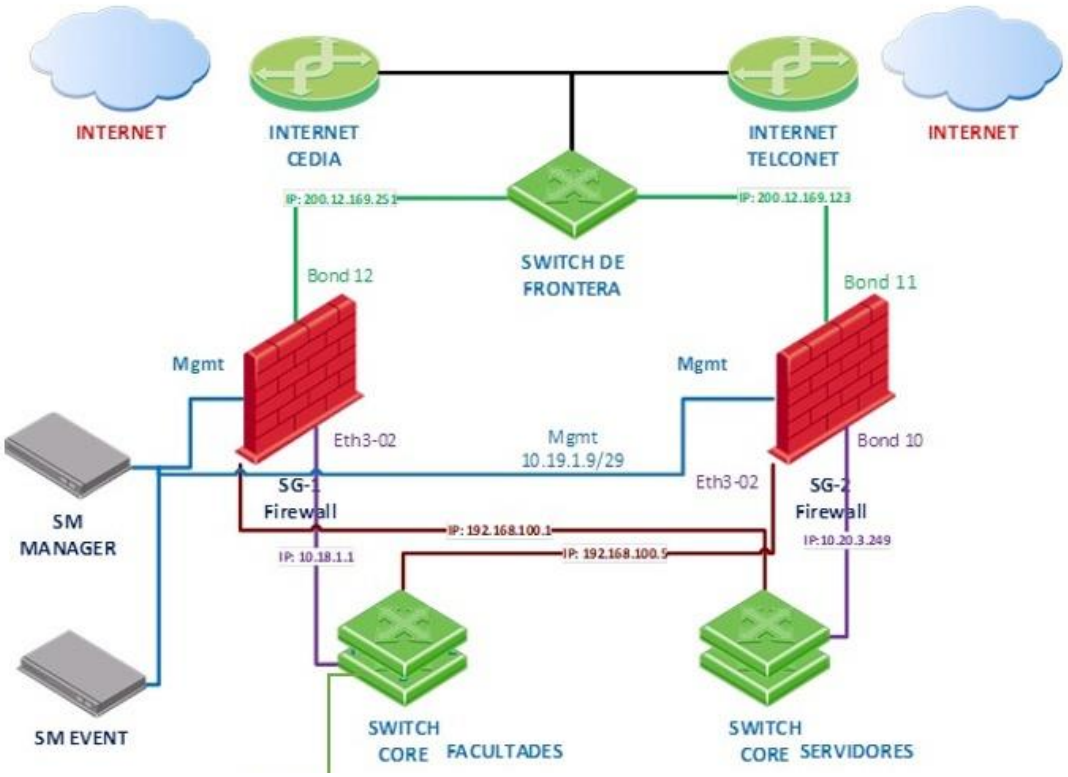


Figura 1 *Diagrama de la infraestructura de red 2017*

Fuente: Memoria Técnica DTIC-UCE Diagrama de Red de la UCE 2017

Al no disponer de una política de seguridad actualizada para la infraestructura de red en la Universidad Central del Ecuador los cambios en las configuraciones de equipos de administración de red son realizados de acuerdo al criterio del administrador. La implementación de controles, medidas y procedimientos de seguridad se las realiza de forma empírica, lo que ocasiona que estén expuestos a riesgos como la pérdida o adulteración de información, filtración de contenido, lo que hace que se afecte significativamente la operatividad de la plataforma tecnológica y se genere la desactualización periódica del equipamiento de red y hardware conectado a la intranet universitaria.

1.1.2. Formulación del problema

En la actualidad existe una gran cantidad de conexiones concurrentes que salen a internet e ingresan hacia la red interna, dando como resultado una creciente probabilidad de amenazas o riesgos de seguridad. Debido a que no se aplica de forma estricta los controles existentes, se provoca un cuello de botella en el tráfico de información, con las consecuentes molestias y retardos en los procesos académicos y administrativos de la universidad, para disminuir estos eventos de seguridad es necesario actualizar la política de seguridad con nuevos controles.

1.2.OBJETIVOS

1.2.1. Objetivo general

Diseñar una política de seguridad para la infraestructura de red de la Universidad Central del Ecuador basada en la ISO / IEC 27002:2013, mediante la aplicación de controles de seguridad que salvaguarden los activos tecnológicos de acuerdo a las necesidades institucionales.

1.2.2. Objetivos específicos

- Analizar la política existente elaborada para la Universidad Central en el año 2015, bajo los estándares ISO/IEC 27000 y COBIT 5 identificando nuevas vulnerabilidades y amenazas de seguridad minimizando el riesgo.
- Valorar la situación actual de la infraestructura de red de la UCE mediante una matriz de riesgos, que permita la identificación de vulnerabilidades y amenazas de seguridad.
- Seleccionar los controles de la norma ISO / IEC 27002:2013 que minimicen las amenazas identificadas y sean la base para el diseño de la nueva política de seguridad.
- Desarrollar la política de seguridad para la infraestructura de red de la UCE, mediante los controles seleccionados de la norma ISO / IEC 27002:2013, que permitan la reducción del impacto y la probabilidad de ocurrencia de los riesgos de seguridad de la información.

1.3. JUSTIFICACIÓN

Una vez que, se analizó la política de seguridad existente elaborada bajo las normas ISO 27000 y Cobit 5, se diseñó una nueva política de seguridad para actualizarla en base a la Norma ISO 27002:2013 que permite establecer los controles necesarios y buenas prácticas para el aseguramiento de la información a nivel de infraestructura de red, así como, en todos los procesos académicos. En esta política de seguridad se define claramente qué está permitido realizar y qué no, con el objetivo de tratar los incidentes de seguridad.

Se valoró los distintos riesgos de seguridad en los activos tecnológicos con los que cuenta la Universidad Central del Ecuador, encontrando vulnerabilidades que comprometen la seguridad de la información como por ejemplo: falta de controles contra software malicioso, desactualización de los programas, insuficientes instalaciones de redundancia en la red, fallas en la manipulación de accesos y actualización de perfiles de usuario, entre otras. Con estos antecedentes, fue importante para la Institución la actualización de la política de seguridad existente para ayudar a mitigar estas amenazas.

Para identificar la probabilidad de ocurrencia de amenazas y vulnerabilidades se escogió MAGERIT, está es una metodología internacional reconocida por ENISA (*European Network and Information Security Agency*) que permite realizar análisis de riegos asociados a los activos de la infraestructura tecnológica de una institución.

Esta metodología nos permitió realizar análisis cualitativos y cuantitativos además de catalogar a los recursos de la información como activos, estas ventajas hacen que sea una metodología completa tanto para el análisis como para la gestión de riesgos en relación a otras metodologías como OCTAVE, MEHARI, ISO/IEC 27005, FRAAP, entre otras.

ESTADO DEL ARTE

Ecuador ha sufrido múltiples ciberataques a la infraestructura tecnológica tanto a instituciones públicas como privadas, constantemente surgen amenazas sofisticadas por lo que es muy importante tomar las medidas necesarias para cambiar la tecnología convencional de seguridad. Entre los ciberataques más relevantes se encuentran los suscitados en abril 2019, se registraron más de 40 millones desde países como Estados Unidos, Brasil, Holanda, Rumania, entre otros. Estos ciberataques fueron dirigidos a

portales públicos impidiéndoles el acceso. “Las principales instituciones afectadas fueron La Cancillería, El Banco Central, La Presidencia, El Servicio de Rentas Internas (SRI), algunos ministerios y universidades”. (El Comercio, 2019)

Escasas son las investigaciones realizadas para el diseño de políticas de seguridad para infraestructura de red de instituciones educativas, sin embargo, se menciona algunas relevantes relacionadas con esta investigación, en las que se utilizan la norma ISO/IEC: 27002:2013.

Según Cevallos (2019), quien diseña “La política de seguridad de la información para el departamento de TICS del Instituto Tecnológico Superior Central Técnico (ITSCT) basado en la norma ISO/IEC 27002:2013”, menciona que es muy importante salvaguardar la información más relevante de las instituciones educativas como la académica, las plataformas virtuales, mediante una adecuada gestión de riegos.

Según Cárdenas (2020), en su trabajo de investigación “Diseño de una política de seguridad de la información para la Unidad Educativa Borja 3 Cavanis”,se basa en la metodología Magerit para el análisis de riesgos de los activos, la detección de vulnerabilidades y amenazas existentes en la institución, establece los lineamientos de seguridad para que el Departamento de Gestión Tecnológica de la institución pueda mitigarlos.

Respecto a políticas de seguridad para la infraestructura de red Palma (2019), en su investigación para el hospital AXXIS basada en la norma ISO/IEC: 2013 plantea la necesidad de implementar controles de acceso en la administración de la infraestructura de red, así como para la información almacenada en la misma, para evitar la pérdida de activos y la continuidad del negocio.

En Colombia, León (2017) menciona que la implementación de controles de la norma ISO/ICE 2700:2013 más las buenas prácticas de seguridad en la fase de auditoria hizo que obtuviese un alto nivel de madurez, lo que concibió que la Universidad gestione la seguridad de una forma más segura y el mejoró manejo adecuado del riego.

Luego de realizar los estudios de la situación actual de las instituciones con relación a los incidentes de seguridad se puede indicar que el objetivo es proteger los activos de su infraestructura tecnológica, esto se logra mediante la implementación de una apropiada normativa, para tal efecto se plantea la aplicación de la norma ISO/IEC 27002:2013, que contiene las directrices y buenas prácticas para la gestión de la seguridad de la información; lo que lleva a pensar que la aplicación de esta norma sería de gran utilidad para la seguridad de la Universidad Central del Ecuador.

CAPÍTULO II

MARCO TEÓRICO

2.1. Sistemas de información

Los Sistemas de información en la actualidad son de vital importancia en las organizaciones ya que con su uso se logra la automatización de procesos mediante la integración y convergencia de las telecomunicaciones para proporcionar apoyo en la toma de decisiones.

La importancia de la información para todas las instituciones públicas o privadas, sean estas grandes, medianas o pequeñas, han hecho que los atacantes evolucionen radicalmente, estos se benefician de las vulnerabilidades en los sistemas informáticos y redes de telecomunicaciones para acceder a información crítica de las instituciones, para ello utilizan técnicas modernas o ciberataques como: ataques con *malwares, spoofing, phishing* o suplantación de identidad, *hijacking* o secuestro, ingeniería social, etc.

2.2. Riesgo Informático

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

“Los riesgos informáticos son problemas potenciales, que pueden afectar a los sistemas de información. Si no tienen las medidas adecuadas para salvaguardar los datos y la información, dichos riesgos se pueden presentar por las vulnerabilidades y amenazas en cualquier momento”. (Morán, 2016)

Cisco (2005) define y clasifica los riegos en los sistemas de la siguiente forma:

2.2.1. Sistemas de bajo riesgo: son los datos que al verse comprometidos (información accesible por el personal no autorizado, información corrompida o eliminada) no se interrumpiría el normal funcionamiento de la institución ni causaría pérdidas económicas. Los sistemas o la información se pueden recuperar sin mucho esfuerzo y la restauración es de corto plazo para continuar con su funcionamiento.

2.2.2. Los sistemas de riesgo mediano: son los datos que al verse comprometidos causaría una interrupción leve en la institución causando bajas pérdidas económicas. Los sistemas o la información demandan un esfuerzo ligero para restaurarse o el proceso de restauración tiene poca dificultad para el restablecimiento de los sistemas.

2.2.3. Sistemas de alto riesgo: son datos que al verse muy comprometidos causarían una interrupción extrema en la institución, causarían pérdidas económicas relevantes y amenazarían la integridad o la seguridad de la institución. Los sistemas o la información requieren de un mayor esfuerzo para restaurarse y restablecer los sistemas.

Para proteger la infraestructura de red de estas posibles amenazas, es necesario, implementar ciertos controles actualizados basados en la evaluación de los riesgos a través de la norma ISO/EC 27002:2013, logrando actualizar: la política, los procedimientos y controles con el objetivo de disminuir los riesgos de la información. La aplicación de estos controles implica el trabajo de toda la comunidad universitaria incluyendo el compromiso del personal que labora en la Dirección de Tecnologías (DTIC - UCE) en las diferentes áreas.

2.3. Principios de seguridad

2.3.1. Seguridad de la Información

La seguridad de la información se basa en tres aspectos fundamentales como son: la confidencialidad, la integridad y disponibilidad, para la protección de datos:

2.3.1.1. Confidencialidad

La confidencialidad implica que la información es accesible únicamente por el personal autorizado, es lo que se conoce como *need-to-know*., con este término se hace referencia a que la información solo debe ponerse en conocimiento de las personas, entidades o sistemas autorizados para su acceso. Ejemplos de falta de confidencialidad, son el robo de información confidencial por parte de un atacante a través de Internet, la divulgación no autorizada a través de las redes sociales de información confidencial o el acceso por parte de un empleado a información crítica de la institución a la que no debería tener acceso (INCIBE, 2015).

La confidencialidad, "busca prevenir el acceso no autorizado ya sea en forma Intencional o no intencional a la información. La pérdida de la confidencialidad puede ocurrir de muchas maneras, como por ejemplo con la publicación intencional de información confidencial de la organización" (Burgos y Campos, 2008, pág 237).

2.3.1.2. Integridad

La integridad considera que la información debe ser correcta y libre de modificaciones y errores. Es posible que sea alterada adrede o sin intención, puede ser incorrecta y se puede basar importantes decisiones en ella. Ejemplos de ataques contra la integridad de la información, que se realizan mediante la alteración malintencionada en carpetas del sistema operativo mediante la

explotación de una vulnerabilidad, o la modificación o eliminación de documentos importantes por parte del personal operativo de una institución o por error humano (INCIBE, 2015).

2.3.1.3. Disponibilidad

La disponibilidad de la información considera que la información esté siempre accesible cuando sea necesaria. Algunos ejemplos de falta de disponibilidad de la información son: cuando se pierde el acceso al correo electrónico institucional debido a un error de configuración del servidor de correo, o bien, cuando se encuentra frente a un ataque de denegación de servicio en el que el sistema impide accesos permitidos (INCIBE, 2015).

"La valoración de los activos de información de la institución en relación a estas tres dimensiones de la seguridad establece la orientación a seguir en la implantación y selección de medidas, también denominadas controles o salvaguardas" (INCIBE, 2015, pág. 3).

INCIBE (2015), menciona que se debe tener en cuenta que la implementación de un determinado control para mejorar la seguridad en una dimensión, puede afectar de forma negativa o positiva a otra de las dimensiones, por ello, es esencial conocer cuál de estas dimensiones es más importante proteger en cada sistema de información.

2.4. Sistema de Gestión de Seguridad

La seguridad de la información puede ser enfocada desde distintos puntos de vista, con diferentes objetivos y según distintas aproximaciones. Una institución que ponga en práctica algunos controles de seguridad básicos, como: un firewall, un antivirus, un

control de acceso físico y guardando las contraseñas de los equipos informáticos, todo ello dirigido y administrado desde el área de Sistemas de Información se podría pensar que se está gestionando la seguridad de la información.

Figura 2 Sistema de Gestión de seguridad

Fuente: (ISO27000)

El Sistema de Gestión de la Seguridad de la Información (SGSI) es de gran apoyo para la elaboración de políticas e instrucciones que se encaminen en la consecución de los objetivos de la institución con la finalidad de disminuir los niveles de riesgo; con un SGSI, se conoce los posibles riesgos a los que se encuentra expuesta su información y los asume, minimiza, transfiere o controla mediante un procedimiento ya establecido, documentado y conocido por todos.

A continuación, se establecen algunos beneficios de la norma internacional relacionada con la implementación de un SGSI, según la ISO27000:

- Establece lineamientos generales internos de la administración de seguridad de la información.
- Establece el perfeccionamiento de controles para el acceso a los sistemas de información.
- Monitorea los controles aplicados para la inspección de los activos de información que son revisados periódicamente.
- Aumenta la confianza entre los usuarios de la institución, debido a los criterios de confidencialidad que se aplican a sus datos.
- El contratar auditorías externas ayudan a identificar debilidades sobre la seguridad y obtener recomendaciones para mejorar la seguridad de la información.
- Ayuda a que las organizaciones continúen su trabajo habitual en caso de incidentes de seguridad de información.
- El cumplimiento de todos los estándares de seguridad de la información le puede permitir a la institución la certificación ISO.
- Ayuda a que le personal interno de la institución conozca la política de seguridad de la información y pueda desenvolverse correctamente en caso de incidentes.

2.5. NORMAS Y ESTÁNDARES

Se conoce el término "normas y estándares" a los acuerdos documentados legales que contienen especificaciones técnicas que establecen modelos o normas de referencia que se utilizan como reglas o guías que cumplen con su intención. En otras palabras, son leguajes frecuentes que permiten el entendimiento y la comunicación entre distintos actores.

En el caso de la gestión de información para que esta pueda ser compartida, debe cumplir un conjunto de normas y estándares que lo hagan posible. Existen entidades

internacionales como ISO, IEC, IEEE, ISACA por nombrar algunas, son las que se encargan de elaborar estos documentos a partir de las diferentes experiencias de diferentes organismos durante su desarrollo e intercambio de información.

2.6. ISO / IEC 27002: 2013

El objetivo de diseñar una política de seguridad para la infraestructura de red es tener un documento actualizado que contemple normas internacionales se seguridad, para ello esta norma es la mejor opción de acuerdo a las necesidades institucionales, para establecer controles y un adecuado monitoreo además de establecer buenas prácticas de la seguridad de la información y la concientización de todos los estamentos.

Según la (ISO27000) es un conjunto de estándares desarrollados por ISO (*International Organization for Standardization*) e IEC (*International Electrotechnical Commission*), que proporcionan un marco de gestión de la seguridad de la información el cual puede ser utilizado por cualquier tipo de institución sea esta, pública o privada, grande o pequeña.

ISO/IEC 27001

Publicada el 15 de octubre de 2005, revisada el 25 de septiembre de 2013 es la norma principal que contiene los requisitos del sistema de gestión de seguridad de la información y la cual contiene en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005.

En este grupo se encuentra la **ISO/IEC 27002** (anteriormente denominada estándar 17799:2005), norma internacional que establece las directrices para las mejores prácticas y apoyar la implantación del Sistema de Gestión de Seguridad de la Información (SGSI) en las instituciones (Ostec Business Security , s.f.).

ISO 27002:2013 proporciona los estándares de seguridad de acuerdo a la probabilidad de riesgos, se gestiona la selección e implementación de controles para la una buena administración y las mejores prácticas de un SGSI dentro de la institución.

Está diseñado para ser utilizado en las instituciones que tienen la intención de:

1. "Seleccionar controles dentro del proceso de implementación de un Sistema de Gestión de Seguridad de la Información basado en ISO / IEC 27001;
2. Implementar controles de seguridad de la información comúnmente aceptados;
3. desarrollar sus propias pautas de gestión de seguridad de la información" (ISO27000).

2.7.CONTROLES NORMA ISO/IEC 27002:2013

Dentro de ISO/IEC 27002:2013 se precisan los dominios objetivos de control que pueden ser implementados dentro de la institución para mitigar el impacto y la probabilidad de ocurrencia de los riesgos para el análisis y el desarrollo de la política de seguridad a diseñar para la Universidad Central.

Se debe resaltar en esta versión los controles relacionados con dispositivos móviles y teletrabajo que estaban asociados a los controles de acceso y que ahora se encuentran dentro de la organización de la seguridad de la información, a continuación, se describe los controles más relevantes que se encuentran en la norma ISO/ICE 27002:2013, la misma que se adjunta como anexo.

Tabla 1 *Dominios, objetivos de control, controles*

5. POLÍTICAS DE SEGURIDAD
5.1. Directrices de gestión.
Objetivo: "Proporcionar orientación y apoyo a la gestión de la seguridad de la información"

5.1.1. Políticas de la seguridad de la información 5.1.2. Revisión de las políticas para la seguridad de la información.
6. ORGANIZACIÓN DE LA SEGURIDAD.
6.1. Organización interna
Objetivo: "Implementación y operación de la seguridad dentro de la organización".
6.1.1. Roles y responsabilidades de la información. 6.1.2. Segregación de tareas. 6.1.3. Contacto con las autoridades 6.1.4. Contactos con grupos de interés especial 6.1.5. Seguridad de información en la gestión de proyectos
6.2 Dispositivos para las móviles y teletrabajo.
Objetivo: "Garantizar la seguridad en el teletrabajo y en el uso de dispositivos móviles".
6.2.1. Políticas de uso de dispositivos para movilidad 6.2.2. Teletrabajo
7. SEGURIDAD LIGADA A LOS RRHH.
7.1. Antes del empleo
Objetivo: Los empleados deben tener claro sus responsabilidades y funciones
7.1.1. Investigación de antecedentes. 7.1.2. Términos y condiciones del empleo.
7.2 Durante el empleo
Objetivo: "Asegurar que los empleados conozcan y cumplan con sus responsabilidades en relación a la seguridad".
7.2.1. Responsabilidades de gestión. 7.2.2. Concienciación, educación y capacitación en seguridad de la información. 7.2.3. Proceso disciplinario.
7.3 Finalización del empleo/cambio en el puesto de trabajo

Objetivo: "Proteger los intereses de la institución, aunque se ejecute un proceso de cambio o la finalización del empleo".
7.3.1. Responsabilidades ante la finalización o cambio.
8. GESTIÓN DE ACTIVOS.
8.1. Responsabilidad sobre los activos.
Objetivo: "Identificar los activos de la organización y definir las responsabilidades de protección adecuada". (UNE-EN, 2017, p. 22)
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.
Objetivo: "Asegurar que la información reciba un nivel adecuado de protección"
8.2.1. Directrices de clasificación de la información. 8.2.2. Etiquetado y manipulación de la información. 8.2.3. Manipulación de archivos de la información.
8.3. Manejo de los soportes de almacenamiento.
Objetivo: "Evitar la revelación, modificación, eliminación de la información"
8.3.1. Gestión de soportes extraíbles. 8.3.2. Eliminación de soportes. 8.3.3. Soportes físicos en tránsito.
9. CONTROL DE ACCESO.
9.1 Requisitos para el control de acceso.
Objetivo: "Limitar el acceso a los recursos de tratamiento de la".
9.1.1. Política de control de acceso 9.1.2. Control de acceso las redes y servicios asociados.
9.2. Gestión de acceso de usuarios.
Objetivo: "Garantizar el acceso de usuarios autorizados a los sistemas".

9.2.1. Gestión de altas y 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. Responsabilidad del usuario.
Objetivo: "Los usuarios son responsables de salvaguardar su información".
9.3.1. Uso de información confidencial o para la autentificación.
9.4. Control de acceso a sistemas y aplicaciones.
Objetivo: "Prevenir el acceso no autorizado a los 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 usuarios. 9.4.4. Uso de utilidades con privilegios del sistema 9.4.5. Control de acceso al código fuente de los programas.
10. CRIPTOGRAFÍA.
10.1. Controles criptográficos.
Objetivo: "Garantizar un uso adecuado y eficaz de la criptografía".
10.1.1. Políticas de uso de los controles criptográficos. 10.1.2. Gestión de claves.
11. SEGURIDAD FÍSICA Y DEL ENTORNO.
11.1. Áreas seguras.
Objetivo: "Prevenir el acceso físico no autorizado".
11.1.1. Perímetros de seguridad física. 11.1.2. Controles físicos de entrada. 11.1.3. Seguridad de oficinas, despacho 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 descarga y descarga.

11.2. Seguridad de los equipos.
Objetivo: "Evitar la pérdida, daño, robo de los activos".
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 los dispositivos de almacenamiento. 11.2.8. Equipos informáticos de uso desatendidos. 11.2.9 Política de puesto de trabajo despejado y pantalla limpia.
12. SEGURIDAD DE LAS OPERACIONES.
12.1. Responsabilidades y procedimientos de operación.
Objetivo: "Asegurar el funcionamiento correcto y seguro de las instalaciones".
12.1.1. Documentación de procedimientos operacionales. 12.1.2. Gestión de cambios. 12.1.3. Gestión de capacidades. 12.1.4. Separación de los recursos de desarrollo, prueba y operación.
12.2. Protección contra código malicioso.
Objetivo: "Asegurar que la información esté protegida contra el malware".
12.2.1. Controles contra el código malicioso.
12.3. Copias de seguridad.
Objetivo: "Evitar la pérdida de datos".
12.3.1 Copias de seguridad de la información
12.4. Registros y supervisión.
Objetivo: "Registrar eventos y generar evidencias".

12.4.1. Registro de eventos. 12.4.2. Protección de la información de registro. 12.4.3. Registro de administración y operación. 12.4.4. Sincronización del reloj.
12.5. Control del software en explotación.
Objetivos: "Asegurar la integridad del software en explotación".
12.5.1. Instalación del software en explotación
12.6. Gestión de la vulnerabilidad técnica
Objetivo: "Reducir los riesgos resultantes de la explotación de las vulnerabilidades".
12.6.1. Gestión de las vulnerabilidades técnicas. 12.6.2. Restricción en la instalación de software.
12.7. Consideraciones sobre la auditoria de sistemas de información.
Objetivo: "Minimizar el impacto de la auditoría en los sistemas operativos".
12.7.1 Controles de auditoría de sistemas de información
13. SEGURIDAD DE LAS COMUNICACIONES.
13.1. Gestión de la seguridad de las redes
Objetivo: "Asegurar la protección de la información en las redes".
13.1.1. Controles de red. 13.1.2. Mecanismos de seguridad asociado a servicios en red. 13.1.3. Segregación en redes.
13.2 Intercambio de información
Objetivo: "Mantener segura la información que se transfiere dentro y fuera".
13.2.1. Políticas y procedimientos de intercambio de información. 13.2.2. Acuerdos de intercambio de información. 13.2.3. Mensajería electrónica. 13.2.4. Acuerdos de confidencialidad o no revelación.

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
14.1. Requisitos de seguridad en los sistemas de información.
Objetivo: "Garantizar que la seguridad de la información sea parte integral de los sistemas de información a través de todo el ciclo de vida".
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 el desarrollo y en los procesos de soporte.
Objetivo: "Garantizar la seguridad de la información en el ciclo de vida de desarrollo de los sistemas de información".
.2.1. Políticas 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 de sistemas seguros 14.2.6. Seguridad en entornos de desarrollo. 14.2.7. Externalización del desarrollo del software 14.2.8. Pruebas de funcionalidad durante el desarrollo de los sistemas. 14.2.9. Pruebas de aceptación de sistemas.
14.3. Datos de prueba.
Objetivo: "Asegurar la protección de los datos de prueba".
14.3.1. Protección de los datos de prueba.
15. RELACIÓN CON PROVEEDORES.
15.1. Seguridad con las relaciones con proveedores.
Objetivo: "Asegurar la protección de los activos que sean accesibles a proveedores".

15.1.1. Política de seguridad de la información en las relaciones con los proveedores 15.1.2. Requisitos de seguridad de contratos con terceros 15.1.3. Cadena de suministro de tecnología de la información y de las comunicaciones
15.2. Gestión de la prestación de servicios por suministradores.
Objetivo: "Mantener un nivel acordado de seguridad y de provisión de servicios".
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 DE SEGURIDAD DE LA INFORMACIÓN.
16.1 Gestión de incidentes de seguridad de la información y mejoras
Objetivo: "Asegurar un enfoque coherente y eficaz para la gestión de incidentes".
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 incidentes de seguridad de la información. 16.1.6. Aprendizaje de los incidentes de seguridad de la información. 16.1.7. Recopilación de evidencias.
17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN
17.1. Continuidad de la seguridad de la información.
Objetivo: "La continuidad de la seguridad de la información debe formar parte de los sistemas de gestión para la correcta evolución del negocio". (UNE-EN, 2017, p. 32)
17.1.1. Planificación de la continuidad de la seguridad de la información 17.1.2. Implementar 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 Redundancia

Objetivo: “Asegurar la disponibilidad de los recursos de tratamiento de la información”. (UNE-EN, 2017, p. 32)
17.2.1 Disponibilidad de instalaciones para el procesamiento de la información

Fuente: (UNE-EN ISO/IEC 27001:2017, 2013)

2.8. Metodología para el análisis de riesgos (Metodología Magerit)

Para el análisis de vulnerabilidades de acuerdo a las observaciones realizadas se utilizó la metodología Magerit, (Consejo Superior de Administración Electrónica, 2012), la cual permitió identificar las amenazas existentes en el uso y manejo de los activos de información. Magerit es una metodología para el análisis de gestión de riesgos de los sistemas de información que ayuda a mantener los riesgos bajo control mediante un tratamiento oportuno.

Con Magerit se realizó el análisis de los activos existentes en la infraestructura tecnológica, las amenazas sobre estos activos, la estimación del impacto y el riesgo, los mismos que se resumen en la matriz de riesgos identificados a través de la norma ISO/IEC 27002:2013.

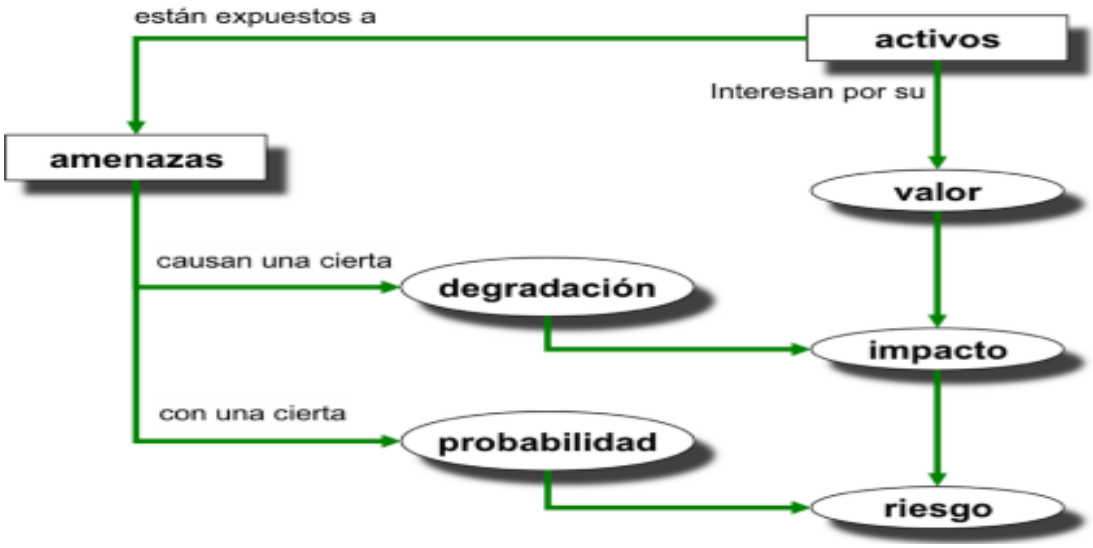


Figura 3 *Fases de la Metodología Magerit*

Fuente: (Magerit 3.0 Libro I - Método., 2012)

2.9. Determinar los activos de la organización

El primer paso se basa en determinar los datos y equipos de la institución, para este análisis se establece un catálogo de activos relevantes clasificados dentro de cada categoría:

Tabla 2 *Determinación de activos Sugiero que la tabla se a interlineado sencillo*

ACTIVO	DEFINICIÓN	EJEMPLOS
[S] Servicio	Los servicios son aquellos que se brindan a los usuarios internos y externos.	Internet, Acceso a cuenta local, correo electrónico, almacenamiento y transferencia de archivos, servicio de directorio activo.
[D] Datos/información	Los datos son información importante para la institución que los usuarios deben proteger. Su clasificación determina los niveles de confidencialidad.	Documentación académica, documentos de gestión administrativa interna, código fuente, manuales de configuración, logs.
[SW] Aplicaciones (software)	Las aplicaciones se refieren a programas, sistemas, desarrollos, entre otros. Estos van ligados con la automatización de los procesos de la institución.	Desarrollos de aplicaciones de acuerdo a las necesidades, servidor de aplicaciones, servidor de correo electrónico, servidor de archivos, bases de datos, utilitarios, antivirus, sistemas operativos, sistema de backups.
[HW]	Tiene relación con los bienes o equipos informáticos que utilizan los usuarios para el	Computadoras (escritorio, laptops), impresoras, periféricos, escáners, modemes, routers, cortafuegos,

ACTIVO	DEFINICIÓN	EJEMPLOS
Equipos informáticos (hardware)	procesamiento o almacenamiento de la información.	punto de acceso wireless, central telefónica, etc.
[COM] Redes de comunicaciones	Abarcan los equipos de infraestructura de red. Activos que permiten la interconectividad e intercambio de información.	Red de cableado estructurado, red telefónica, ADSL, red inalámbrica, Internet, red privada virtual.
[SI] Soporte de información	Son todos los dispositivos de almacenamiento de información.	Discos duros, almacenamiento en red, Cd-rom, dispositivos USB, DVD, tarjetas de memoria, cintas magnéticas, etc.
[AUX] Equipamiento auxiliar	Se describe al equipamiento que complementa los activos informáticos apoyando la infraestructura de red.	Generadores eléctricos, fuentes de alimentación, equipos de climatización, robots de discos y de cintas, suministros esenciales, controles de acceso, cajas fuertes, entre otros.
[L] Instalaciones	Se relaciona con las edificaciones donde se encuentra la infraestructura tecnológica.	Edificios, data center, oficinas, dependencias.
[P] Personal	Son todos los usuarios involucrados con los procesos y sistemas de información dentro de la institución.	Técnicos, administradores de sistemas, administradores de bases de datos, desarrolladores, etc.

Fuente: (Magerit 3.0 Libro II Catálogo de elementos, 2012)

Las dimensiones de valoración de activos dependen de sus características y atributos en donde se valora las derivaciones de la materialización de una amenaza, basado en el impacto que tendría en relación a su disponibilidad, confidencialidad e integridad y autenticidad.

2.10. Criterio de valoración de activos

A continuación, se describe los criterios de valoración de los activos en cuanto a la confidencialidad, integridad y disponibilidad, de la siguiente forma:

Tabla 3 *Criterio de Valoración de confidencialidad según Magerit*

VALOR	CONFIDENCIALIDAD
0	Puede ser conocida y utilizada por cualquier persona, dentro o fuera de la institución.
1	Puede ser conocida y utilizada por cualquier persona, dentro de la institución.
2	Puede ser conocida y utilizada por un grupo de personas que la necesiten para realizar su trabajo.
3	Puede ser conocida y utilizada por un grupo muy reducido por personas, cuya divulgación podría ocasionar perjuicio a la institución o a terceros.

Fuente: (Magerit 3.0 Libro II Catálogo de elementos, 2012)

Tabla 4 *Criterio de valoración de la integridad según Magerit*

VALOR	INTEGRIDAD
0	Cuya modificación no autorizada puede repararse fácilmente, o que no afecta a las actividades de la institución.
1	Cuya modificación no autorizada puede repararse, aunque podría ocasionar un perjuicio para la institución o terceros.
2	Cuya modificación no autorizada es de difícil reparación, y podría ocasionar un perjuicio significativo para la institución o terceros.
3	Cuya modificación no autorizada no podría repararse, impidiendo la realización de las actividades.

Fuente: (Magerit 3.0 Libro II Catálogo de elementos, 2012)

Tabla 5 *Criterio de valoración de la disponibilidad según Magerit*

VALOR	DISPONIBILIDAD
0	Cuya inaccesibilidad no afecta la actividad normal de la Institución.
1	Cuya inaccesibilidad durante una semana podría ocasionar un perjuicio significativo para la Institución.
2	Cuya inaccesibilidad durante la jornada laboral podría impedir la ejecución de las actividades de la Institución.
3	Cuya inaccesibilidad durante una hora podría impedir la ejecución de las actividades de la Institución.

Fuente: (Magerit 3.0 Libro II Catálogo de elementos, 2012)

De acuerdo Magerit calculando el promedio de las escalas se obtiene el nivel de criticidad de los activos de la institución, dependiendo de los criterios de valoración el nivel de criticidad puede ser alto, medio y bajo, como se muestra en la tabla 6.

Tabla 6 *Criterio de valoración del nivel de criticidad según Magerit*

NIVEL DE CRITICIDAD	
ALTO	2 – 3
MEDIO	1 – 2
BAJO	0 – 1

Fuente: (Magerit 3.0 Libro II Catálogo de elementos, 2012)

Para una mejor comprensión de los niveles de valoración de criticidad se los distingue mediante colores de la siguiente forma:

- **Verde**: El impacto es menor y no compromete la continuidad del negocio.
- **Amarillo**: El impacto es apreciable pero no compromete la continuidad del negocio.
- **Rojo**: El impacto es importante y afecta totalmente la continuidad del negocio.

Nota: Adaptado de: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

2.11. Escala de valoración de la probabilidad

Para estimar cuan probable o improbable es para que se materialice una amenaza, Magerit utiliza la siguiente escala para la valoración de la probabilidad.

Tabla 7 *Probabilidad de Ocurrencia*

VALOR	***DESCRIPCIÓN***
0	La amenaza no se materializa nunca.
1	La amenaza se materializa una vez cada año.
2	La amenaza se materializa una vez cada mes.
3	La amenaza se materializa una vez cada semana.

Fuente: (Magerit 3.0 Libro II Catálogo de elementos, 2012)

2.12. Identificación de amenazas

En un análisis de riesgos de sistemas de información se debe considerar las posibles amenazas sobre los activos, en el siguiente listado se menciona las principales:

- De origen Natural: son sucesos que ocurren sin la intervención del ser humano, pueden ser de tipo natural como terremotos, inundaciones, ante lo que el sistema de información es víctima pasiva, entre los principales encontramos:
    - Fuego
    - Agua

    - Desastres Naturales
- De origen industrial: son los que ocurren de forma accidental y derivados de la actividad humana, pero de tipo industrial, en esta categoría se encuentran principalmente:
    - Corte del suministro eléctrico
    - Condiciones inadecuadas de temperatura o humedad
    - Fallo de servicios de comunicaciones
    - Desastres industriales
- Errores ya fallos no intencionados: son errores causados por el ser humano realizados sin premeditación, en este grupo se encuentran:
    - Fuga de Información
    - Introducción de falsa información
    - Acceso no autorizado
    - Vulnerabilidad de programas (software)
    - Corrupción de la información
    - Destrucción de información
    - Interceptación de información (escucha)
    - Indisponibilidad del personal
    - Agotamiento de recursos
    - Errores de los usuarios
    - Errores del administrador
    - Errores de configuración
    - Degradación de los soportes de almacenamiento de la información
    - Difusión de software dañino
    - Errores de mantenimiento / actualización de programas (software)

- Errores de mantenimiento / actualización de equipos (hardware)
- Caída del sistema por sobrecarga

- Ataques intencionales: son causados deliberadamente por el ser humano, personas que tienen accesos no autorizado a los sistemas de información y pueden causar problemas con ataques intencionados con el fin de favorecerse indebidamente de la información, causar daño y perjuicio a una institución, en esta categoría se encuentran:
  - Denegación de servicio
  - Robo
  - Ataques destructivos
  - Extorsión
  - Ingeniería social
  - Manipulación de logs
  - Abuso de privilegios de acceso
  - Manipulación de equipos
  - Manipulación de configuración
  - Alteración de la información

    Fuente: (Magerit 3.0 Libro II Catálogo de elementos, 2012, págs. 25-47)

2.13. Estimación e impacto

Impacto se conoce como el daño que se produce sobre el activo el cual se calcula en base a tablas de doble entrada:

Tabla 8 *Valoración del impacto valor * degradación*

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

Fuente: (Magerit 3.0 Libro III, 2012)

Los activos con una calificación MA (muy alta) deben ser atendidos por la institución de manera inmediata.

Tabla 9 *Valoración del impacto*

VALOR	***DESCRIPCIÓN***
0	No existen consecuencias si se materializa la amenaza
1	El daño derivado de la materialización de la amenaza no tiene consecuencias relevantes para la organización.
2	El daño derivado de la materialización de la amenaza tiene consecuencias relevantes para la organización.
3	El daño derivado de la materialización de la amenaza tiene consecuencias graves para la organización.

Fuente: (Magerit 3.0 Libro III, 2012)

2.14. Análisis del riesgo

El análisis de riegos es una herramienta de gestión y parte esencial del proceso de seguridad el cual debe mantenerse permanentemente actualizado en un entorno controlado minimizando los riesgos hasta un nivel aceptable los cuales se realizan mediante el despliegue de políticas de seguridad.

2.15. Análisis y valoración del riesgo a través de Magerit

Riesgo es la medida de daño probable sobre un sistema de información, al conocer el impacto de las amenazas sobre los activos se debe tener en cuenta la probabilidad de ocurrencia.

Tabla 10 *Valoración de riesgo*

RANGO	*DESCRIPCIÓN*
Riesgo <= 4	El COCIBER considera el riesgo poco relevante
Riesgo > 6	El COCIBER considera el riesgo importante y debe proceder a su tratamiento.

Fuente: (Magerit 3.0 Libro III, 2012)

El riesgo es directamente proporcional al impacto y la probabilidad en donde se debe distinguir varias zonas para su tratamiento.

Tabla 11 *Riesgo en función del impacto y la probabilidad*

TABLA DE RIESGO

		PROBABILIDAD		
		Bajo	**Medio**	**Alto**
IMPACTO	**Alto**	**3**	**6**	**9**
	Medio	**2**	**4**	**6**
	Bajo	**1**	**2**	**3**

Fuente: (Magerit 3.0 Libro I - Método., 2012)

Magerit determina el riesgo en un mapa de calor en el cual distribuye por zonas acorde al daño que figura en el activo de la institución.

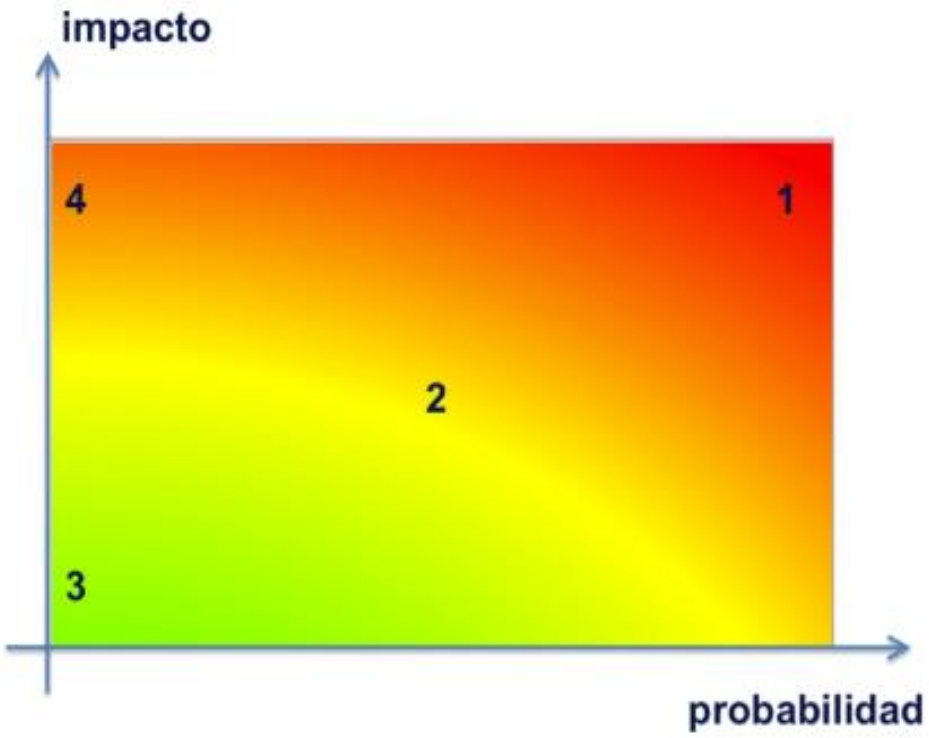


Figura 4 *Mapa de riesgos*

Fuente. (Magerit 3.0 Libro I - Método., 2012)

Para visualizar y comprender la valoración del riego se ubica a los activos de acuerdo a la zona en el mapa de la siguiente forma:

Zona 1: riego muy probable, muy alto impacto

Zona 2: franja amarilla, situaciones poco probables de impacto medio y situaciones muy probables e impacto bajo.

Zona 3: riesgo improbable de bajo impacto

Zona 4: riesgo improbable, de alto impacto

2.16. Salvaguardas o contramedidas

Las salvaguardas o también conocidas como contramedidas son los procedimientos tecnológicos que reducen el riesgo en los activos y permiten hacer frente a las amenazas que varían de acuerdo a las nuevas tecnologías, las más relevantes según Magerit 3.0:

1. Protección de datos / información
2. Protección de los servicios
3. Protección de los equipos
4. Protección de las comunicaciones

2.17. Política de seguridad.

La política de seguridad son un conjunto de reglas, procedimientos y buenas prácticas que aseguren un nivel de seguridad de acuerdo a las necesidades de los sistemas con el fin de minimizar el riesgo.

UNIR (2020), menciona que la política de seguridad es una serie de normas y directrices que garantizan la confidencialidad, integridad y disponibilidad de la información que se la define a alto nivel con la implementación de controles, se desarrolla bajo procedimientos e instrucciones técnicas.

CAPÍTULO III

SITUACIÓN ACTUAL

3. LA UNIVERSIDAD CENTRAL DEL ECUADOR

3.1. Descripción de la Institución

El Estatuto vigente de la Universidad Central del Ecuador fue aprobado en octubre de 2019, el cual menciona en su base legal que es una institución de educación superior que:

> Se rige por la Constitución de la República del Ecuador, la Ley Orgánica de Educación Superior (LOES) y su Reglamento General, los reglamentos y las resoluciones expedidas por la Secretaría de Educación Superior, Ciencia y Tecnología, el Consejo de Educación Superior (SENESCYT), el Consejo de Aseguramiento de la Calidad de la Educación Superior (CACES), el Estatuto Universitario, los reglamentos y las resoluciones expedidas por el Honorable Consejo Universitario (HCU), así como las demás normativas aplicables a las Universidades del Ecuador (Estatuto Universitario, 2019).

Para la Dirección de Tecnologías el presente Estatuto toma las siguientes consideraciones:

> **Artículo 66**.- Director de Tecnologías de Información y Comunicaciones (Tics): Será nombrado por el Rector, siendo este cargo de libre nombramiento y remoción, se encargará de regulación, planificación de los recursos tecnológicos orientados al uso de y transferencia de la información del personal de la comunidad universitaria. En caso de ausencia temporal, el Rector, nombrará un

profesional que cumpla con las funciones, hasta que el Director de Tecnología de Informática y Comunicaciones (Tics), retome sus labores por las cuales fue nombrado. En caso de ausencia definitiva el Rector nombrará su reemplazo (Estatuto Universitario, 2019).

Las áreas de la Dirección de Tecnologías son las siguientes:

a. Responsable de soporte tecnológico de hardware y software;

b. Responsable de proyectos de software y producción;

c. Responsable de desarrollo de software;

d. Responsable de infraestructura tecnológica;

e. Responsable de seguridad informática, y;

f. Los demás que se encuentren bajo su responsabilidad.

Artículo 66.2.- Funciones:

Dentro de las funciones del Director de Tecnologías que establece el Estatuto Universitario (2019) y por ende la dirección de tecnologías se describen las siguientes: Proponer las acciones de planificación e implementación de soluciones tecnológicas alineado con los planes de la Universidad Central del Ecuador que optimicen los procesos académicos de investigación y administraciones institucionales;

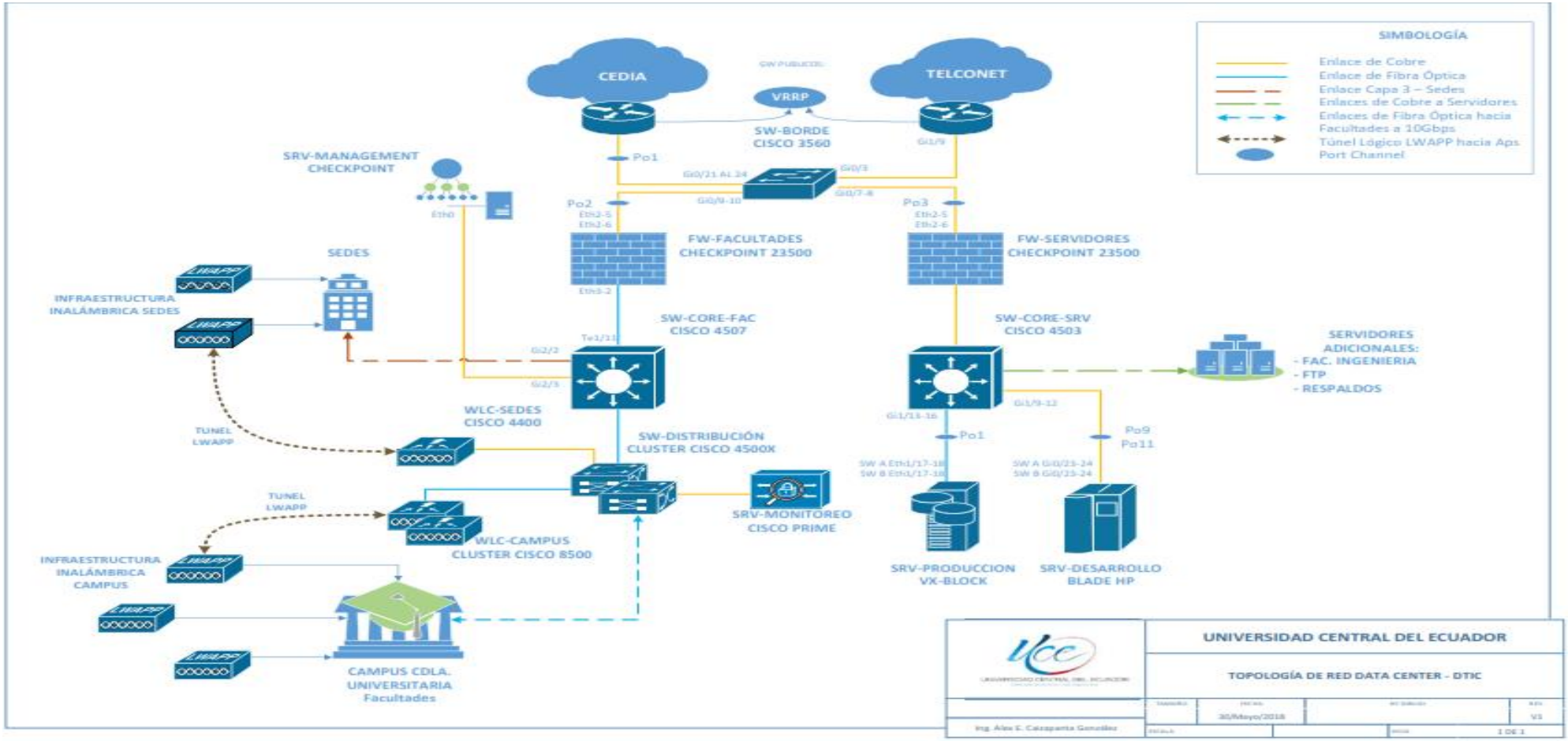
a. Desarrollar, implementar y administrar las políticas y lineamientos referentes a las tecnologías de información y comunicación aprobados en la Universidad Central del Ecuador;
b. Elaborar las políticas y programas de gestión documental de la Universidad Central del Ecuador;
c. Elaborar y dar seguimiento al plan operativo anual y al plan anual de política pública y al plan anual de compras;

d. Elaborar, ejecutar y evaluar el plan de mantenimiento preventivo y correctivo de la infraestructura tecnológica;
e. Administrar la infraestructura tecnológica de la Universidad Central del Ecuador;
f. Garantizar la provisión de equipos y procesos informáticos para que se ejecuten las actividades en todas las dependencias;
g. Desarrollar, implementar y administrar el software para el desarrollo de la gestión del sistema integral de información de la Universidad Central del Ecuador;
h. Desarrollar y aplicar las políticas y lineamientos para la seguridad informática de la Universidad Central del Ecuador;
i. Proponer políticas para el análisis de funcionalidad de software y control de calidad;
j. Proponer metodología para el desarrollo de sistemas en diferentes plataformas;
k. Proponer estándares de atención para el soporte técnico;
l. Proponer plataformas tecnológicas y equipos para la utilización en la Universidad Central del Ecuador;
m. Evaluar y controlar las puestas en producción de los servicios tecnológicos;
n. Realizar los informes de viabilidad de la adquisición de hardware y software de la Universidad Central del Ecuador;
o. Coordinar con el área de Tics de las Facultades la aplicación de las políticas de la dirección;
p. Elaborar informes para las autoridades sobre las actividades desarrolladas por la dirección;

q. Preparar informes de gestión semestral para conocimiento del Vicerrector Administrativo y Financiero;

r. Proponer los requerimientos de capacitación para el personal que se encuentra bajo su responsabilidad.

Figura 5 *Diagrama de la infraestructura de red 2020*



Fuente Memoria Técnica infraestructura de red 2020

3.2. Identificación de activos.

Luego de las inspecciones técnicas realizadas en la Dirección de Tecnologías se considera que los principales activos que se encuentran en la Universidad Central son los siguientes:

1. **Servicios Universitarios**
    a. Internet Administrativos
    b. Correo Institucional
    c. Directorio Activo
    d. Gestión Parque Informático

2. **Datos e Información**
    a. Estatutos, reglamentos
    b. Documentos confidenciales – roles
    c. Documentos académicos - notas
    d. Documentos públicos
    e. Base de datos – académicas

3. **Aplicaciones institucionales**
    a. Página web institucional
    b. Sistema académico institucional
    c. Sistema de educación virtual
    d. Sistema de gestión documental
    e. Sistema de admisión posgrados
    f. Sistema de nóminas
    g. Sistema de titulación
    h. Sistema de talento humano

i. Sistema de emisión de títulos

j. Sistema de recaudaciones

k. Sistema de mesa de ayuda

l. Sistema de Historias clínicas Hospital del día

m. Sistema integrado de bibliotecas

4. Equipos Informáticos

a. Servidores

b. PC’s (Mac - todo en uno – escritorio)

c. Impresoras

d. Cámaras de vigilancia

e. Pantallas virtuales

f. Telefonía Ip

5. Redes de Comunicaciones

a. Switchs

b. Routers

c. Access Points

d. Firewall

e. Controladoras Wifi

f. Cableado estructurado

6. Soporte de Información

a. Almacenamiento en Red

b. Back up de servidores

c. Disco Duro Externo

d. Servidor FTP

e. Cintas Magnéticas

f. Nube Microsoft

7. **Equipamiento Auxiliar**

    a. Fuentes de alimentación

    b. Aire acondicionado

    c. Generadores eléctricos

    d. Control de acceso

8. **Instalaciones**

    a. Departamento de TI UCE

    b. Centro de datos Facultades

    c. Data Center Institucional

9. **Personal**

    a. Director de Tecnologías

    b. Soporte nivel 1 – Facultades – DTIC

    c. Soporte nivel 2 – Infraestructura

    d. Soporte desarrollo

3.3. Valoración de criticidad de activos

Una vez identificados los activos el siguiente paso es valorar la criticidad de los activos de acuerdo a los criterios de confidencialidad, integridad y disponibilidad.

Tabla 12 *Valoración de criticidad de activos*

TIPO	IDENTIDAD	ACTIVO	PROCESO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CRITICIDAD
Servicios	S1	Internet Administrativo	Infraestructura	2	2	2	2,0
	S2	Correo Institucional	Infraestructura	2	2	2	2,0
	S3	Directorio Activo	Infraestructura	2	3	3	2,7
	S4	Gestión del parque informático	Soporte Usuario	2	2	2	2,0
Datos e Información	D1	Estatutos reglamentos	Seguridad de la Información	1	2	2	1,7
	D2	Documentos Confidenciales - roles	Seguridad de la Información	3	3	2	2,7
	D3	Documentos académicos - notas	Seguridad de la Información	2	3	2	2,3
	D4	Documentos públicos	Seguridad de la Información	1	2	2	1,7
	D5	Base de datos - académicas	Seguridad de la Información	1	1	1	1,0
Aplicaciones	SW1	Página web institucional	Desarrollo / InfraesDatos	1	2	2	1,7
	SW2	Sistema académico institucional	Desarrollo / InfraesDatos	3	3	3	3,0
	SW3	Sistema de educación virtual	Desarrollo / InfraesDatos	2	2	3	2,3
	SW4	Sistema de gestión documental	Soporte Usuario	1	2	2	1,7
	SW5	Sistema de admisión posgrados	Desarrollo / Mantenimiento	2	2	1	1,7
	SW6	Sistema de nóminas	Desarrollo / InfraesDatos	3	3	3	3,0

TIPO	IDENTIDAD	ACTIVO	PROCESO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CRITICIDAD
(Software)	SW7	Sistema de titulación	Desarrollo / InfraesDatos	2	2	1	1,7
	SW8	Sistema de talento humano	Desarrollo / InfraesDatos	1	2	1	1,3
	SW9	Sistema de emisión de títulos	Soporte Usuario	1	2	1	1,3
	SW10	Sistema de recaudaciones	Desarrollo / Mantenimiento	3	3	3	3,0
	SW11	Sistema de mesa de ayuda	Soporte Usuario	1	1	1	1,0
	SW12	Sistema de Historias clínicas Hospital del Día	Infraestructura	2	2	1	1,7
	SW13	Sistema integrado de bibliotecas	Desarrollo / InfraesDatos	1	1	1	1,0
Equipos Informáticos	HW1	Servidores	Mantenimiento	3	3	3	3,0
	HW2	PC's Mac Todo en uno	Mantenimiento	3	2	2	2,3
	HW3	Impresoras	Mantenimiento	1	1	2	1,3
	HW4	Cámaras de vigilancia	Redes	3	2	2	2,3
	HW5	Pantallas virtuales	Redes	2	1	1	1,3
	HW6	Telefonía IP	Redes	1	1	1	1,0
	COM1	Switchs	Infraestructura	3	3	3	3,0
	COM2	Routers	Infraestructura	3	3	3	3,0

TIPO	IDENTIDAD	ACTIVO	PROCESO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CRITICIDAD
Redes de Comunicaciones	COM3	Access Points	Infraestructura	2	1	2	1,7
	COM4	Firewalls	Infraestructura	3	3	3	3,0
	COM5	Controladoras Wifi	Infraestructura	1	2	2	1,7
	COM6	Cableado estructurado	Infraestructura	3	2	3	2,7
Soporte de Información	SI1	Almacenamiento en Red	Respaldos	2	3	3	2,7
	SI2	Back up de servidores	Respaldos	3	3	3	3,0
	SI3	Disco Duro Externo	Respaldos	1	2	2	1,7
	SI4	Servidor FTP	Respaldos	2	2	2	2,0
	SI5	Cintas magnéticas	Respaldos	2	1	2	1,7
	SI6	Nube MS	Respaldos	2	1	2	1,7
Equipamiento Auxiliar	AUX1	Fuentes de alimentación	Infraestructura	2	2	3	2,3
	AUX2	Aire acondicionado	Mantenimiento	1	2	2	1,7
	AUX3	Sistema anti incendios	Infraestructura	1	2	2	1,7
	AUX4	Generadores eléctricos	Infraestructura	1	2	3	2,0
	AUX5	Control de acceso	Seguridad de la Información	3	3	3	3,0
Instalaciones	L1	Departamento de TI UCE	Infraestructura	2	3	3	2,7

TIPO	IDENTIDAD	ACTIVO	PROCESO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CRITICIDAD
	L2	Centro de datos facultades	Infraestructura	2	3	3	2,7
	L3	Data Center Institucional	Infraestructura	3	3	3	3,0
Personal	P1	Director de Tecnologías	Director DTIC	2	2	2	2,0
	P2	Soporte Nivel 1- Facultades -Dtic	Soporte Usuario	2	2	1	1,7
	P3	Soporte Nivel 2 - Infraestructura	Infraestructura	2	2	1	1,7
	P4	Soporte desarrollo	Desarrollo / InfraesDatos	2	2	1	1,7

Elaborado por el autor de la investigación

Los activos críticos con probabilidad de amenaza son aquellos que luego de la respectiva valoración la criticidad tiene calificaciones mayores o iguales a 2.

Luego de la valoración los activos críticos para la Universidad Central y que se debe analizar la probabilidad, el impacto para determinar el riesgo, resultado de la Tabla 12 son los siguientes:

- Internet Administrativo
- Correo Institucional
- Directorio Activo
- Sistema Académico
- Sistema Educación Virtual
- Servidores
- Pc´s Mac Todo en uno

Switchs

- Routers
- Firewall
- Cableado Estructurado
- Centro de datos Facultades
- Data Center

3.4. Valoración de la probabilidad

Una vez valorada la criticidad de los activos se procede a valorar la probabilidad de amenazas sobre los activos de la Institución:

Tabla 13 *Matriz de Probabilidad*

	ACTIVO	SERVICIOS				DATOS E INFORMACIÓN		APLICACIONES				EQUIPOS INFORMÁTICO			REDES DE COMUNICACIONES				SOPORTE DE INFORMACIÓN			EQUIPO AUXILIAR			INSTALACIONES			PERSONAL
N°	AMENAZA	S1	S2	S3	S4	D2	D3	SW2	SW3	SW6	SW10	HW1	HW2	HW4	COM1	COM2	COM4	COM6	SI1	SI2	SI4	AUX1	AUX4	AUX5	L1	L2	L3	P1
1	Fuego	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
2	Daños por agua	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	Desastres naturales	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0
4	Corte del suministro eléctrico	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
5	Condiciones inadecuadas de temperatura o humedad	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	3	0	0	0	1	1	1	1	1	0	0
6	Fallo de servicios de comunicaciones	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	0	0	2	2	2	2	2
7	Desastres industriales	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
8	Fuga de información	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
9	Introducción de falsa información	1	1	1	2	1	1	1	1	1	1	1	3	1	0	0	1	1	1	1	1	0	0	1	1	1	1	1
10	Acceso no autorizado	1	1	1	2	2	2	1	1	1	1	1	3	2	0	0	0	0	0	0	0	2	0	2	0	0	0	0
11	Vulnerabilidad de programas (software)	1	0	0	3	0	1	1	1	1	1	1	3	1	1	1	0	0	0	0	0	0	0	1	0	0	0	0

	ACTIVO	SERVICIOS				DATOS E INFORMACIÓN		APLICACIONES				EQUIPOS INFORMÁTICO			REDES DE COMUNICACIONES				SOPORTE DE INFORMACIÓN			EQUIPO AUXILIAR			INSTALACIONES			PERSONAL
N°	AMENAZA	S1	S2	S3	S4	D2	D3	SW2	SW3	SW6	SW10	HW1	HW2	HW4	COM1	COM2	COM4	COM6	SI1	SI2	SI4	AUX1	AUX4	AUX5	L1	L2	L3	P1
12	Corrupción de la información	1	1	1	3	1	1	0	0	0	0	0	3	1	1	1	0	0	1	1	1	0	0	0	1	1	1	1
13	Destrucción de información	1	1	1	2	1	1	1	1	1	1	0	3	1	0	0	0	0	0	0	0	0	0	0	1	1	1	1
14	Interceptación de información (escucha)	2	1	1	3	2	2	1	1	1	1	1	3	2	1	1	0	1	1	1	1	0	0	0	1	1	1	1
15	Indisponibilidad del personal	2	2	2	3	2	2	3	3	3	3	1	3	3	3	3	1	2	2	2	2	0	0	0	2	2	2	2
16	Agotamiento de recursos	1	1	1	3	1	1	1	1	1	1	1	3	3	1	1	0	1	3	3	3	2	0	1	2	2	2	1
17	Errores de los usuarios	2	3	1	3	3	3	2	2	2	2	3	3	3	1	1	1	2	0	0	0	3	0	2	2	2	2	2
18	Errores del administrador	2	1	1	2	1	1	2	2	2	2	2	2	1	2	2	2	2	1	1	1	3	0	2	1	1	1	1
19	Errores de configuración	1	1	1	3	1	3	3	2	2	2	2	2	1	2	2	2	2	1	1	1	3	0	2	1	1	1	0
20	Degradación de los soportes de almacenamiento de la información	2	3	2	3	1	2	3	3	2	2	2	3	2	2	2	1	2	2	2	2	0	0	2	2	2	2	2
21	Difusión de software dañino	3	3	2	3	0	0	2	2	2	2	1	3	3	1	1	1	1	1	1	1	0	0	1	2	2	2	2

	ACTIVO	SERVICIOS				DATOS E INFORMACIÓN		APLICACIONES				EQUIPOS INFORMÁTICO			REDES DE COMUNICACIONES				SOPORTE DE INFORMACIÓN			EQUIPO AUXILIAR			INSTALACIONES			PERSONAL
N°	AMENAZA	S1	S2	S3	S4	D2	D3	SW2	SW3	SW6	SW10	HW1	HW2	HW4	COM1	COM2	COM4	COM6	SI1	SI2	SI4	AUX1	AUX4	AUX5	L1	L2	L3	P1
22	Errores de mantenimiento / actualización de programas (software)	3	3	2	3	0	0	2	2	2	2	2	3	3	2	2	2	2	2	2	2	0	0	2	2	2	2	2
23	Errores de mantenimiento / actualización de equipos (hardware)	3	3	3	3	0	0	2	2	2	2	1	3	1	1	1	1	3	1	3	3	2	2	2	2	2	2	2
24	Caída del sistema por sobrecarga	3	2	2	3	0	0	3	3	3	3	3	3	3	2	2	2	3	2	2	2	3	0	1	1	1	1	1
25	Denegación de servicio	1	1	1	1	0	0	1	1	1	1	1	1	1	1	1	0	1	1	1	1	0	0	1	1	1	1	1
26	Robo	0	0	0	1	0	0	0	0	0	0	0	2	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
27	Ataques destructivos	1	1	1	2	0	0	1	1	1	1	1	2	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0
28	Extorsión	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
29	Ingeniería social	2	2	1	2	0	0	1	1	1	1	0	2	2	0	0	0	2	0	0	0	0	0	2	0	0	0	0
30	Manipulación de logs	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

	ACTIVO	SERVICIOS				DATOS E INFORMACIÓN		APLICACIONES				EQUIPOS INFORMÁTICO			REDES DE COMUNICACIONES				SOPORTE DE INFORMACIÓN			EQUIPO AUXILIAR			INSTALACIONES			PERSONAL
N°	AMENAZA	S1	S2	S3	S4	D2	D3	SW2	SW3	SW6	SW10	HW1	HW2	HW4	COM1	COM2	COM4	COM6	SI1	SI2	SI4	AUX1	AUX4	AUX5	L1	L2	L3	P1
31	Abuso de privilegios de acceso	1	1	1	3	2	2	2	2	2	2	0	3	1	0	0	0	0	0	0	0	0	0	2	0	0	0	0
32	Manipulación de equipos	1	1	1	3	0	0	1	1	1	1	1	3	2	1	1	1	1	0	0	0	0	0	3	1	1	1	1
33	Manipulación de configuración	2	2	2	3	0	0	2	2	1	1	2	2	2	2	2	2	2	1	1	1	0	0	2	1	1	1	1
34	Alteración de la información	2	2	1	3	1	1	2	2	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Fuente: El autor, en base a Metodología MAGERIT

Para la valoración de la probabilidad, Magerit establece que se debe utilizar la siguiente escala ocurrencia: 0 nunca; 1 año; 2 mes y 3 semana

3.5. Estimación e impacto

Una vez obtenida la matriz de probabilidad se procede a valorar el impacto

Tabla 14 *Matriz de impacto*

ACTIVO		SERVICIOS				DATOS		APLICACIONES				EQUIPOS INFORMÁTICOS			REDES DE COMUNICACIONES				SOPORTE DE INFORMACIÓN			EQUIPAMIENTO AUXILIAR			INSTALACIONES			PERSONAL
N°	AMENAZA	S1	S2	S3	S4	D2	D3	SW2	SW3	SW6	SW10	HW1	HW2	HW4	COM1	COM2	COM4	COM6	SI1	SI2	SI4	AUX1	AUX4	AUX5	L1	L2	L3	P1
1	Fuego	0	0	0	1	0	0	0	0	0	0	3	1	0	0	3	3	1	0	0	0	1	3	2	1	1	3	1
2	Daños por agua	0	0	0	1	0	0	0	0	0	0	3	1	0	0	3	3	1	0	0	0	1	3	2	1	1	3	1
3	Desastres naturales	0	0	0	1	0	0	0	0	0	0	3	1	0	0	3	3	1	0	0	0	1	3	2	1	1	3	1
4	Corte del suministro eléctrico	1	1	1	1	1	1	1	1	1	1	0	1	1	0	0	0	1	0	0	0	0	0	2	1	1	0	1
5	Condiciones inadecuadas de temperatura o humedad	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	0	0	0	0	1	1	1	1	0	0
6	Fallo de servicios de comunicaciones	1	1	1	1	1	1	1	1	1	1	3	1	1	3	3	3	3	0	0	0	0	0	0	1	3	3	1
7	Desastres industriales	0	0	0	1	1	1	0	0	0	0	0	1	1	0	0	0	1	0	0	0	1	3	0	0	0	0	1

ACTIVO		SERVICIOS				DATOS		APLICACIONES				EQUIPOS INFORMÁTICOS			REDES DE COMUNICACIONES				SOPORTE DE INFORMACIÓN			EQUIPAMIENTO AUXILIAR			INSTALACIONES			PERSONAL
N°	AMENAZA	S1	S2	S3	S4	D2	D3	SW2	SW3	SW6	SW10	HW1	HW2	HW4	COM1	COM2	COM4	COM6	SI1	SI2	SI4	AUX1	AUX4	AUX5	L1	L2	L3	P1
8	Fuga de información	0	1	1	0	2	1	2	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	Introducción de falsa información	0	0	1	0	0	0	1	0	1	1	1	0	1	0	0	0	0	1	1	1	0	0	1	0	0	0	0
10	Acceso no autorizado	2	2	2	2	2	2	3	3	3	3	3	2	1	1	1	1	1	2	2	2	0	0	2	0	0	3	0
11	Vulnerabilidad de programas (software)	2	0	0	1	0	1	1	1	1	1	1	2	1	1	1	3	0	0	0	0	0	0	1	0	0	0	0
12	Corrupción de la información	0	0	0	1	1	1	1	1	1	1	1	1	0	0	0	1	0	1	1	1	0	0	0	1	1	1	1
13	Destrucción de información	1	1	3	1	3	3	2	1	2	2	2	1	1	0	0	1	0	2	2	2	0	0	0	1	1	1	1
14	Interceptación de información (escucha)	0	0	1	0	2	2	1	1	1	1	1	1	0	0	0	0	0	1	1	1	0	0	0	1	1	2	1
15	Indisponibilidad del personal	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
16	Agotamiento de recursos	2	1	1	0	0	0	3	3	1	1	3	1	1	1	1	1	1	1	1	1	0	1	1	0	0	3	0
17	Errores de los usuarios	2	0	1	1	1	1	2	2	2	2	2	1	0	2	3	3	1	1	1	1	0	0	1	1	1	2	1
18	Errores del administrador	2	0	1	1	0	0	2	2	2	2	3	1	0	2	3	3	1	1	1	1	0	0	1	1	1	2	1

ACTIVO		SERVICIOS				DATOS		APLICACIONES				EQUIPOS INFORMÁTICOS			REDES DE COMUNICACIONES				SOPORTE DE INFORMACIÓN			EQUIPAMIENTO AUXILIAR			INSTALACIONES			PERSONAL
N°	AMENAZA	S1	S2	S3	S4	D2	D3	SW2	SW3	SW6	SW10	HW1	HW2	HW4	COM1	COM2	COM4	COM6	SI1	SI2	SI4	AUX1	AUX4	AUX5	L1	L2	L3	P1
19	Errores de configuración	2	1	1	1	0	0	2	2	2	2	3	1	0	2	3	3	1	1	1	1	0	0	1	1	1	2	1
20	Degradación de los soportes de almacenamiento de la información	0	1	1	0	0	0	3	3	1	1	3	0	1	0	0	1	0	2	2	2	0	1	1	0	0	3	0
21	Difusión de software dañino	3	2	2	1	0	0	2	2	2	2	2	1	1	1	1	1	0	1	1	1	0	0	1	0	0	1	0
22	Errores de mantenimiento / actualización de programas (software)	3	3	3	1	0	0	1	1	1	1	1	1	1	2	2	3	0	1	1	1	0	1	2	0	2	2	0
23	Errores de mantenimiento / actualización de equipos (hardware)	3	3	3	1	0	0	1	1	1	1	1	1	1	2	2	3	0	1	1	1	0	1	2	0	2	2	0
24	Caída del sistema por sobrecarga	2	1	1	0	0	0	3	3	1	1	3	1	1	1	1	1	1	1	1	1	0	1	1	0	0	3	0
25	Denegación de servicio	2	2	2	1	0	0	3	2	1	1	2	1	1	2	3	2	2	0	0	0	0	0	0	0	0	3	0
26	Robo	0	0	0	1	0	0	0	0	0	0	3	1	0	3	3	3	1	2	2	2	0	2	1	0	3	3	0
27	Ataques destructivos	0	0	0	1	0	0	0	0	0	0	3	1	0	3	3	3	1	2	2	2	1	2	1	0	3	3	0
28	Extorsión	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2
29	Ingeniería social	1	1	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2
30	Manipulación de logs	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
31	Abuso de privilegios de acceso	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
32	Manipulación de equipos	1	0	0	1	0	0	0	0	0	0	3	1	1	3	3	3	2	0	0	0	1	3	1	0	0	3	0
33	Manipulación de configuración	2	1	1	1	0	0	2	2	2	2	3	1	0	2	3	3	1	1	1	1	0	0	1	1	1	2	1
34	Alteración de la información	2	1	1	1	0	0	2	2	2	2	3	1	0	2	3	3	1	1	1	1	0	0	1	1	1	2	1

Fuente: El autor, en base a la Metodología MAGERIT

Para la estimación del impacto, Magerit menciona que se debe utilizar la siguiente escala para calificar de la siguiente forma: 0 no hay consecuencias; 1 no hay consecuencias relevantes; 2 consecuencias relevantes y 3 hay consecuencias graves

3.6.Valoración del Riesgo

Tabla 15 *Matriz Riesgo en función del impacto y la probabilidad*

	ACTIVO	SERVICIOS				DATOS		APLICACIONES				EQUIPOS INFORMÁTICOS			REDES DE COMUNICACIONES				SOPORTE DE INFORMACIÓN			EQUIPAMIENTO AUXILIAR			INSTALACIONES			PERSONAL
N°	AMENAZA	S1	S2	S3	S4	D2	D3	SW2	SW3	SW6	SW10	HW1	HW2	HW4	COM1	COM2	COM4	COM6	SI1	SI2	SI4	AUX1	AUX4	AUX5	L1	L2	L3	P1
1	Fuego	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0
2	Daños por agua	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	Desastres naturales	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	3	0	0	0	0	0
4	Corte del suministro eléctrico	1	1	1	1	1	1	1	1	1	1	0	1	1	0	0	0	1	0	0	0	0	0	2	1	1	0	1
5	Condiciones inadecuadas de temperatura o humedad	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	3	0	0	0	0	1	1	1	1	0	0
6	Fallo de servicios de comunicaciones	2	2	2	2	2	2	2	2	2	2	6	2	2	6	6	6	6	0	0	0	0	0	0	2	6	6	2
7	Desastres industriales	0	0	0	1	1	1	0	0	0	0	0	1	1	0	0	0	1	0	0	0	1	3	0	0	0	0	1
8	Fuga de información	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

	ACTIVO	SERVICIOS				DATOS		APLICACIONES				EQUIPOS INFORMÁTICOS			REDES DE COMUNICACIONES				SOPORTE DE INFORMACIÓN			EQUIPAMIENTO AUXILIAR			INSTALACIONES			PERSONAL
N°	AMENAZA	S1	S2	S3	S4	D2	D3	SW2	SW3	SW6	SW10	HW1	HW2	HW4	COM1	COM2	COM4	COM6	SI1	SI2	SI4	AUX1	AUX4	AUX5	L1	L2	L3	P1
9	Introducción de falsa información	0	0	1	0	0	0	1	0	1	1	1	0	1	0	0	0	0	1	1	1	0	0	1	0	0	0	0
10	Acceso no autorizado	2	2	2	4	4	4	3	3	3	3	3	6	2	0	0	0	0	0	0	0	0	0	4	0	0	0	0
11	Vulnerabilidad de programas (software)	2	0	0	3	0	1	1	1	1	1	1	6	1	1	1	0	0	0	0	0	0	0	1	0	0	0	0
12	Corrupción de la información	0	0	0	3	1	1	0	0	0	0	0	3	0	0	0	0	0	1	1	1	0	0	0	1	1	1	1
13	Destrucción de información	1	1	3	2	3	3	2	1	2	2	0	3	1	0	0	0	0	0	0	0	0	0	0	1	1	1	1
14	Interceptación de información (escucha)	0	0	1	0	4	4	1	1	1	1	1	3	0	0	0	0	0	1	1	1	0	0	0	1	1	2	1
15	Indisponibilidad del personal	2	2	2	3	2	2	3	3	3	3	1	3	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0
16	Agotamiento de recursos	2	1	1	0	0	0	3	3	1	1	3	3	3	1	1	0	1	3	3	3	0	0	1	0	0	6	0
17	Errores de los usuarios	4	0	1	3	3	3	4	4	4	4	6	3	0	2	3	3	2	0	0	0	0	0	2	2	2	4	2
18	Errores del administrador	4	0	1	2	0	0	4	4	4	4	6	2	0	4	6	6	2	1	1	1	0	0	2	1	1	2	1
19	Errores de configuración	2	1	1	3	0	0	6	4	4	4	6	2	0	4	6	6	2	1	1	1	0	0	2	1	1	2	0
20	Degradación de los soportes de	0	3	2	0	0	0	9	9	2	2	6	0	2	0	0	1	0	4	4	4	0	0	2	0	0	6	0

	ACTIVO	SERVICIOS				DATOS		APLICACIONES				EQUIPOS INFORMÁTICOS			REDES DE COMUNICACIONES				SOPORTE DE INFORMACIÓN			EQUIPAMIENTO AUXILIAR			INSTALACIONES			PERSONAL
N°	AMENAZA	S1	S2	S3	S4	D2	D3	SW2	SW3	SW6	SW10	HW1	HW2	HW4	COM1	COM2	COM4	COM6	SI1	SI2	SI4	AUX1	AUX4	AUX5	L1	L2	L3	P1
	almacenamiento de la información																											
21	Difusión de software dañino	9	6	4	3	0	0	4	4	4	4	2	3	3	1	1	1	0	1	1	1	0	0	1	0	0	2	0
22	Errores de mantenimiento / actualización de programas (software)	9	9	6	3	0	0	2	2	2	2	2	3	3	4	4	6	0	2	2	2	0	0	4	0	4	4	0
23	Errores de mantenimiento / actualización de equipos (hardware)	9	9	9	3	0	0	2	2	2	2	1	3	1	2	2	3	0	1	3	3	0	2	4	0	4	4	0
24	Caída del sistema por sobrecarga	6	2	2	0	0	0	9	9	3	3	9	3	3	2	2	2	3	2	2	2	0	0	1	0	0	3	0
25	Denegación de servicio	2	2	2	1	0	0	3	2	1	1	2	1	1	2	3	0	2	0	0	0	0	0	0	0	0	3	0
26	Robo	0	0	0	1	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
27	Ataques destructivos	0	0	0	2	0	0	0	0	0	0	3	2	0	3	3	3	1	0	0	0	0	0	0	0	0	0	0
28	Extorsión	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
29	Ingeniería social	2	2	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
30	Manipulación de logs	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

	ACTIVO	SERVICIOS				DATOS		APLICACIONES				EQUIPOS INFORMÁTICOS			REDES DE COMUNICACIONES				SOPORTE DE INFORMACIÓN			EQUIPAMIENTO AUXILIAR			INSTALACIONES			PERSONAL
N°	AMENAZA	S1	S2	S3	S4	D2	D3	SW2	SW3	SW6	SW10	HW1	HW2	HW4	COM1	COM2	COM4	COM6	SI1	SI2	SI4	AUX1	AUX4	AUX5	L1	L2	L3	P1
31	Abuso de privilegios de acceso	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
32	Manipulación de equipos	1	0	0	3	0	0	0	0	0	0	3	3	2	3	3	3	2	0	0	0	0	0	3	0	0	3	0
33	Manipulación de configuración	4	2	2	3	0	0	4	4	2	2	6	2	0	4	6	6	2	1	1	1	0	0	2	1	1	2	1
34	Alteración de la información	4	2	1	3	0	0	4	4	2	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Fuente: El autor, en base a la Metodología MAGERIT

3.7. Resumen de amenazas encontradas en los activos

Tabla 16 *Resumen de amenazas de atención inmediata para la institución.*

	ACTIVO	SERVICIOS				DATOS		APLICACIONES				EQUIPOS INFORMÁTICOS			REDES DE COMUNICACIONES				SOPORTE DE INFORMACIÓN			EQUIPAMIENTO AUXILIAR			INSTALACIONES			PERSONAL
N°	AMENAZA	S1	S2	S3	S4	D2	D3	SW2	SW3	SW6	SW10	HW1	HW2	HW4	COM1	COM2	COM4	COM6	SI1	SI2	SI4	AUX1	AUX4	AUX5	L1	L2	L3	P1
1	Fuego																											
2	Daños por agua																											
3	Desastres naturales																											
4	Corte del suministro eléctrico																											
5	Condiciones inadecuadas de temperatura o humedad																											
6	Fallo de servicios de comunicaciones											6			6	6	6	6								6	6	
7	Desastres industriales																											
8	Fuga de información																											
9	Introducción de falsa información																											
10	Acceso no autorizado												6															
11	Vulnerabilidad de programas (software)												6															
12	Corrupción de la información																											

	ACTIVO	SERVICIOS				DATOS		APLICACIONES				EQUIPOS INFORMÁTICOS			REDES DE COMUNICACIONES				SOPORTE DE INFORMACIÓN			EQUIPAMIENTO AUXILIAR			INSTALACIONES			PERSONAL
N°	AMENAZA	S1	S2	S3	S4	D2	D3	SW2	SW3	SW6	SW10	HW1	HW2	HW4	COM1	COM2	COM4	COM6	SI1	SI2	SI4	AUX1	AUX4	AUX5	L1	L2	L3	P1
13	Destrucción de información																											
14	Interceptación de información (escucha)																											
15	Indisponibilidad del personal																											
16	Agotamiento de recursos																										6	
17	Errores de los usuarios											6																
18	Errores del administrador											6				6	6											
19	Errores de configuración							6				6				6	6											
20	Degradación de los soportes de almacenamiento de la información							9	9			6															6	
21	Difusión de software dañino	9	6																									
22	Errores de mantenimiento / actualización de programas (software)	9	9	6													6											

	ACTIVO	SERVICIOS				DATOS		APLICACIONES				EQUIPOS INFORMÁTICOS			REDES DE COMUNICACIONES				SOPORTE DE INFORMACIÓN			EQUIPAMIENTO AUXILIAR			INSTALACIONES			PERSONAL
N°	AMENAZA	S1	S2	S3	S4	D2	D3	SW2	SW3	SW6	SW10	HW1	HW2	HW4	COM1	COM2	COM4	COM6	SI1	SI2	SI4	AUX1	AUX4	AUX5	L1	L2	L3	P1
23	Errores de mantenimiento / actualización de equipos (hardware)	9	9	9																								
24	Caída del sistema por sobrecarga	6						9	9			9																
25	Denegación de servicio																											
26	Robo																											
27	Ataques destructivos																											
28	Extorsión																											
29	Ingeniería social																											
30	Manipulación de logs																											
31	Abuso de privilegios de acceso																											
32	Manipulación de equipos																											
33	Manipulación de configuración											6				6	6											
34	Alteración de la información																											
		4	**3**	**2**	**0**	**0**	**0**	**3**	**2**	**0**	**0**	**7**	**2**	**0**	**1**	**4**	**5**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**3**	**0**

Fuente: El autor, en base a la Metodología MAGERIT

La tabla 16 muestra en resumen las amenazas de los activos críticos de la UCE o las que presentan el riesgo más alto el mismo que deben ser atendido de forma inmediata con la aplicación de los controles de la norma ISO/IEC 27002:2013 por parte de la Dirección de Tecnologías de la Información y Comunicación y los centros de datos de tecnologías en las diferentes facultades de la institución con el personal técnico encargado.

3.8. Mapa de riesgos

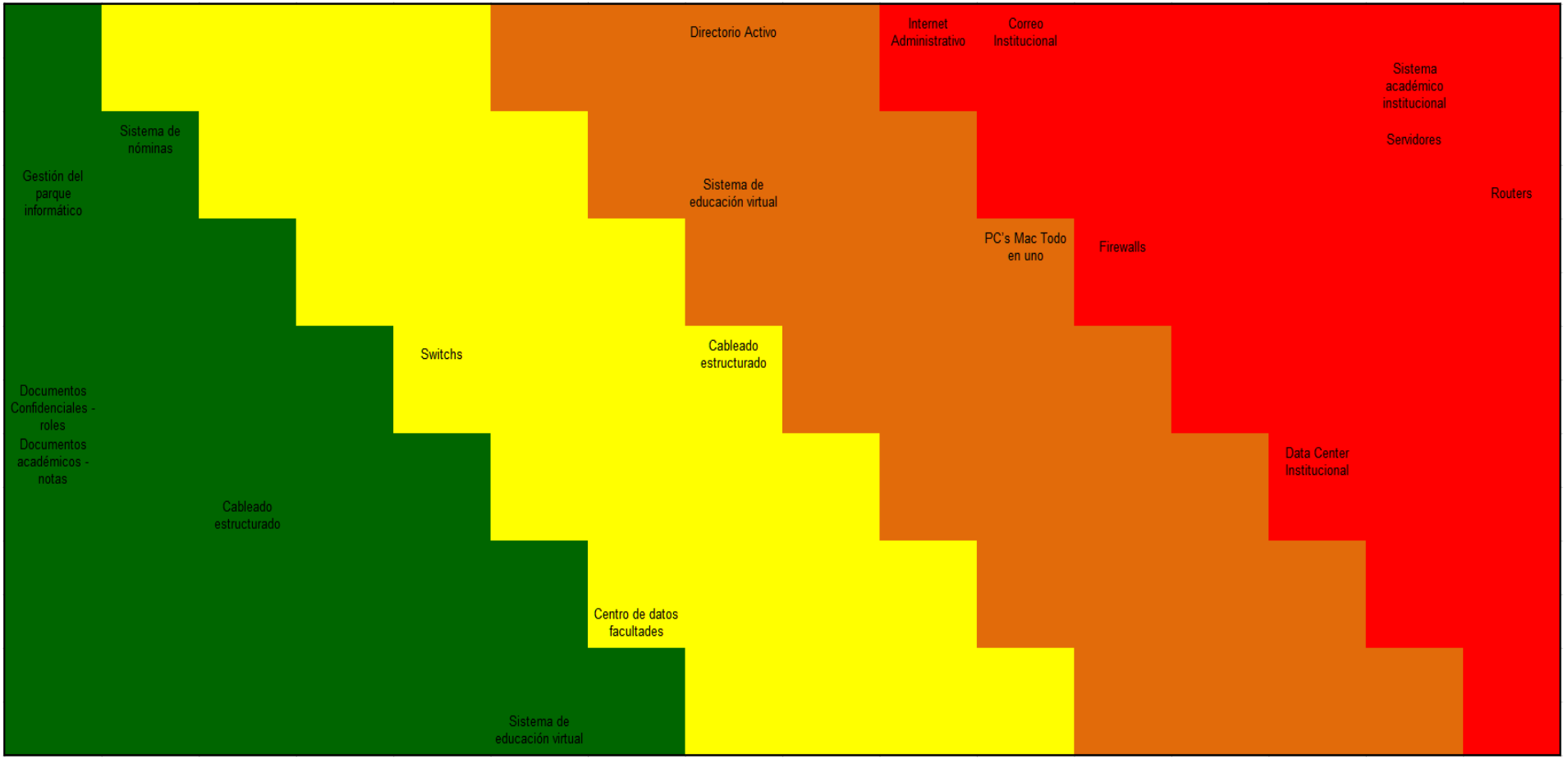


Figura 5: Mapa de riesgos
Fuente: El autor, en base a la Metodología MAGERIT

3.9. Selección de salvaguardas o contramedidas.

Luego de obtener la valoración de los riesgos encontrados en los activos tecnológicos de la Universidad Central, según la metodología Magerit se procede a la selección de salvaguardas o contramedidas mediante la determinación de los controles establecidos en la norma ISO/IEC 27002:2013

Tabla 17 *Determinación de controles según norma ISO/IEC 27002:2013*

Activo	Amenaza	Vulnerabilidad	Control ISO/IEC 27002:2013
Internet Administrativo	Difusión de software dañino	Falta de controles contra código malicioso	12.2.1
	Errores de mantenimiento / actualización de programas (software)	No se actualizan periódicamente los programas	11.2.4
	Errores de mantenimiento / actualización de equipos (hardware)	Falla en el cumplimiento de mantenimiento de equipos	11.2.4
	Caída del sistema por sobrecarga	Falta de provisión de capacidades	12.1.3
Correo Institucional	Difusión de software dañino	Falta de controles contra código malicioso	12.2.1
	Errores de mantenimiento / actualización de programas (software)	No se actualizan periódicamente los programas	11.2.4

Activo	Amenaza	Vulnerabilidad	Control ISO/IEC 27002:2013
	Errores de mantenimiento / actualización de equipos (hardware)	Falla en el cumplimiento de mantenimiento de equipos	11.2.4
Directorio Activo	Errores de mantenimiento / actualización de programas (software)	No se actualizan periódicamente los programas	11.2.4
	Errores de mantenimiento / actualización de equipos (hardware)	Falla en el cumplimiento de mantenimiento de equipos	11.2.4
Sistema Académico	Errores de configuración	Falta de concienciación y capacitación	7.2.2
	Degradación de los soportes de almacenamiento de la información	Falta de gestión de soportes extraíbles	8.3.1
	Caída del sistema por sobrecarga	Falta de provisión de capacidades	12.1.3
Sistema Educación Virtual	Degradación de los soportes de almacenamiento de la información	Falta de gestión de soportes extraíbles	8.3.1
	Caída del sistema por sobrecarga	Falta de provisión de capacidades	12.1.3
Servidores	Fallo de servicios de comunicaciones	Falta de redundancias en la red	17.2.1

Activo	Amenaza	Vulnerabilidad	Control ISO/IEC 27002:2013
	Errores de los usuarios	Falta de procedimientos documentados	12.1.1
	Errores del administrador	Falta de registros de actividad del administrador	12.4.3
	Errores de configuración	Falta de concienciación y capacitación	7.2.2
	Degradación de los soportes de almacenamiento de la información	Falta de gestión de soportes extraíbles	8.3.1
	Caída del sistema por sobrecarga	Falta de provisión de capacidades	12.1.3
	Manipulación de configuración	Falla en la política de control de acceso	9.1.1
Pc´s Mac Todo en uno	Vulnerabilidad de programas (software)	Falta de restricción en la instalación de programas	12.6.2
	Corrupción de la información	Falta de respaldos apropiados	12.3.1
	Errores del administrador	Falta de registros de actividad del administrador	12.4.3
	Errores de configuración	Falta de concienciación y capacitación	7.2.2

Activo	Amenaza	Vulnerabilidad	Control ISO/IEC 27002:2013
	Errores de mantenimiento / actualización de programas (software)	No se actualizan periódicamente los programas	11.2.4
	Manipulación de configuración	Falla en la política de control de acceso	9.1.1
Switchs	Fallo de servicios de comunicaciones	Falta de redundancias en la red	17.2.1
Routers	Fallo de servicios de comunicaciones	Falta de redundancias en la red	17.2.1
	Errores del administrador	Falta de registros de actividad del administrador	12.4.3
	Errores de configuración	Falta de concienciación y capacitación	7.2.2
	Errores de mantenimiento / actualización de programas (software)	No se actualizan periódicamente los programas	11.2.4
	Manipulación de configuración	Falla en la política de control de acceso	9.1.1
Firewall	Fallo de servicios de comunicaciones	Falta de redundancias en la red	17.2.1

Activo	Amenaza	Vulnerabilidad	Control ISO/IEC 27002:2013
	Errores del administrador	Falta de registros de actividad del administrador	12.4.3
	Errores de configuración	Falta de concienciación y capacitación	7.2.2
	Errores de mantenimiento / actualización de programas (software)	No se actualizan periódicamente los programas	11.2.4
	Manipulación de configuración	Falla en la política de control de acceso	9.1.1
Cableado Estructurado	Fallo de servicios de comunicaciones	Falta de redundancias en la red	17.2.1
Centro de datos Facultades	Fallo de servicios de comunicaciones	Falta de redundancias en la red	17.2.1
Data Center	Fallo de servicios de comunicaciones	Falta de redundancias en la red	17.2.1
	Agotamiento de recursos	Falla por carga desmesurada	12.1.3
	Degradación de los soportes de almacenamiento de la información	Falta de gestión de soportes extraíbles	8.3.1

Elaborado por el autor de la investigación en base a la norma ISO/IEC 27002:2013

3.9.1. Comparación con la política de seguridad ISO 27000 y COBIT 5

En la Universidad Central del Ecuador existente una política de seguridad elaborada en el año 2015, bajo los controles del estándar ISO/IEC 27000 y COBIT 5 la cual se orienta a las recomendaciones y responsabilidades de las mejores prácticas para la seguridad de la información.

La política existente es actualizada con la nueva, la que se basa en los controles de la norma ISO/IEC 27002:2013 entre los que se destaca nuevas directrices para la criptografía, la seguridad de las comunicaciones y lo que tiene relación con proveedores, entre otras.

Para la implementación de la política de seguridad se debe tomar en cuenta los controles con énfasis en la gestión de activos, el desarrollo de software seguro, pruebas de seguridad de los sistemas, profundizar la evaluación de eventos de seguridad, la planificación, implementación de la continuidad del negocio y el uso o implementación de instalaciones redundantes de infraestructura.

CAPÍTULO IV

PROPUESTA DE LA POLÍTICA DE SEGURIDAD PARA LA INFRAESTRUCTURA DE RED DE LA UNIVERSIDAD CENTRAL DEL ECUADOR

4.1. INTRODUCCIÓN

Luego el análisis realizado conjuntamente con la Dirección de Tecnologías de los principales riesgos a los que se encuentra expuesta la institución, se seleccionó los controles a aplicarse según la norma ISO/ICE 27002:2013 y se presenta la siguiente Política de Seguridad para la infraestructura de red de la Universidad Central del Ecuador.

4.2. OBJETIVO

La presente política de seguridad para la infraestructura de red de la Universidad Central del Ecuador basada en la ISO / IEC 27002:2013 establece los controles de seguridad para salvaguardar los activos tecnológicos y disminuir el riesgo.

4.3. ALCANCE

En este documento se establece las directrices para garantizar la seguridad de información de la institución mediante la aplicación de controles para proteger la confidencialidad, integridad y disponibilidad de la información.

4.4. REFERENCIAS NORMATIVAS

La presente política se basa en la norma internacional ISO/IEC 27002:2013, ésta proporciona pautas, controles para establecer estándares de seguridad y poder minimizar los riesgos encontrados en la infraestructura de la Universidad Central del Ecuador.

4.5. TÉRMINOS Y DEFINICIONES

En la política de seguridad se presentan los siguientes términos y definiciones

- **Seguridad de la Información**

  Conjunto de técnicas y medidas que se utilizan para proteger la información dentro de la institución y que el acceso o modificación sea realizada solo por personal autorizado con la finalidad de asegurar la continuidad de los procesos (Excellence, 2018).

INCIBE (2015), define los siguientes términos:

- **Confidencialidad**

  La confidencialidad implica que la información es accesible únicamente por el personal autorizado, es lo que se conoce como *need-to-know*., con este término se hace referencia a que la información solo debe ponerse en conocimiento de las personas, entidades o sistemas autorizados para su acceso.

- **Integridad**

  Considera que la información debe ser correcta, libre de destrucción o modificación inadecuada y errores e incluye asegurar el no repudio y autenticidad de la información.

- **Disponibilidad**

  La disponibilidad de la información estará siempre accesible para cuando sea necesaria de una forma adecuada y segura.

- **Vulnerabilidad**

INCIBE (2017), señala una debilidad o fallo en un sistema o en las medidas de seguridad implementadas que pone en riesgo la seguridad de la información permitiendo que un atacante pueda comprometer la integridad, confidencialidad y disponibilidad de la misma.

- **Amenaza**

Es la afectación probable que puede sufrir un activo dentro de una infraestructura a causa de eventos naturales o eventos provocados, es decir se puede sufrir efectos negativos sobre algún elemento de los sistemas (INCIBE, 2017).

- **Riesgo**

El riesgo es la probabilidad de que una amenaza se materialice produciendo un incidente de seguridad aprovechándose de una vulnerabilidad, causando pérdida de información o daños en los activos.

- **Incidente de seguridad**

Es la inminente amenaza de violación de una política de seguridad con afectaciones negativas en las que se pueden comprometer uno o varios activos de la institución.

4.6. ABREVIATURAS

- UCE: Universidad Central del Ecuador
- DTIC: Dirección de Tecnologías de la Información y Comunicación
- ISO: Organización Internacional de Normalización
- IEC: *International Electrotechnical Commission*

- TI: Tecnologías de la Información
- LOSEP: Ley Orgánica del Servicio Público

4.7. RESPONSABILIDADES

Dentro del Estatuto Universitario, aprobado en octubre 2019, se establecen funciones y responsabilidades del Director como de la Dirección de Tecnologías de la Información y Comunicación de la Universidad Central en donde establece que se deben optimizar los procesos académicos de investigación, administrativos institucionales en que se deben desarrollar, implementar y administrar las políticas y lineamientos referentes a las tecnologías de información y comunicación en coordinación con los diferentes áreas del DTC y los centros de datos de las diferentes Facultades que conforman la UCE.

Tabla 18 *Dignidades y responsabilidades involucrados*

DIGNIDAD	RESPONSABILIDAD
Rector de la UCE o su delegado	Aprobación de la presente política de seguridad
Director de Tecnologías	Tramitar la aprobación de esta política Aplicación y difusión de la política
Áreas de DTIC - UCE	Implantar los controles que conforman esta política Monitorear la correcta aplicación de la política
Centro de datos Facultades	Cumplir y hacer cumplir lo descrito en la presente política de seguridad
Funcionarios UCE	Conocer, aplicar y concienciar está política

Elaborado por el autor de la investigación

4.8. DESARROLLO DE LA POLÍTICA

Luego del análisis de riesgos se describen los principales elementos que conforman esta política de seguridad, la misma cuenta únicamente con los activos más críticos en donde se encontraron amenazas y vulnerabilidades.

4.8.1. Directrices de la Dirección de Tecnologías

Área:	**Políticas de seguridad de la información**
Objetivo:	Garantizar que la DTIC de la Universidad Central del Ecuador, cuente con una política de seguridad actualizada, con estándares internacionales.
Control:	ISO/IEC 27002: 5, 5.1 Directrices de la Dirección de Tecnologías de la Información

Artículo 1. La Dirección de Tecnologías de la Información y Comunicación de la Universidad Central del Ecuador se encargará de gestionar la aprobación de la presente política ante la máxima autoridad, la cual complementa métodos y políticas desarrolladas anteriormente.

Artículo 2. La DTIC se encargará de solicitar la creación y aprobación ante la máxima autoridad del Comité de Seguridad de la Información de la Universidad Central del Ecuador.

Artículo 3. La DTIC es quien se encarga de la revisión, actualización o modificación documentada de esta política basada en la Norma ISO/ICE 27002:2013 con una periodicidad de al menos dos semestres académicos (un año) a través del Comité de Seguridad de la Información de la UCE

Artículo 4. La DTIC deberá promover la difusión de esta política dentro de la UCE con todos los funcionarios universitarios para su aplicación e implantación de procesos para su concienciación.

Área:	**Seguridad ligada a los recursos humanos**
Objetivo:	Garantizar que los funcionarios de los tres estamentos universitarios conozcan la implementación de la política y la apliquen conscientemente.
Control:	ISO/IEC 27002: 7.2.2. Concienciación Educación y Capacitación en Seguridad de la Información.

Artículo 5. Los funcionarios universitarios deberán ser informados de las normas y procedimientos a tener en cuenta en sus puestos de trabajo de acuerdo a sus funciones para salvaguardar la seguridad de la información.

Artículo 6. En la DTIC, así como en las diferentes facultades se gestionará el presupuesto para la capacitación en temas de seguridad tecnológica para los funcionarios universitarios de la UCE, tanto para el personal técnico y no técnico.

Artículo 7. La UCE apoyará a la DTIC y a las facultades en la elaboración del plan anual de capacitación sobre el uso de infraestructura tecnológica, las responsabilidades legales y el uso adecuado de los servicios de información.

Artículo 8. Los funcionarios universitarios están en la obligación de cumplir con lo descrito en esta política de seguridad en relación a las actividades inherentes a sus funciones.

Artículo 9. La DTIC deberá implementar capacitaciones especializadas para el personal técnico de la UCE relacionado con la seguridad de la información, este personal

son los administradores de la infraestructura tecnológica tales como: aplicaciones, equipos informáticos y redes de comunicación, soportes de información y equipamiento auxiliar.

Artículo 10. La DTIC debe fortalecer los canales de comunicación con el personal técnico de la UCE, para poder solventar con mayor eficiencia los posibles eventos de seguridad que puedan producir.

Área:	**Gestión de activos**
Objetivo:	Resguardar la información de la universidad considerada confidencial o sensible, mediante el uso efectivo de soportes extraíbles.
Control:	ISO/IEC 27002: 8.3.1. Gestión de soportes extraíbles.

Artículo 11. La DTIC, así como los centros de datos de facultades deberán gestionar la adquisición de soportes extraíbles para respaldo de la información que se encuentre en los equipos de las diferentes facultades y/o dependencias.

Artículo 12. Es obligación del usuario analizar con el antivirus proporcionado por la UCE los medios extraíbles, para evitar la pérdida de información.

Artículo 13. Es responsabilidad del funcionario universitario el salvaguardar la información almacenada en medios extraíbles tales como: discos duros o memorias USB en lugares física y ambientalmente apropiados.

Artículo 14. La DTIC y el personal técnico de los centros de datos de facultades, utilizarán técnicas criptográficas para la protección de los medios extraíbles asignados que contengan información sensible y/o confidencial o aquellos asignados a las máximas autoridades.

Área:	**Control de acceso**
Objetivo:	Mejorar los controles de acceso a los diferentes activos de la infraestructura tecnológica de la UCE.
Control:	ISO/IEC 27002: 9.1.1. Política de Control de acceso

Artículo 15. La Dirección de Tecnologías establecerá nuevas directrices para la entrega de credenciales a los funcionarios universitarios para el acceso a los diferentes activos que conforma la infraestructura tecnológica de la UCE.

Artículo 16. Las credenciales de los funcionarios universitarios deberán ser definidas de acuerdo a su función; y, así establecer los perfiles de usuario y roles, para evitar los accesos no autorizados.

Artículo 17. Las credenciales otorgadas deberán ser revisadas al menos cada período académico en coordinación con la Dirección de Talento Humano, con la finalidad de identificar y actualizar los perfiles de los funcionarios o notificar de manera inmediata para el retiro de las mismas si es que el funcionario cesó en sus funciones en la UCE.

Artículo 18. Para garantizar la seguridad de la información, se deberá aplicar la regla de menor privilegio conocida también como menor autoridad para el acceso a las diferentes aplicaciones universitarias.

Artículo 19. Para el acceso a la administración de la infraestructura tecnológica se otorgará acceso con privilegio especial únicamente a aquellos funcionarios universitarios que cumplan estas funciones, debidamente autorizadas con un documento formal, a través de la Dirección del DTIC – UCE.

Artículo 20. La DTIC informará a todos los funcionarios universitarios que las credenciales son: confidenciales, individuales e intransferibles en ninguna circunstancia.

Artículo 21. Para el acceso a los diferentes activos de infraestructura universitaria se deberá utilizar contraseñas seguras, las que deben cumplir con requisitos mínimos tales como:

- La longitud debe ser de al menos 8 (ocho) caracteres y un máximo de 16 (dieciséis).
- Contener al menos una letra mayúscula, letras minúsculas y números.
- La vigencia de la contraseña no debe ser mayor a 90 días o el usuario podrá realizar el cambio cuando lo requiera.
- No deberán incluir el *nick* de usuario, fecha de nacimiento, ni otra información personal del funcionario que sea fácil de descifrar.

Artículo 22. De forma obligatoria, los funcionarios: docentes, administrativos y estudiantes deben cambiar la contraseña asignada temporalmente en su primer acceso a las plataformas universitarias.

Artículo 23. Se deberá generar credenciales especiales para los usuarios que requieran conexiones externas para asegurar el acceso a la información que se realice por redes privadas virtuales (VPN) o servicios de acceso remoto (SAR) las que siempre deberán ser implementadas con técnicas de encriptación.

Área:	**Seguridad de los equipos**
Objetivo:	Asegurar el óptimo funcionamiento de los activos que conforman infraestructura tecnológica de la UCE.
Control:	ISO/IEC 27002: 11.2.4. Mantenimiento de los equipos

Artículo 24. En cumplimiento a la Norma 410 Tecnologías de la Información de la Contraloría General del Estado, tanto la DTIC como los centros de datos de facultades y/o dependencias deberán presentar a la autoridad competente el plan de mantenimiento preventivo anual de los activos de la infraestructura tecnológica a su cargo.

Artículo 25. Enviar con anticipación el cronograma aprobado por las autoridades de los centros de datos de facultades y/o dependencias la programación de mantenimiento preventivo de los equipos a todos los estamentos universitarios, con la finalidad de evitar contratiempos tanto para el personal técnico autorizado que lo realiza como para los usuarios finales.

Artículo 26. El plan de mantenimiento de los activos se regirá a las recomendaciones del fabricante o proveedor de acuerdo a las especificaciones técnicas de cada activo que conforma la infraestructura tecnológica de la UCE.

Artículo 27. De forma obligatoria la DTIC, así como los centros de datos de facultades solicitarán y dará seguimiento el presupuesto para la contratación de mantenimiento para determinados activos parte de la infraestructura tecnológica en el Plan Anual de Adquisiciones (PAC).

Artículo 28. Tanto en la DTIC como en los centros de datos de facultades y/o unidades académicas, se encuentra autorizado para realizar el mantenimiento y reparación de equipos únicamente el personal técnico especializado.

Artículo 29. El personal técnico deberá llevar el control del mantenimiento correctivo y preventivo que se realice a los activos de la infraestructura tecnológica de la UCE, en forma física y digital.

Área:	**Seguridad en la operativa**
Objetivo:	Actualizar los manuales de uso y procedimientos establecidos
Control:	ISO/IEC 27002: 12.1; 12.2; 12.3; 12; 4 y 12.6

Documentación y procedimientos de operación

Artículo 30. La DTIC elaborará y difundirá los manuales o instructivos de usuario para la instalación, operación o guía todas las aplicaciones internas como externas con las que cuenta la UCE para garantizar su correcto funcionamiento y operatividad.

Artículo 31. La DTIC deberá mantener actualizados los manuales de usuarios de las aplicaciones universitarias de forma periódica de acuerdo a los controles de cambio que se registren.

Artículo 32. La DTIC deberá llevar el registro físico y digital de las versiones de los manuales de usuario para tener control sobre las actualizaciones que se realicen a las aplicaciones.

Gestión de Capacidades

Artículo 33. La DTIC quien administra los recursos tecnológicos de la UCE deberá realizar el monitoreo permanente de las capacidades de los principales activos de la infraestructura, (servidores, *switchs. routers, firewalls*) para garantizar la continuidad de las operaciones.

Artículo 34. La DTIC y los centros de datos de facultades analizarán la utilización y consumo de los activos de la infraestructura tecnológica con el objetivo de optimizar el desempeño de todos los servicios de TI que dispone la UCE, con la finalidad de evitar cuellos de botella o caída de los servicios.

Artículo 35. La DTIC y los centros de facultades proyectarán las necesidades de futuras demandas de capacidad para la implementación de actualizaciones o nuevo equipamiento de infraestructura tecnológica.

Protección contra código malicioso

Artículo 36. La DTIC deberá establecer las directrices al personal técnico de las diferentes áreas académicas, con la finalidad de que todos los activos asignados al personal administrativo docentes y estudiantes, se encuentre dentro del dominio establecido UCE, para su protección y monitoreo.

Artículo 37. De manera expresa se prohíbe a todos los funcionarios la instalación de software sin previa autorización en los computadores o dispositivos de propiedad de la UCE.

Artículo 38. Las computadoras de los funcionarios, deben ser configuradas con perfiles restringidos para la modificación de configuraciones de sistemas operativos y/o aplicaciones de la UCE.

Artículo 39. Es responsabilidad del personal técnico de las diferentes unidades académicas instalar y verificar que todos los computadores cuenten con las últimas actualizaciones de seguridad en los sistemas operativos, en los sistemas de procesamiento de datos, el antivirus institucional actualizado y activo.

Copias de seguridad de la información

Artículo 40. La DTIC debe garantizar la seguridad y el acceso a los respaldos de los sistemas informáticos universitarios, mediante instrucciones definidas por escrito a los funcionarios responsables de las mismas.

Artículo 41. Los respaldos de los sistemas informáticos deben ser almacenados en dispositivos como NAS, discos externos en buen estado o en la nube, cumpliendo estándares técnicos para el efecto el que incluya un plan de contingencia.

Artículo 42. Los funcionarios universitarios, deben realizar el respaldo de la información a su cargo con responsabilidad en un sitio seguro en función a un cronograma previamente establecido, que evite la alteración o pérdida de la información pública.

Registros de actividad del administrador y operador del sistema

Artículo 43. La DTIC deberá entregar las directrices al personal técnico encargado de la administración de la infraestructura tecnológica de la UCE para el registro del *logs* en caso de requerir auditorias.

Artículo 44. Los funcionarios con privilegios de administración de los sistemas informáticos universitarios deben registrar todos los cambios que se realicen en los mismos con la finalidad de llevar un control eficiente.

Artículo 45. El personal técnico tanto de la DTIC como la de las unidades académicas debe establecer procedimientos para el registro de incidentes de seguridad, mediante mesa de ayuda, los cuales, deben ser atendidos en forma inmediata.

Artículo 46. Los cambios, modificaciones o funcionalidades en los sistemas universitarios se los debe realizar mediante una solicitud por escrito dirigida a la Dirección de Tecnologías de la Información y Comunicación de la UCE.

Artículo 47. Los funcionarios técnicos de las diferentes áreas académicas deberán registrar en un reporte detallado los eventos de seguridad que se susciten en los puestos de trabajo, tanto de, docentes como del personal administrativo.

Área:	**Gestión de la continuidad del negocio**
Objetivo:	Asegurar la disponibilidad y continuidad de la información.
Control:	ISO/IEC 27002: 17.2.1. Redundancias - Disponibilidad de instalaciones, para el procesamiento de información.

Artículo 48. La DTIC gestionará el presupuesto para la implementación de instalaciones y equipamiento redundante para garantizar la continuidad del negocio, la confidencialidad, integridad y disponibilidad de la información.

Artículo 49. La DTIC deberá implementar procesos de continuidad de negocios para evitar las interrupciones en los sistemas universitarios o en procesos administrativos con la implementación de mecanismos para una recuperación efectiva ante un incidente de seguridad.

Artículo 50. La DTIC deberá implementar procesos para reducir los niveles de riesgo, sea por fallas de seguridad imprevista o desastres naturales implementando planes de recuperación de desastres a corto o mediano plazo.

Artículo 51. La DTIC, así como los centros de datos de facultades deberán gestionar la instalación de enlaces de fibra óptica redundantes a las conexiones del Core de la red para garantizar la disponibilidad y continuidad de las comunicaciones.

Área:	**Cumplimiento**
Objetivo:	Asegurar el cumplimiento de las normas y directrices establecidas en esta política de seguridad por parte de todos los estamentos universitarios.
Control:	ISO/IEC 27002: 18.2.2. Cumplimiento de las políticas y normas de seguridad.

Artículo 49. Es de responsabilidad del director/a, de la DTIC velar por el cumplimiento de esta normativa y procedimientos de seguridad en la UCE, así como de tomar los correctivos necesarios cuando amerite.

Artículo 50. Es responsabilidad de los funcionarios universitarios conocer, concientizar y aplicar la presente política de seguridad.

Artículo 51. Es responsabilidad del Comité de Seguridad de la Información de la UCE asegurar la implementación de todos los controles establecidos en esta política mediante un informe por escrito para verificar el cumplimiento de todas las condiciones de seguridad requeridas.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

- Conjuntamente con el personal de infraestructura de la Dirección de Tecnologías de Información y Comunicación de la Universidad Central del Ecuador, se realizó el análisis de riesgos y valoración de la situación actual de la infraestructura de la Institución, se utilizó la metodología Magerit, para obtener los activos más críticos expuestos a vulnerabilidades y amenazas

- Entre los activos críticos se encontró *software* en donde se almacena información sensible y de vital importancia para la institución expuestos a riegos inminentes, por lo que sin tomar las medidas adecuadas se pueden materializar las amenazas encontradas.

- De acuerdo a las vulnerabilidades y amenazas encontradas en el análisis se evidencia que era imprescindible la actualización de la política de seguridad con nuevos controles, estándares y procedimientos de seguridad, para una correcta administración de todos los activos y evitar incidentes dentro de la infraestructura tecnológica garantizando el manejo eficiente y seguro de los procesos.

- Para reducir incidentes de seguridad y salvaguardar la integridad, confidencialidad y disponibilidad de la información se seleccionó controles específicos de la Norma ISO IEC 27002:2013 que conforman la presente política además de buenas prácticas para la gestión de seguridad.

5.2. Recomendaciones

Se recomienda:

- Que a través de la Dirección de Tecnologías de la Información y Comunicación de la Universidad Central del Ecuador se gestione la aprobación de la presente política de seguridad ante la autoridad competente para su inmediata aplicabilidad.
- La difusión de la política en los diferentes medios universitarios para conocimiento de todos los estamentos, con la finalidad de aplicarla de manera urgente ya que la seguridad de la información es responsabilidad y compromiso de todos.
- La capacitación en temas de seguridad de la información a todos los funcionarios universitarios.
- La creación oficial del Comité de Gestión de la Seguridad de la Información (CSI) de la Universidad Central del Ecuador con la designación de sus miembros. Este Comité será el encargado de la aplicación, monitoreo, evaluación y actualización de la presente política, así como gestionar la provisión permanente del presupuesto para la adquisición de infraestructura tecnológica y personal especializado seguridad de la información.

Referencias

Burgos Salazar Jorge y Campos Pedro G. (2008). Obtenido de http://ceur-ws.org/Vol-488/paper13.pdf

Cárdenas, C. I. (2020). *Diseño de una política de seguridad de la Información para la Unidad Educativa Borja 3 Cavanis basado en la norma ISO-IEC27002:2013.* Obtenido de https://repositorio.uisek.edu.ec/handle/123456789/3656?locale=es

Cevallos Jarro, H. Y. (2019). *Diseño de una política de seguridad de la información para el área de TICS del Instituto Tecnológico Superior Central Técnico, basado en la norma de seguridad ISO/IEC27002:2013*. Obtenido de http://repositorio.uisek.edu.ec/handle/123456789/3320

Cisco. (2005). *Política de seguridad de la red: Informe oficial de mejores prácticas*. Obtenido de https://www.cisco.com/c/es_mx/support/docs/availability/high-availability/13601-secpol.html

El Comercio/Actualidad/Seguridad. (2019). Obtenido de https://www.elcomercio.com/actualidad/ecuador-denuncia-millones-ciberataques-assange.html

Espín, D. N. (2015). Obtenido de https://repositorio.pucesa.edu.ec/bitstream/123456789/1555/1/76092.pdf

Estatuto Universitario. (2019). *uce.edu.ec/web/normativa*. Obtenido de https://drive.google.com/file/d/1YYR1d-ryEwhTXl4TkJ6OOMeyPTujp09I/view

Excellence, I. (2018). *https://www.pmg-ssi.com/*. Obtenido de https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/

FUNDIBEQ. (s.f.). *Fundación Iberoamericana para la gestión de la calidad.* Obtenido de https://www.fundibeg.org/.informacion/infoiso/iso-seguridad-de-la-informacion

INCIBE. (2015). *https://www.incibe.es/*. Obtenido de Gestión de riesgos: https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_proteccion-de-la-informacion.pdf

INCIBE. (2017). *https://www.incibe.es/*. Obtenido de Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian?: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

ISO27000. (s.f.). Obtenido de iso27000.es/sgsi.html

León, L. A. (2017). *Plan director de seguridad para una Universidad colombiana.* Obtenido de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/64685/6/arleonlTFM0617memoria.pdf

Magerit 3.0 Libro I - Método. (2012). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Obtenido de http://administracionelectronica.gob.es

Magerit 3.0 Libro II Catálogo de elementos. (octubre de 2012). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Obtenido de http://administracionelectronica.gob.es

Magerit 3.0 Libro III. (2012). *Guía de técnicas.* Obtenido de http://administracionelectronica.gob.es

Mentor, A. (2016). *Normas ISO sobre gestión de seguridad de la información*. Obtenido de Gobierno de España: Ministerio de Educación Cultura y Deporte: http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/normas_iso_sobre_gestin_de_seguridad_de_la_informacin.html

Morán, C. E. (2016). *Diseño de un sistema de seguridad de la Información basado en la ISO/IEC/27001: 2013 para el Instituto Nacional de Vías Territorial Mariño.* Obtenido de https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/11876/1/12990690.pdf

Ostec Business Security . (s.f.). Obtenido de Buenas prácticas para gestión de la seguridad de la información: https://ostec.blog/es/generico/iso-27002-buenas-practicas-gsi

Palma, M. F. (diciembre de 2019). *Diseño de una política de seguridad de la información basada en el norma ISO27002:2013 para el control de accesoa la infraestructura de red de AXXIS hospital.* Obtenido de https://repositorio.uisek.edu.ec/handle/123456789/3647

Transparencia UCE. (2019). *uce.edu.ec/web/transparencia*. Obtenido de http://repositorio.uce.edu.ec/archivos/rectorado/LOTAIP/LOTAIP_OCTUBRE/Literal_b2-Distributivo_del_personal.pdf

UNE-EN ISO/IEC 27001:2017. (2013). *Tecnología de la información, Técnicas de seguridad Sistemas de Gestión de la Seguridad de la Información, Requisitos (ISO/IEC 27002:2013 incluyendo Cor 1:2014 y Cor 2:2015).*

UNIR. (14 de 05 de 2020). *Universidad Internacional de la Rioja*. Obtenido de Claves de las políticas de seguridad informática:

https://www.unir.net/ingenieria/revista/noticias/politicas-seguridad-informatica/549204996232/

Anexo 1 *Documento de autorización de la Universidad Central del Ecuador.*

UNIVERSIDAD CENTRAL DEL ECUADOR

DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Oficio Nro. UCE-DTIC-2020-0489-O

Quito, 12 de marzo de 2020

Asunto: Respuesta a solicitud

Señor Ingeniero
Alfonso Fabián Portilla Hernández
Coordinador de Tecnologías de Información FCM
UNIVERSIDAD CENTRAL DEL ECUADOR
En su Despacho

De mi consideración:

En respuesta al Oficio No. FCM-DTIC-2020-010, mediante el cual solicita la autorización para poder realizar el trabajo de investigación denominado "Diseño de una política de seguridad para la infraestructura de la red de la Universidad Central del Ecuador basada en la ISO / ICE 27002:2013", tengo a bien indicar que su requerimiento ha sido autorizado.

En base a lo anteriormente indicado, solicito de la manera más comedida todos los trabajos que requiera levantamiento y acciones correspondientes sean debidamente coordinados a través del Area de Insfraestructura de DTIC; así como también agradeceré se presente un informe de los resultados obtenidos a fin de analizar la factibilidad de implementación dentro de esta institución.

Finalmente, pongo a su disposición las facilidades necesarias para una exitosa culminación de sus objetivos, así como también solicito la discrecionalidad de la información.

Con sentimientos de distinguida consideración.

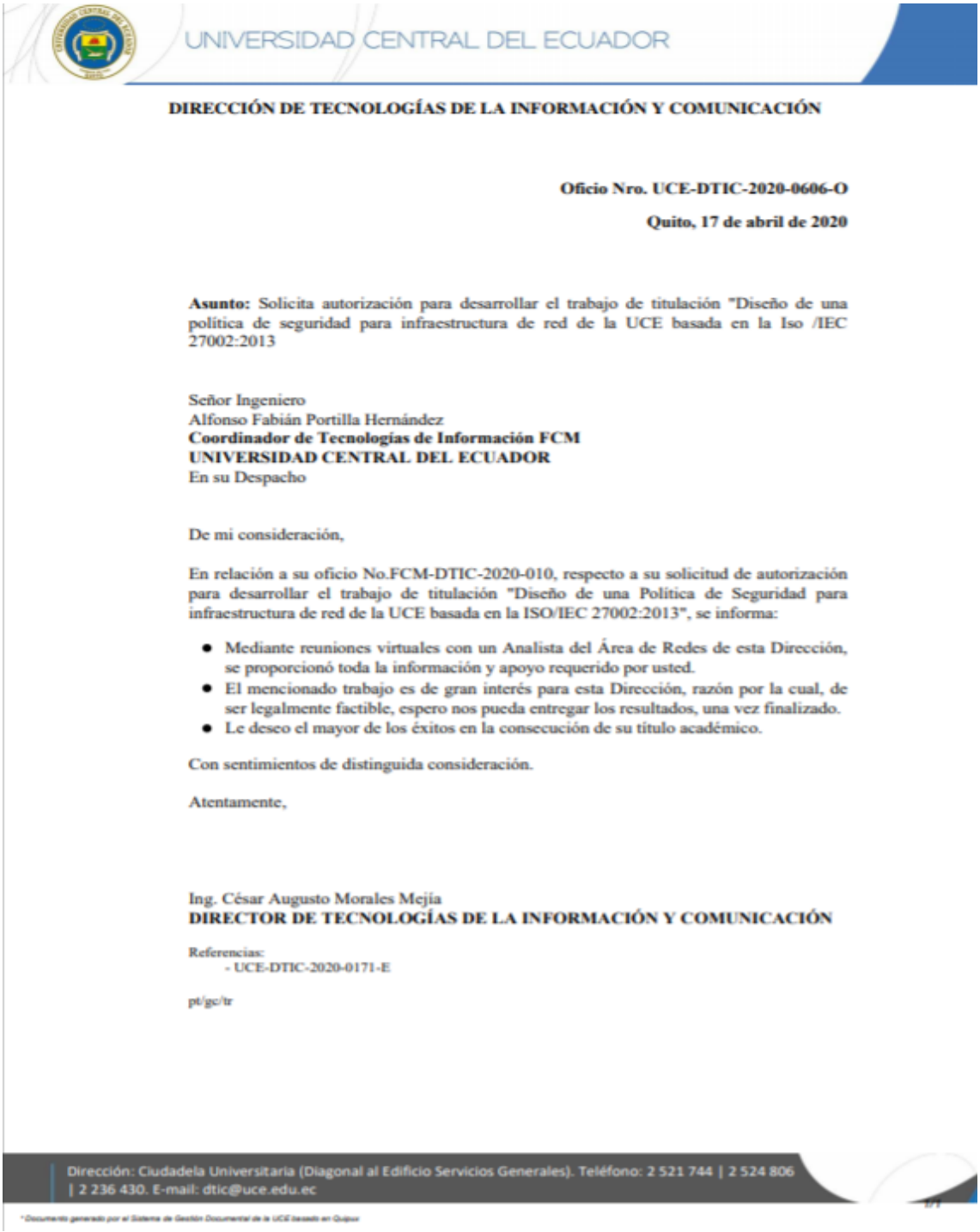
Atentamente,

Ing. César Augusto Morales Mejía
DIRECTOR DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Anexos:
- FCM-DTIC-2020-010.pdf

tr

Anexo 2 *Documento de autorización uso de Información de la UCE*



UNIVERSIDAD CENTRAL DEL ECUADOR

DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Oficio Nro. UCE-DTIC-2020-0606-O

Quito, 17 de abril de 2020

Asunto: Solicita autorización para desarrollar el trabajo de titulación "Diseño de una política de seguridad para infraestructura de red de la UCE basada en la Iso /IEC 27002:2013

Señor Ingeniero
Alfonso Fabián Portilla Hernández
Coordinador de Tecnologías de Información FCM
UNIVERSIDAD CENTRAL DEL ECUADOR
En su Despacho

De mi consideración,

En relación a su oficio No.FCM-DTIC-2020-010, respecto a su solicitud de autorización para desarrollar el trabajo de titulación "Diseño de una Política de Seguridad para infraestructura de red de la UCE basada en la ISO/IEC 27002:2013", se informa:

- Mediante reuniones virtuales con un Analista del Área de Redes de esta Dirección, se proporcionó toda la información y apoyo requerido por usted.
- El mencionado trabajo es de gran interés para esta Dirección, razón por la cual, de ser legalmente factible, espero nos pueda entregar los resultados, una vez finalizado.
- Le deseo el mayor de los éxitos en la consecución de su título académico.

Con sentimientos de distinguida consideración.

Atentamente,

Ing. César Augusto Morales Mejía
DIRECTOR DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Referencias:
- UCE-DTIC-2020-0171-E

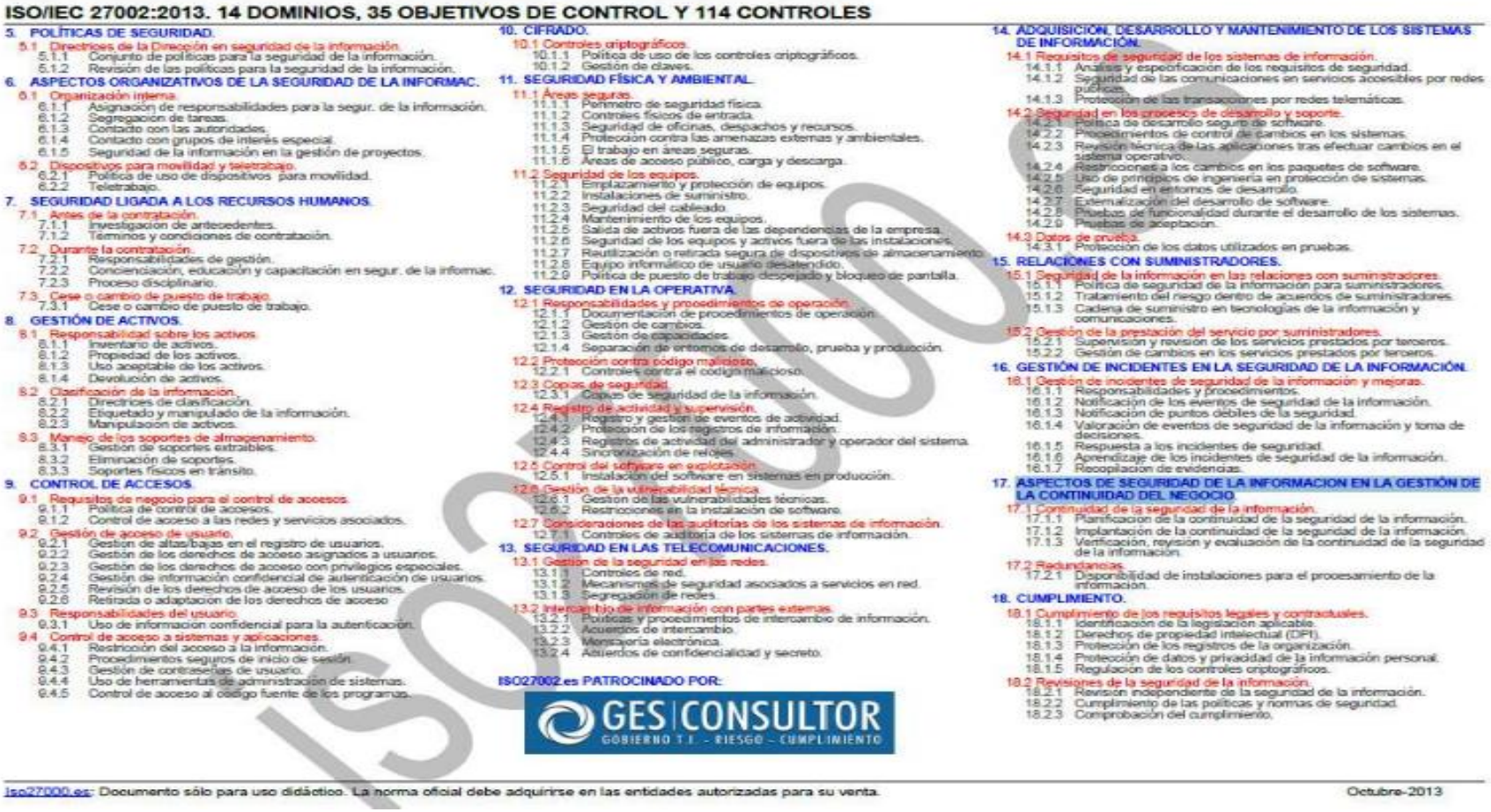
pt/gc/tr

Dirección: Ciudadela Universitaria (Diagonal al Edificio Servicios Generales). Teléfono: 2 521 744 | 2 524 806 | 2 236 430. E-mail: dtic@uce.edu.ec

1/1

*Documento generado por el Sistema de Gestión Documental de la UCE basado en Quipux

Anexo 3 *Controles ISO/IEC 27002: 2013*



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

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

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

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

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

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

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

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

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

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

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.

Octubre-2013