Escuela Superior Politécnica del Litoral

Facultad de Ingeniería en Electricidad y Computación

Diseño de un conjunto de políticas y controles para la gestión y mitigación de riesgos de seguridad informática del área de soporte técnico de una unidad de tecnología en una Universidad Pública de la ciudad de Guayaquil

Proyecto de Titulación

Previo la obtención del Título de:

Magíster en Seguridad Informática

Presentado por:

Luis Enrique Anchundia Solórzano

Gilson Adalberto Chacha Olivares

Guayaquil – Ecuador

Año: 2025

Agradecimiento

Agradezco a Dios por la sabiduría brindada durante el proceso que fue la maestría y el presente trabajo.

Agradezco a mi madre, que siempre está para mí y es el pilar fundamental de mi vida.

A mi hermana, quien ha sido un apoyo fundamental siempre, a mis sobrinas que me llenan de alegría todos los días.

A mi novia que me ha apoyado en todo momento.

A las autoridades que me brindaron la oportunidad de avanzar un escalón más como profesional.

Ing. Luis Enrique Anchundia Solórzano

Agradecimiento

Quiero expresar mi más profundo agradecimiento a todas las personas que hicieron posible la realización de esta tesis. Principalmente a mis padres por el apoyo incondicional que han sido pilares fundamentales de mi formación personal y profesional.

A la Escuela Superior Politécnica del Litoral (ESPOL), por brindarme la oportunidad de continuar mi formación académica de excelencia. A los docentes de la Maestría, por compartir su conocimiento con pasión, exigencia y compromiso.

A mis colegas de la institución, por su colaboración, tiempo y aportes durante la fase de recolección de información y validación de resultados.

Finalmente, gracias a todas las personas que, de una u otra manera, me ayudaron a culminar esta etapa. Esta tesis no es solo el cierre de un ciclo, sino el inicio de nuevos retos que asumo con entusiasmo, compromiso y responsabilidad.

¡Gracias Totales!

Lic. Gilson Adalberto Chacha Olivares

Dedicatoria

Este trabajo va dedicado especialmente a mis padres y mi familia.

A mi padre Olmedo, que, aunque ya no esté conmigo terrenalmente siempre estará a mi lado espiritualmente siendo un apoyo constante desde el cielo.

A mi madre Liliam, mi mayor tesoro, siempre presente en todo momento con su apoyo y amor incondicional.

A mi hermana Lorena, que siempre me ha apoyado desde que inicie mis estudios hasta ahora.

A mis sobrinas Karla y Marianny, que me motivan con su alegría y cariño.

A mi novia Georgina, que ha estado conmigo durante todo este proceso brindándome su apoyo y amor.

Ing. Luis Enrique Anchundia Solórzano

Dedicatoria

Dedico este trabajo a Dios, por ser mi guía y fortaleza en cada paso de este camino.

A mis padres cuyo amor incondicional, valores y sacrificios han sido el pilar de mi formación personal y profesional. Gracias por enseñarme que el esfuerzo constante y la humildad son el verdadero camino al éxito.

A mis hermanos y seres queridos, por su apoyo, paciencia y palabras de aliento cuando más las necesité. Cada logro que alcanzo es también suyo.

Y a mí mismo, por no rendirme, por creer, por avanzar a pesar de los desafíos. Esta tesis representa no solo un logro académico, sino un compromiso con mis sueños.

Lic. Gilson Adalberto Chacha Olivares

Declaración Expresa

Nosotros Luis Enrique Anchundia Solórzano y Gilson Adalberto Chacha Olivares, acordamos y reconocemos que:

La titularidad de los derechos patrimoniales de autor (derechos de autor) del proyecto de graduación corresponderá a los autores, sin perjuicio de lo cual la ESPOL recibe en este acto una licencia gratuita de plazo indefinido para el uso no comercial y comercial de la obra con facultad de sublicenciar, incluyendo la autorización para su divulgación, así como para la creación y uso de obras derivadas. En el caso de usos comerciales se respetará el porcentaje de participación en beneficios que corresponda a favor del autor o autores.

La titularidad total y exclusiva sobre los derechos patrimoniales de patente de invención, modelo de utilidad, diseño industrial, secreto industrial, software o información no divulgada que corresponda o pueda corresponder respecto de cualquier investigación, desarrollo tecnológico o invención realizada por nosotros durante el desarrollo del proyecto de graduación, pertenecerán de forma total, exclusiva e indivisible a la ESPOL, sin perjuicio del porcentaje que nos corresponda de los beneficios económicos que la ESPOL reciba por la explotación de nuestra innovación, de ser el caso.

En los casos donde la Oficina de Transferencia de Resultados de Investigación (OTRI) de la ESPOL comunique a los autores que existe una innovación potencialmente patentable sobre los resultados del proyecto de graduación, no se realizará publicación o divulgación alguna, sin la autorización expresa y previa de la ESPOL.

Guayaquil, 25 de agosto del 2025.

Ing. Luis Enrique
Anchundia Solórzano

Lic. Gilson Adalberto
Chacha Olivares

Evaluadores

M.Sc. Lenin Eduardo Freire Cobo

Tutor

M.Sc. Juan Carlos García Plúa

Revisor

Resumen

Esta tesis aborda las complicaciones en la gestión de riesgos de seguridad informática en el área de soporte técnico de una universidad pública de Guayaquil. Se identificó una alta exposición a amenazas como malware, accesos no autorizados y errores humanos, debido a la ausencia de políticas claras y controles específicos.

Como solución, se diseñó un conjunto de políticas y controles basados en los estándares ISO/IEC 27001 e ISO 31000. A través de entrevistas y análisis de riesgos, se identificaron activos críticos, se evaluaron vulnerabilidades y se establecieron medidas correctivas según la criticidad. El resultado es una propuesta estructurada de controles preventivos, detectivos y correctivos que, de implementarse, fortalecería la protección de la información institucional y alinearía a la universidad con la Ley Orgánica de protección de datos personales y buenas prácticas internacionales.

Palabras clave: Seguridad informática, Gestión de riesgos, Controles de seguridad

Abstract

This thesis addresses the complications in managing IT security risks in the technical support area of a public university in Guayaquil. High exposure to threats such as malware, unauthorized access, and human error was identified due to the absence of clear policies and specific controls.

As a solution, a set of policies and controls based on the ISO/IEC 27001 and ISO 31000 standards was designed. Through interviews and risk analysis, critical assets were identified, vulnerabilities were assessed, and corrective measures were established according to criticality. The result is a structured proposal for preventive, detective, and corrective controls that, if implemented, would strengthen the protection of institutional information and align the university with the Organic Law on Personal Data Protection and international best practices.

Keywords: IT security, Risk management, Security controls

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

La gestión de la seguridad informática en instituciones de educación superior es cada vez más crítica, dada la creciente dependencia de sistemas digitales que manejan datos sensibles de estudiantes, docentes y personal administrativo. En una universidad pública de Guayaquil, el área de soporte técnico enfrenta complicaciones en esta materia, con una alta exposición a amenazas como phishing, malware, accesos no autorizados y fallas técnicas. Esta situación se ve agravada por la falta de políticas y controles específicos, así como una limitada cultura de seguridad entre los usuarios.

Frente a este panorama, esta tesis propone el diseño de un conjunto de políticas y controles de seguridad informática enfocados exclusivamente en el soporte técnico, tomando como base los estándares internacionales ISO/IEC 27001 e ISO 31000. Estos marcos proporcionan un enfoque estructurado y adaptable para la identificación, análisis y tratamiento de riesgos, así como para el desarrollo de controles técnicos y administrativos que fortalezcan la confidencialidad, integridad y disponibilidad de la información.

El alcance del trabajo se limita al diseño conceptual, con la finalidad de establecer un marco claro que pueda ser implementado posteriormente por la institución. Para ello, se plantean los siguientes objetivos: identificar los activos y sistemas críticos del área de soporte técnico; analizar las principales vulnerabilidades y amenazas; categorizar los riesgos según su nivel de criticidad; y definir controles de seguridad específicos alineados con normas internacionales.

Con esta propuesta se busca no solo reducir los riesgos actuales, sino también generar una base sólida para la mejora continua de la seguridad institucional, cumpliendo con la normativa nacional vigente en materia de protección de datos y preparándose para los desafíos tecnológicos futuros.

CAPÍTULO I

GENERALIDADES

1.1. Antecedentes

En una universidad pública de la ciudad de Guayaquil, el área de soporte técnico enfrenta serias dificultades en la gestión de riesgos de seguridad informática, lo que incrementa la vulnerabilidad de los sistemas y datos institucionales. Entre los principales riesgos se encuentran ciberataques como phishing, malware y ataques de denegación de servicio distribuido (DDoS), así como accesos no autorizados, errores humanos y fallas técnicas en los equipos y plataformas utilizadas. La falta de procedimientos claros para identificar y mitigar estos riesgos, junto con la escasa conciencia de los usuarios sobre buenas prácticas de seguridad, dificulta la labor del soporte técnico y compromete la estabilidad operativa de la universidad. Además, el crecimiento acelerado de la infraestructura tecnológica y la ausencia de controles específicos agravan la exposición de información confidencial de estudiantes y personal administrativo, afectando la continuidad de los servicios y la eficiencia en la resolución de incidentes dentro del área de soporte técnico.

1.2. Descripción del problema

La falta de políticas y controles específicos en el área de soporte técnico expone a la institución a graves consecuencias, como la pérdida de datos confidenciales relacionados con el personal administrativo y los estudiantes. Esto puede generar daños a la reputación de la universidad, elevados costos financieros y sanciones legales por incumplimiento de normativas de protección de datos, como la Ley Orgánica de Protección de Datos Personales (LOPDP). Por ello, se propone realizar un análisis de riesgos específicamente enfocado en las actividades y responsabilidades del soporte técnico dentro del área de TI. Este análisis permitirá identificar vulnerabilidades y establecer medidas para mitigar el impacto de posibles incidentes, tomando como referencia normas internacionales como las ISO 27001 y 31000.

De acuerdo con un estudio realizado por la alianza del software, el 90% de líderes de empresas están de acuerdo en que los datos son uno de los recursos críticos y distintivos entre las empresas y organizaciones [1]. Así mismo, los datos generados por instituciones educativas son considerados un activo de alto valor en cuanto a la gestión de la seguridad de la información se refiere, entre esos datos se encuentran los de gestión administrativa, datos de servicio público y datos culturales. La importancia de estos datos hace que la mayoría de los ciberataques y amenazas vayan dirigidos hacia las instituciones de educación superior, por lo cual es necesario tomar medidas de control para asegurar la protección de los datos [1]. Por otro lado, la información es un activo crucial para toda organización y esta se encuentra en diversas formas como escrita o impresa en papel, almacenada en medios electrónicos, enviada a través de correos electrónicos, en clips de video o transmitida oralmente. Además, la seguridad de la información tiene como objetivo principal preservar la

confidencialidad, la integridad y la disponibilidad de la información [2]. También, las amenazas hacia la seguridad de la información cuestan grandes cantidades de dinero, horas de suspensión de actividades y causan incertidumbre en grandes y pequeñas empresas. Adicionalmente, la pérdida de activos de información implica riesgos financieros y de reputación, por lo que toda organización debe contar con un sistema de seguridad que analice y gestione estos riesgos [3]. La ISO 31000 es una herramienta en la cual su principal objetivo es estandarizar las diferentes normas, técnicas y paradigmas que varían entre industrias para llevar un correcto control de gestión de riesgos adaptándose a todo tipo de organización [4]. Por otro lado, el diseño de un análisis de riesgos en el contexto de la ISO/IEC 27001 implica un proceso sistemático para identificar, evaluar y tratar los riesgos de seguridad de la información dentro de una organización. Este estándar establece los requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI) y requiere que las organizaciones identifiquen los activos de información, evaluación de las amenazas, calificación de los riesgos y tratamiento [5].

Como trabajadores del área de TI de una institución superior del país, el acceso a los sistemas, datos y procesos críticos es parte de nuestra responsabilidad diaria en la institución. Esto nos facilitaría la obtención de información necesaria para la evaluación de riesgos y la implementación de controles dentro del área de soporte técnico. Además, del conocimiento previo de la infraestructura tecnológica de la institución es una ventaja que agilizará el desarrollo del marco de trabajo.

La ejecución del proyecto es viable desde un punto de vista técnico debido a la disponibilidad de marcos internacionales estandarizados de ciberseguridad que servirán como base, tales como ISO 27001, ISO 31000.

1.3. Solución propuesta

Para solucionar el problema relacionado con la gestión y mitigación de riesgos de seguridad informática específicamente en el área de soporte técnico de una unidad de tecnología en una universidad pública de Guayaquil, se propone diseñar un conjunto de políticas y controles de seguridad basados en estándares internacionales tales como la ISO 27001 e integrado junto con las directrices de gestión de riesgos indicadas en la ISO 31000. La implementación de esta solución permitirá identificar, evaluar y tratar los riesgos de manera sistemáticas, garantizando la confidencialidad, integridad y disponibilidad de los activos críticos en el soporte técnico de la universidad. Además, al implementar políticas y controles alineados con estas normativas, se fortalecen la confidencialidad, integridad y disponibilidad de los datos, elementos claves para la protección de los procesos académicos, administrativos y de investigación de la universidad [1].

Este diseño abarca políticas orientadas a regular el acceso, proteger la información y gestionar incidentes, complementadas por controles destinados a prevenir, detectar y corregir posibles riesgos relacionados con la seguridad de la información durante el soporte técnico en la universidad.

También, se plantea un marco de análisis de riesgos basado en la norma ISO 31000, que permitirá identificar amenazas, vulnerabilidades y riesgos asociados a los activos del soporte técnico de TI, priorizándolos mediante matrices de impacto y probabilidad. Cabe destacar que esta solución se limitará exclusivamente a la fase de diseño, sin proceder a su implementación, enfocándose en proporcionar un marco conceptual y metodológico que pueda servir de base para futuras acciones.

La solución propuesta ofrece beneficios clave en el área de soporte técnico de la universidad. En primer lugar, fomenta una seguridad integral al reducir significativamente los riesgos relacionados con ciberataques, accesos no autorizados y fallos operativos, fortaleciendo la protección de los activos críticos. Además, garantiza el cumplimiento normativo, asegurando la alineación con la Ley Orgánica de Protección de Datos Personales (LOPDP) y otros marcos legales relevantes, lo que disminuye el riesgo de sanciones legales. Asimismo, incrementa la resiliencia institucional, dotando a la universidad de la capacidad para detectar y responder de manera ágil a incidentes de seguridad informática en el soporte técnico, minimizando impactos financieros y reputacionales asociados.

1.4. Objetivo general

Diseñar un conjunto de políticas y controles destinados a la gestión y mitigación de riesgos de seguridad del soporte técnico en el área de Tecnologías de la Información de una universidad pública en Guayaquil, con el propósito de garantizar una seguridad integral.

1.5. Objetivos específicos

1. Identificar los principales activos de información y sistemas críticos de la universidad.
2. Analizar las vulnerabilidades y amenazas a las que están expuestos estos activos.
3. Categorizar los principales riesgos a los que se expone la universidad dentro de sus actividades en soporte técnico de TI.
4. Definir un conjunto de controles de seguridad específicos para mitigar los principales riesgos identificados en los sistemas y procesos del soporte

técnico del área de TI.

1.6. Metodología

En el presente proyecto de titulación se desarrollará un estudio transversal, mediante el cual se llevará a cabo un levantamiento de información a través de entrevistas en el departamento de tecnologías de la información específicamente del área de soporte técnico. Esta recolección de datos permitirá obtener información detallada sobre los activos críticos que se procesan en el área de soporte técnico de la institución de educación superior. Además, este enfoque facilitará una evaluación del estado actual de los activos más relevantes en términos de gestión y mitigación de riesgos.

La población de interés corresponde al departamento de Soporte Técnico de la universidad, conformado por aproximadamente siete personas. Se seleccionará una muestra no probabilística de tres individuos mediante muestreo por conveniencia, incluyendo al director de Ingeniería en Sistemas, un analista y un asistente de soporte técnico, con el objetivo de recopilar información clave sobre los activos críticos del área de acuerdo con su experiencia en la misma.

Se llevará a cabo un estudio basado en entrevistas a las personas seleccionadas del área de soporte técnico de TI, con el objetivo de identificar y recopilar información sobre aquellos activos críticos que administra y posee el área, tanto de hardware como de software, que son de vital importancia para los procesos de la institución.

Durante las entrevistas se abordarán temas como:

- Identificación de activos críticos
- Evaluación de políticas y controles actuales
- Prácticas y cultura de seguridad
- Historial de incidentes de soporte técnico en la institución

A través de la información obtenida y luego de una evaluación a las respuestas recopiladas se pretende definir que activos de soporte técnico deben estar obligadamente bajo una correcta gestión de riesgos. También se definirá los controles de mitigación necesarios para cuando un riesgo se convierta en un problema real.

CAPITULO II

MARCO TEÓRICO

2.1. SEGURIDAD DE LA INFORMACIÓN

«Un activo es todo aquello que tiene valor para la organización. La información es un activo importante y esencial para las necesidades de negocio de una organización.» [2]

La seguridad de la información se define como un conjunto de políticas, controles, procedimientos y tecnologías diseñadas para la protección de datos y los sistemas de información contra amenazas internas y externas. La seguridad de la información es un conjunto de acciones y medidas continuas, más allá de simples reglas o herramientas. Se centra en garantizar la confidencialidad, integridad y disponibilidad de la información, con el objetivo de minimizar los riesgos y asegurando la continuidad académica y administrativa. [6]

Confidencialidad: Garantiza que la información esté accesible solo para personas, entidades o procesos autorizados, previniendo el acceso no autorizado.

Integridad: Asegura que los datos no sean alterados o manipulados de manera no autorizada, manteniendo su precisión, consistencia y confiabilidad.

Disponibilidad: Garantiza que los sistemas, servicios y datos estén accesibles y utilizables cuando se necesiten por los usuarios autorizados.

En el contexto universitario los sistemas académicos y/o administrativos son fundamentales para la continuidad de las operaciones académicas y administrativas. La creciente dependencia de tecnologías digitales aumenta la exposición a riesgos y amenazas que comprometen la operación normal de estas instituciones.

Las amenazas en la seguridad informática en un entorno universitario representan eventos o agentes que tienen el potencial de explotar vulnerabilidades y comprometer la confidencialidad, integridad o disponibilidad de los activos de información. Estas pueden originarse tanto de fuentes internas como externas y se relacionan con riesgos inherentes y residual al entorno académico y administrativo.

Acceso Apropiado

Esta definición sostiene que la información es segura si, y solo si, hay acceso apropiado a la misma. El acceso apropiado considera lo siguiente:

Acceso Autorizado: Solo los usuarios autorizados deberían poder acceder a la información.

Acciones Permitidas: Los usuarios autorizados solo deberían poder realizar acciones sobre la información que estén autorizados a hacer.

Contexto: Se debe considerar el contexto específico en el que se utiliza la información.

Esta definición tiene como objetivo cerrar la brecha entre los aspectos técnicos y no técnicos de la seguridad de la información. Reconoce que el comportamiento humano, las políticas y los procedimientos juegan un papel importante en la seguridad de la información, no solo los controles técnicos. [7]

La gestión de seguridad incluye componentes como [8]:

- Proceso de seguridad.
- Gestión y análisis de riesgos.
- Implementación y gestión de controles de seguridad.
- Roles y responsabilidades organizacionales.
- Clasificación de la información.
- Planes y políticas de seguridad de la información, procedimientos, estándares, directrices, líneas de base, clasificación de la información y documentación.
- Seguridad del personal y privacidad.
- Concientización sobre seguridad y educación y capacitación continuas.

Principales amenazas en el contexto universitario

En un entorno universitario, las principales amenazas de seguridad informática incluyen [9]:

Ciberataques dirigidos: Actividades como el phishing, ransomware y ataques de denegación de servicio (DDoS), que buscan afectar sistemas críticos como plataformas académicas y registros estudiantiles.

Errores humanos: Incluyen configuraciones incorrectas, uso de contraseñas débiles y negligencia en el manejo de información sensible. Estos errores, ya sean intencionales o no, representan vectores comunes de riesgo y pueden facilitar accesos no autorizados a sistemas y datos críticos.

Acceso no autorizado: Lallie et al. (2025) destacan que las amenazas internas, facilitadas por usuarios legítimos sin formación adecuada, pueden derivar en accesos no autorizados a sistemas críticos, comprometiendo la confidencialidad y la integridad de la información.

Fallas tecnológicas: Incluyen interrupciones inesperadas en los sistemas provocadas por errores de hardware, fallos de software o configuraciones deficientes. A esto se suma la dependencia de proveedores externos para servicios críticos, lo que incrementa el riesgo de afectaciones operativas ante fallas en su infraestructura o disponibilidad.

Amenazas físicas: Comprenden eventos como desastres naturales, cortes de energía y robo de dispositivos, los cuales comprometen la disponibilidad y protección de los datos institucionales. Además, la dependencia de proveedores externos para servicios críticos introduce riesgos adicionales, ya que un ataque o fallo técnico en su infraestructura puede traducirse en una pérdida de disponibilidad para la universidad, constituyendo una amenaza física indirecta.

2.2. GESTIÓN DE RIESGOS EN TECNOLOGÍA DE LA INFORMACIÓN

La gestión de riesgos en la tecnología de información (TI) es un proceso fundamental para garantizar la seguridad y continuidad de los sistemas y datos de una organización. En el contexto de la seguridad informática, el riesgo se define como la posibilidad de que una amenaza explote una vulnerabilidad y cause un impacto negativo en los activos de información [10].

Importancia de la Gestión de Riesgos en TI

Las organizaciones modernas dependen en gran medida de sus sistemas de TI para llevar a cabo operaciones críticas. La Universidad Pública de la ciudad de Guayaquil no es una excepción, ya que maneja información sensible como datos académicos, administrativos y personales de estudiantes y empleados. Una gestión de riesgos eficaz permite:

- Identificar y priorizar riesgos: Reconocer cuáles son las amenazas más significativas y focalizar los recursos en mitigarlas.

- Proteger los activos de información: Implementar controles adecuados para salvaguardar la confidencialidad, integridad y disponibilidad de la información.
- Cumplir con regulaciones y normativas: Asegurar el cumplimiento de leyes y estándares aplicables, como la ISO 27001 o la Ley Orgánica de Protección de Datos Personales.
- Mejorar la toma de decisiones: Proporcionar información valiosa para decisiones estratégicas y operativas relacionadas con la seguridad de TI.

Proceso de Gestión de Riesgos en TI

El proceso de gestión de riesgos generalmente sigue un ciclo continuo que incluye las siguientes etapas [11]:

1.1 Identificación de Riesgos:

- Activos: Catalogar los activos de TI, como hardware, software, datos y personas.
- Amenazas: Enumerar posibles amenazas como malware, accesos no autorizados, errores humanos o desastres naturales.
- Vulnerabilidades: Detectar debilidades en los sistemas que podrían ser explotadas por amenazas.

2.1 Análisis y Evaluación de Riesgos:

- Probabilidad: Estimar la frecuencia con la que puede ocurrir cada riesgo.
- Impacto: Determinar las consecuencias potenciales en caso de que el riesgo se materialice.
- Niveles de Riesgo: Calcular el nivel de riesgo combinando probabilidad e impacto, generalmente utilizando matrices de riesgo.

3.1 Tratamiento de Riesgos:

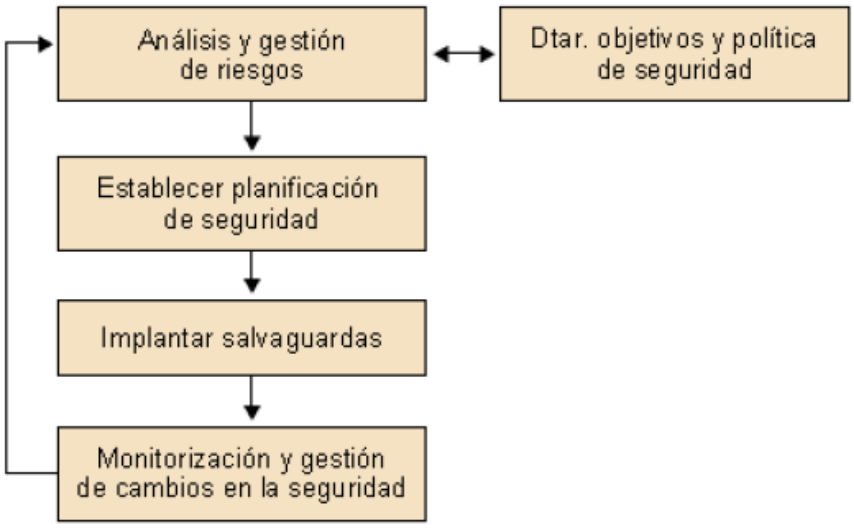
- Mitigación: Implementar controles para reducir la probabilidad o el impacto del riesgo.
- Aceptación: Decidir aceptar el riesgo si es bajo o si el costo de mitigación es superior al beneficio.
- Transferencia: Delegar el riesgo a terceros, por ejemplo, mediante seguros.
- Evitar: Eliminar actividades que generan el riesgo.

4.1 Monitoreo y Revisión:

- Seguimiento Continuo: Evaluar la eficacia de los controles y ajustar según sea necesario.
- Actualización del Análisis: Revisar y actualizar la evaluación de riesgos ante cambios en el entorno o la infraestructura.

A continuación, el siguiente gráfico corresponde al ciclo de vida correcto de la seguridad de la información, según los autores Daniel Cruz Allende, Arsenio Tortajada Gallego y Antonio José Segovia Henares. [12]

Figura 1 *Ciclo de vida de la seguridad de la información*



Políticas y Controles para la Gestión de Riesgos

Las políticas y controles son herramientas esenciales para formalizar y estandarizar el enfoque de gestión de riesgos.

- **Políticas de Seguridad:** Documentos que establecen las directrices y responsabilidades en materia de seguridad de la información.
- **Controles Técnicos:** Implementaciones como firewalls, sistemas de detección de intrusos, cifrado y autenticación multifactor.
- **Controles Administrativos:** Procedimientos y prácticas como gestión de contraseñas, capacitación en seguridad y planes de respuesta a incidentes.
- **Controles Físicos:** Medidas para proteger el entorno físico, como cerraduras, vigilancia y control de acceso a instalaciones.

Normativas y Estándares Internacionales

Adoptar marcos y estándares reconocidos internacionalmente mejora la eficacia y confiabilidad de la gestión de riesgos.

- **ISO/IEC 27001:** Proporciona un modelo para establecer, implementar y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).
- **ISO 31000:** Ofrece principios y directrices genéricas sobre gestión de riesgos.
- **NIST SP 800-30:** Guía para la realización de evaluaciones de riesgos en sistemas de información.

2.3. MITIGACIÓN DE RIESGOS EN TECNOLOGÍAS DE LA INFORMACIÓN

Mitigar riesgos implica encontrar soluciones a posibles problemas. Existen diversas estrategias para abordar los riesgos, cada una con sus propios desafíos y necesidades de recursos. Sin embargo, a pesar de los esfuerzos, muchos proyectos de TI fracasan debido a una gestión de riesgos inefectiva. Para evaluar

y priorizar los riesgos, se utilizan técnicas como la calificación de riesgos, que combina la probabilidad y el impacto de un evento, y el examen de factores de riesgo, que ayuda a determinar la profundidad del análisis requerido.[13]

Los riesgos pueden clasificarse en dos tipos: aquellos que podemos prevenir y aquellos que no. Dependiendo de su gravedad, podemos decidir si los evitamos por completo o si implementamos medidas para reducir sus consecuencias. [14]

Controles: Son mecanismos diseñados para salvaguardar nuestros sistemas y datos de cualquier acción que pueda comprometer su integridad o confidencialidad. Estos pueden ser de naturaleza técnica (como firewalls o encriptación) o administrativa (como políticas de acceso o programas de capacitación) [15].

Controles preventivos

Los controles de carácter preventivo tienen como objetivo evitar que se produzcan fallos en la seguridad. [16]

Autenticación. – El control de autenticación se utiliza para confirmar que una persona es quien dice ser. Esto se logra mediante diferentes métodos, como claves de acceso, códigos personales (PIN) y tecnologías modernas que garantizan una autenticación más segura, como dispositivos de seguridad, tarjetas electrónicas, certificados digitales o sistemas como Kerberos.

Autorización. – El control de autorización define y administra qué acciones están permitidas dentro de un sistema específico. Por ejemplo, un administrador de base de datos o el responsable de la información pueden determinar quién tiene permisos para modificar un archivo compartido utilizado por un grupo de usuarios en línea.

Cumplimiento del control de acceso. – La integridad y confidencialidad de los datos se protegen con controles de acceso, aplicados mediante políticas como

Control de Acceso Obligatorio o Control de Acceso Discrecional, y respaldados por permisos, listas de control y perfiles. Su eficacia depende de la correcta configuración y diseño de las medidas de seguridad.

No repudio. – La responsabilidad en un sistema requiere asegurar que los emisores no puedan negar el envío de información ni los receptores negar su recepción. La no repudio, enfocada en prevenir y detectar negaciones indebidas, utiliza mecanismos como certificados digitales para evitar rechazos fraudulentos.

Comunicaciones protegidas. – En sistemas distribuidos, la seguridad depende de comunicaciones confiables. Para proteger la información sensible en tránsito, se aplican métodos de cifrado como redes privadas virtuales y tecnologías criptográficas (e.g., RSA, MD5, DES). Esto mitiga riesgos como intercepciones, espionaje y capturas de datos en la red.

Privacidad de las transacciones. – Los sistemas públicos y privados deben garantizar la privacidad de las personas. Para proteger las transacciones individuales, se emplean controles como SSL y Secure Shell, que evitan la exposición de información privada. [16]

Controles Detectivos

Los controles detectivos tienen como objetivo identificar violaciones en los procedimientos internos de una organización, como registros fraudulentos o discrepancias financieras, a través de verificaciones aleatorias y revisiones realizadas por auditores internos y externos. Aunque no están diseñados para prevenir eventos inesperados, su enfoque investigativo permite detectar problemas después de que ocurren, proporcionando información oportuna a la gerencia sobre desviaciones en procesos o actividades. Son especialmente útiles en economías avanzadas con altos niveles de cumplimiento, donde complementan a los controles preventivos. [17]

Controles Correctivos

Los controles correctivos, según el Comité de Organizaciones Patrocinadoras de la Comisión Treadway (COSO), se centran en las acciones necesarias para abordar problemas identificados tras la supervisión y revisión de sistemas operativos. Estos controles se manifiestan como actividades específicas, como ajustes en programas de capacitación, introducción de nuevos sistemas de recompensas o sanciones más estrictas por incumplimientos. Su propósito principal es prevenir la repetición de errores, garantizando así un mejor rendimiento y estándares más altos. Además, son herramientas clave para actualizar políticas existentes y adaptarlas a nuevas tendencias operativas. Aunque irregularidades financieras pueden no ser detectadas inicialmente, estos controles buscan mitigar riesgos futuros mediante una clara comunicación de objetivos organizacionales. Algunos expertos también sugieren que la mejora continua en liderazgo y gestión, junto con colaboraciones entre los sectores público y privado, puede fortalecer los controles y mejorar la prestación de servicios esenciales. La transferencia de conocimiento y la planificación de sucesión, comunes en el sector privado, se destacan como prácticas útiles para mejorar el desempeño y la eficacia en las instituciones públicas. [17]

Planes de contingencia

Un plan de contingencia es esencial para prevenir y mitigar los efectos de desastres imprevistos que pueden afectar la continuidad de las operaciones de una organización. Este plan detallado incluye estrategias para identificar posibles riesgos, minimizar su impacto y restaurar los servicios afectados lo más rápido posible. El objetivo principal es mantener la disponibilidad de los sistemas de información y garantizar la continuidad del negocio en caso de cualquier interrupción. El Análisis de Impacto en el Negocio (BIA) es una herramienta

fundamental para evaluar los riesgos y priorizar las acciones necesarias para implementar un plan de contingencia efectivo. [18]

Planes de recuperación

Un desastre puede interrumpir las operaciones críticas de una empresa. Un Plan de Recuperación de Desastres (DRP) es esencial para minimizar el impacto de estos eventos. Este plan detallado incluye procedimientos para restaurar los sistemas y datos afectados. Desarrollar un DRP requiere un análisis cuidadoso de los riesgos y la implementación de medidas preventivas. Aunque implica costos, un DRP es una inversión valiosa, especialmente en la era digital, donde los datos se han convertido en un activo crucial para las organizaciones. [19]

La recuperación de desastres es una parte especializada del plan general para mantener el negocio funcionando en caso de crisis. Se centra exclusivamente en la tecnología, buscando restaurar los sistemas informáticos y las redes de una empresa después de un desastre. Esto implica recuperar la información perdida, reparar o reemplazar el equipo dañado y volver a conectar todos los sistemas para que la empresa pueda operar nuevamente lo antes posible. Para lograr esto, se identifican las partes más importantes de la tecnología, se crean planes para guardar copias de seguridad de los datos y se instalan sistemas adicionales para evitar que un solo fallo detenga todo el funcionamiento. [20]

CAPÍTULO III

IDENTIFICACIÓN DE LOS PRINCIPALES SERVICIOS DE SOPORTE TÉCNICO DE LA UNIDAD DE TECNOLOGÍA DE UNA IES

3.1 IDENTIFICACIÓN DE SERVICIOS CLAVES

Después de llevar a cabo entrevistas con miembros clave del equipo de soporte técnico de la unidad de tecnología, se indicó que se ofrecen diversos servicios para atender las diferentes situaciones bajo su responsabilidad dentro de la universidad. Los servicios proporcionados son los siguientes:

Atención a usuarios (incidencias y requerimientos):

Gestión de incidencias relacionadas con fallos en equipos informáticos, como pantallas que no encienden, problemas con teclados o errores en sistemas operativos.

Atención a requerimientos no críticos, como la instalación de nuevos sistemas, creación de accesos directos a programas o carpetas, y personalización de plantillas.

Resolución de problemas de red, errores en aplicaciones (como utilitarios de Office) y restablecimiento de cuentas bloqueadas.

Mantenimiento preventivo y correctivo de equipos:

Realización de mantenimientos preventivos planificados que incluyen limpieza de hardware y software.

Reparaciones correctivas para restaurar equipos dañados.

Gestión de impresoras:

Mantenimiento preventivo y correctivo de dispositivos de impresión institucional.

Coordinación del servicio de impresión institucional para garantizar su operatividad.

Coordinación con proveedores:

Gestión de garantías y mantenimiento de equipos mediante contratos con proveedores externos.

Enlace entre los usuarios y proveedores para el trámite de garantías.

Elaboración de informes técnicos:

Generación de informes para dar de baja equipos obsoletos o dañados.

Análisis comparativo de equipos para recomendar opciones según las necesidades operativas.

Gestión de inventarios:

Mantenimiento actualizado de inventarios de hardware y software.

Coordinación con el área de Activos Fijos para registrar movimientos y custodias de equipos.

Adquisición de equipos y software:

Gestión de compras de tecnología, incluyendo hardware, licencias de software y otros recursos necesarios para la operatividad de las unidades.

Capacitación del personal:

Formación continua del equipo técnico mediante cursos y certificaciones, alineados con las exigencias institucionales y tecnológicas.

Campañas de concienciación en seguridad informática:

Organización de actividades educativas para prevenir incidentes de seguridad, como el phishing y otros ataques cibernéticos.

Gestión de solicitudes a través de diferentes canales:

Uso de plataformas como la mesa de ayuda, correo electrónico y teléfono para recibir y atender solicitudes de los usuarios.

Gestión de políticas de acceso y seguridad:

Implementación de políticas para asignar perfiles de usuarios con accesos mínimos necesarios.

Aplicación de medidas de seguridad en equipos finales, como la instalación de antivirus actualizados.

Protocolo de manejo de crisis tecnológicas:

Respuesta a problemas críticos como interrupciones de internet, fallos en servicios de data centers y sistemas de correo electrónico institucional.

3.2 PRIORIZACIÓN DE LOS SERVICIOS

En el ámbito del soporte técnico, resulta fundamental establecer un sistema de priorización de tareas, dado el volumen significativo de solicitudes y requerimientos que se presentan de manera cotidiana. Para abordar esta demanda de manera eficiente, se han implementado criterios internos de priorización que permiten atender las solicitudes en función de su relevancia y urgencia.

Los criterios de priorización que se aplican en el área de soporte técnico son los siguientes:

Impacto en la continuidad operativa del negocio: Aquellos problemas que impiden que un usuario o área estratégica de la organización pueda llevar a cabo sus funciones de manera efectiva se clasifican como de alta prioridad, dado que afectan directamente la operatividad y productividad de la institución.

Jerarquía del usuario: Las solicitudes provenientes de usuarios con roles de mayor relevancia dentro de la estructura organizacional, tales como el Rectorado, Vicerrectorado o Consejo Directivo, reciben prioridad sobre las de otros usuarios, en función de su impacto en la toma de decisiones y en la gestión institucional.

Gravedad del problema: Los incidentes que afectan a un número significativo de usuarios o que comprometen el funcionamiento de sistemas críticos, como servidores, redes o aplicaciones esenciales, son considerados prioritarios debido a su alcance y potencial impacto en la infraestructura tecnológica de la organización.

Tiempo de resolución: Aquellos problemas que pueden ser resueltos de manera rápida y eficiente, como el restablecimiento de contraseñas o la solución de incidencias menores, suelen priorizarse sobre tareas que requieren un proceso más extenso, como la instalación de nuevos sistemas o la implementación de mejoras tecnológicas.

3.3 RESULTADOS Y ANÁLISIS

Una vez identificados los servicios que brinda el equipo de soporte técnico en el área de Tecnologías de la Información (TI), así como los criterios establecidos para priorizar las solicitudes y requerimientos, es posible realizar una categorización detallada de dichos servicios en función de su nivel de prioridad. Esta clasificación permite una gestión más eficiente de los recursos disponibles, asegurando que las incidencias y solicitudes sean atendidas de acuerdo con su

impacto en la operatividad de la organización y la jerarquía de los usuarios involucrados.

A continuación, se presenta una categorización de los servicios ofrecidos por el departamento de soporte técnico, organizados según su nivel de prioridad:

Servicios Críticos (Alta Prioridad)

Esta categoría comprende aquellos servicios que requieren una atención inmediata debido a su impacto en la continuidad operativa de la institución o en el desempeño de áreas estratégicas. La demora en su resolución puede ocasionar interrupciones significativas en las actividades organizacionales.

Incidentes que requieren atención inmediata:

- Fallas en equipos de cómputo que impiden su encendido o arranque.
- Problemas de conectividad en la red institucional (internet o intranet).
- Fallos en servidores o data centers que afectan a múltiples usuarios.
- Disrupciones en aplicaciones críticas, tales como sistemas de gestión documental, correo electrónico, Office 365 o Quipux.
- Interrupción en el servicio de impresión institucional.

Usuarios prioritarios:

- Rectorado, Vicerrectorado, Consejo Politécnico y demás unidades de alto nivel jerárquico.
- Directivos, gerentes y otros usuarios clave cuya labor impacta la toma de decisiones organizacionales.

Servicios Urgentes (Media Prioridad)

Los servicios clasificados en esta categoría, aunque no críticos, requieren resolución en un tiempo razonable, ya que afectan la productividad de los usuarios y dificultan la realización de sus actividades diarias.

- Problemas que afectan la productividad:

- Fallos en aplicaciones utilitarias (ejemplo: Microsoft Word, Excel, entre otros).
- Instalación de sistemas operativos o software esencial para el desarrollo de tareas laborales.
- Incidentes relacionados con periféricos (teclados, monitores, impresoras personales, etc.).
- Bloqueo de cuentas de usuario y solicitudes de restablecimiento de contraseñas.

Usuarios:

- Personal administrativo y operativo cuya labor se ve comprometida por la incidencia reportada.

Servicios Rutinarios (Baja Prioridad)

Esta categoría incluye solicitudes que no afectan directamente la operatividad institucional y que pueden ser atendidas en un plazo mayor sin comprometer la productividad del usuario.

Solicitudes de mejoras e instalaciones adicionales:

- Instalación de software no crítico o de uso complementario.
- Creación de accesos directos, iconos en el escritorio o plantillas personalizadas.
- Asesoría técnica en procesos de adquisición de hardware o software.
- Programación y ejecución de mantenimiento preventivo.
- Actas de entrega recepción de bienes tecnológicos a usuarios.

Usuarios:

- Cualquier usuario que requiera asistencia para mejoras o instalaciones sin carácter de urgencia.

Servicios de Mantenimiento y Gestión (Prioridad Programada)

Corresponde a tareas de mantenimiento y gestión de los recursos tecnológicos, programadas de manera periódica para garantizar la operatividad y disponibilidad de los equipos y sistemas.

Mantenimiento correctivo y preventivo:

- Ejecución de limpieza y optimización de hardware y software.
- Reparación de equipos dañados.
- Coordinación de procesos de garantía con proveedores.
- Mantenimiento preventivo de dispositivos de impresión y otros periféricos.

Gestión de inventarios y compras:

- Actualización y control del inventario de hardware y software.
- Gestión de adquisiciones tecnológicas, incluyendo licencias de software y equipos de cómputo.
- Elaboración de informes técnicos para la baja de equipos obsoletos o dañados que ya no son de utilidad para la institución.

Servicios de Seguridad y Concientización (Prioridad Preventiva)

Esta categoría engloba servicios destinados a la protección de la infraestructura tecnológica y a la concienciación del usuario sobre buenas prácticas en ciberseguridad.

Medidas de seguridad:

- Implementación de técnicas de hardening en equipos informáticos (restricción de acceso a BIOS, configuración de permisos, entre otros).
- Instalación, actualización y monitoreo de software antivirus.

- Gestión de perfiles de usuario, evitando concesión innecesaria de privilegios administrativos.

Concienciación y respuesta ante incidentes:

- Desarrollo de campañas educativas para la prevención de ataques de ingeniería social (ejemplo: phishing).
- Implementación de protocolos de respuesta ante incidentes de seguridad, incluyendo bloqueo de cuentas comprometidas y procedimientos para restablecimiento de credenciales.

La identificación y categorización de los principales servicios de soporte técnico de la unidad de tecnología de la universidad permite comprender el alcance y la importancia de las funciones desempeñadas en este ámbito. A través de un análisis detallado, se ha establecido que el equipo de soporte técnico no solo responde a incidencias y requerimientos de los usuarios, sino que también desempeña un papel clave en la gestión de mantenimiento, adquisición de tecnología, coordinación con proveedores y fortalecimiento de la seguridad informática.

Asimismo, la priorización de los servicios según su impacto operativo y urgencia contribuye a la optimización de los recursos, garantizando que las incidencias críticas sean atendidas con la inmediatez requerida, mientras que los servicios rutinarios y programados se gestionen de manera eficiente sin comprometer la continuidad del negocio. Este enfoque estructurado no solo mejora la calidad del servicio brindado, sino que también permite establecer estrategias de mejora continua que respondan a la evolución de las necesidades tecnológicas de la universidad.

En definitiva, el análisis desarrollado en este capítulo sienta las bases para la implementación de políticas y controles más eficientes en la gestión del soporte

técnico, asegurando una respuesta oportuna a los incidentes, un uso adecuado de los recursos tecnológicos y la adopción de medidas preventivas para mitigar riesgos en el entorno digital institucional.

CAPÍTULO IV

ANÁLISIS DE RIESGOS EN LOS SERVICIOS CRÍTICOS DE SOPORTE TÉCNICO DE LA UNIDAD DE TECNOLOGÍA DE LA INSTITUCIÓN DE EDUCACIÓN SUPERIOR

4.1 IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN

Con base en los resultados del análisis desarrollado en la sección 3.3, se han identificado los siguientes activos de información presentes en el área de soporte técnico de la institución pública:

Infraestructura Tecnológica

- Equipos de cómputo: PCs, laptops, AIO y estaciones de trabajo utilizadas por los usuarios.
- Dispositivos periféricos: Impresoras, teclados, monitores, escáneres y otros dispositivos de cómputo.

Sistemas de Información y Aplicaciones

- Sistema de gestión documental (almacenamiento y flujo de documentos oficiales). Correo electrónico (Office 365, Quipux).
- Software administrativo (Microsoft Word, Excel, Power point, entre otros).
- Aplicaciones de seguridad: Software antivirus y antimalware (Consola de administración del antivirus ESET PROTECT).
- Aplicaciones de escritorio: (Sistemas Financieros, contables, Talento humano, sistema académico, entre otros)
- Plataformas de gestión de usuarios: Control de acceso a cuentas y perfiles de usuarios tanto de dominio como locales.
- Sistemas de restablecimiento de contraseñas y bloqueo de cuentas (desbloqueo a través de PowerShell para usuarios que se encuentran enrolados al dominio de la institución.)

Datos y Documentación

- Informes técnicos: Documentos sobre mantenimiento, adquisiciones y bajas de equipos.
- Inventarios de hardware y software: Registro de activos tecnológicos.
- Actas de entrega-recepción: Documentación formal de asignación de equipos a usuarios.

Recursos Humanos y Concienciación

- Personal de soporte TI: Encargados de mantenimiento y gestión tecnológica.
- Campañas de concienciación: Información educativa sobre seguridad informática y prevención de ataques.

4.2 ANÁLISIS DE VULNERABILIDADES Y AMENAZAS

El análisis de vulnerabilidades y amenazas en este contexto permitirá identificar los posibles puntos débiles en los servicios críticos de soporte técnico, así como las amenazas que podrían comprometer la seguridad de la información y la continuidad operativa. Para este análisis, se han considerado los siguientes aspectos:

4.2.1 VULNERABILIDADES

Las vulnerabilidades detectadas en los servicios de soporte técnico incluyen:
Infraestructura tecnológica desactualizada.

Falta de procedimientos documentados: Ausencia de protocolos estandarizados para la gestión de incidencias y solicitudes.

Gestión ineficiente de credenciales: Uso compartido de cuentas administrativas y contraseñas débiles. (Creación de usuarios dominios con perfiles de administrador)

Falta de controles de acceso: Acceso no restringido a información crítica dentro del área de soporte. (Uso indebido de Anydesk, Team Viewer, uso de credenciales genéricas o contraseñas débiles)

Capacitación insuficiente: Falta de formación en ciberseguridad para el personal técnico.

4.2.2 AMENAZAS

Las principales amenazas que pueden impactar la seguridad en los servicios brindados por soporte técnico incluyen:

AMENAZAS EXTERNAS

Ataques de malware y ransomware: Programas maliciosos diseñados para cifrar, robar o destruir datos críticos.

Ataques de phishing y suplantación de identidad: Intentos de engaño a los usuarios para obtener credenciales de acceso.

Intrusiones y explotación de vulnerabilidades: Actores maliciosos aprovechando brechas de seguridad en el software y hardware.

Negación de servicio (DoS/DDoS): Saturación de la infraestructura tecnológica, impidiendo su correcto funcionamiento.

AMENAZAS INTERNAS

Accesos no autorizados: Intentos de intrusión por parte de actores internos y externos.

Errores humanos: Configuraciones incorrectas, eliminación accidental de datos o negligencia en el manejo de información sensible.

Fallas en la infraestructura: Problemas de hardware, cortes eléctricos y fallos en la red que afectan la disponibilidad del servicio.

Uso inadecuado de recursos tecnológicos: Instalación de software no autorizado, uso indebido de internet y dispositivos externos.

4.2.3 VULNERABILIDADES Y AMENAZAS EN LOS SERVICIOS DEL ÁREA DE SOPORTE TÉCNICO

Con base en los activos de información identificados en la sección 4.1 del presente trabajo, se procede a utilizar el software PILAR como herramienta de apoyo para el análisis y la gestión de riesgos en los sistemas de información.

El software PILAR es una herramienta especializada en el análisis de riesgos de seguridad informática, que permite identificar, valorar y gestionar amenazas sobre activos de información. Está orientado a facilitar el cumplimiento de normas internacionales como la ISO/IEC 27001, automatizando la identificación de vulnerabilidades y proponiendo controles adecuados para mitigar los riesgos [21].

Figura 2 *Ingreso de los activos de información en el software pilar*

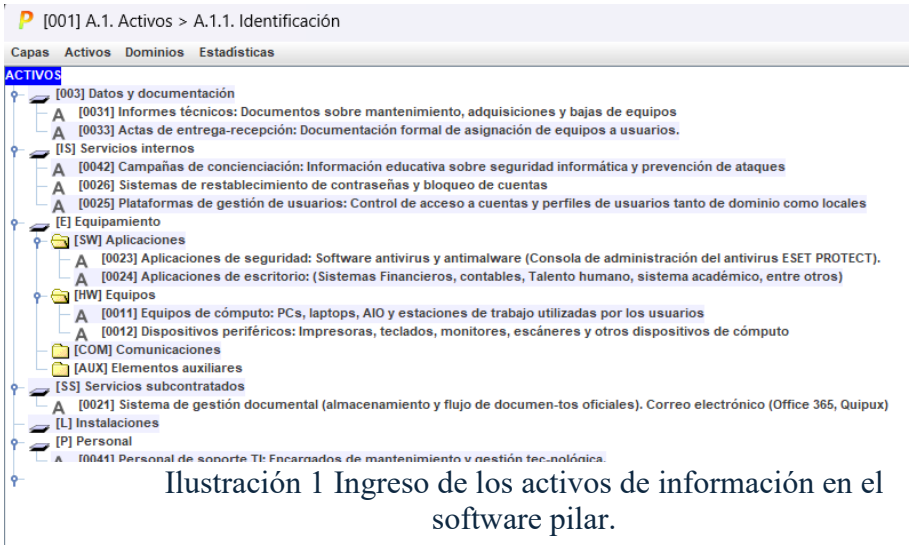
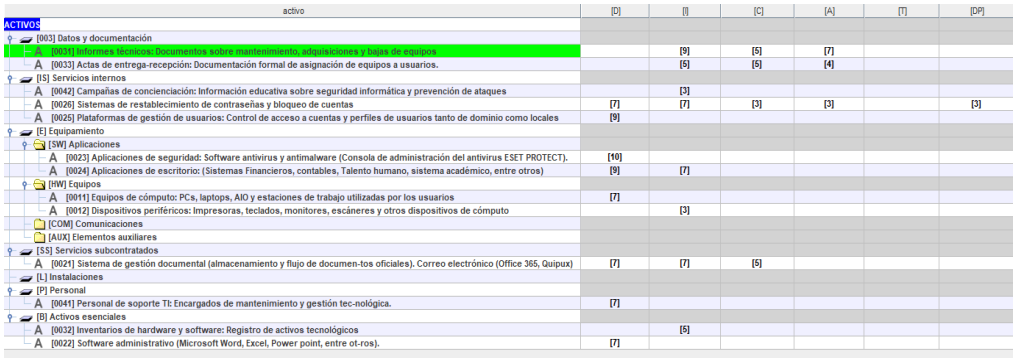


Ilustración 1 Ingreso de los activos de información en el software pilar.

Una vez los activos de información han sido ingresados se procede a realizar la valoración de los activos. Para realizar la valorización se toman en cuenta los siguientes criterios: confidencialidad, integridad, disponibilidad, autenticidad de los usuarios y de la información y por último datos personales.

Figura 3 *Valoración de los activos*



activo	[D]	[I]	[C]	[A]	[T]	[DP]
ACTIVOS						
[003] Datos y documentación						
[0031] Informes técnicos: Documentos sobre mantenimiento, adquisiciones y bajas de equipos		[9]	[5]	[7]		
[0033] Actas de entrega-recepción: Documentación formal de asignación de equipos a usuarios.		[5]	[5]	[4]		
[IS] Servicios internos						
[0042] Campañas de concienciación: Información educativa sobre seguridad informática y prevención de ataques		[3]				
[0026] Sistemas de restablecimiento de contraseñas y bloqueo de cuentas	[7]	[7]	[3]	[3]		[3]
[0025] Plataformas de gestión de usuarios: Control de acceso a cuentas y perfiles de usuarios tanto de dominio como locales	[9]					
[E] Equipamiento						
[SW] Aplicaciones						
[0023] Aplicaciones de seguridad: Software antivirus y antimalware (Consola de administración del antivirus ESET PROTECT).	[10]					
[0024] Aplicaciones de escritorio: (Sistemas Financieros, contables, Talento humano, sistema académico, entre otros)	[9]	[7]				
[HW] Equipos						
[0011] Equipos de cómputo: PCs, laptops, AIO y estaciones de trabajo utilizadas por los usuarios	[7]					
[0012] Dispositivos periféricos: Impresoras, teclados, monitores, escáneres y otros dispositivos de cómputo		[3]				
[COM] Comunicaciones						
[AUX] Elementos auxiliares						
[SS] Servicios subcontratados						
[0021] Sistema de gestión documental (almacenamiento y flujo de documen-tos oficiales). Correo electrónico (Office 365, Quipux)	[7]	[7]	[5]			
[L] Instalaciones						
[P] Personal						
[0041] Personal de soporte TI: Encargados de mantenimiento y gestión tec-nológica.	[7]					
[B] Activos esenciales						
[0032] Inventarios de hardware y software: Registro de activos tecnológicos		[5]				
[0022] Software administrativo (Microsoft Word, Excel, Power point, entre ot-ros).	[7]					

Una vez completada la valorización de los activos el software pilar nos brinda una lista de amenazas por cada categoría de activos que se definieron anteriormente.

Figura 4 *Amenazas en datos y documentación*

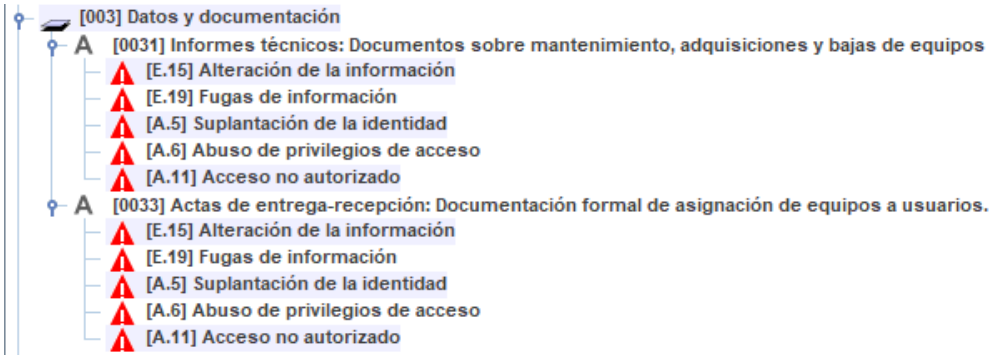


Figura 5 *Amenazas en servicios internos*

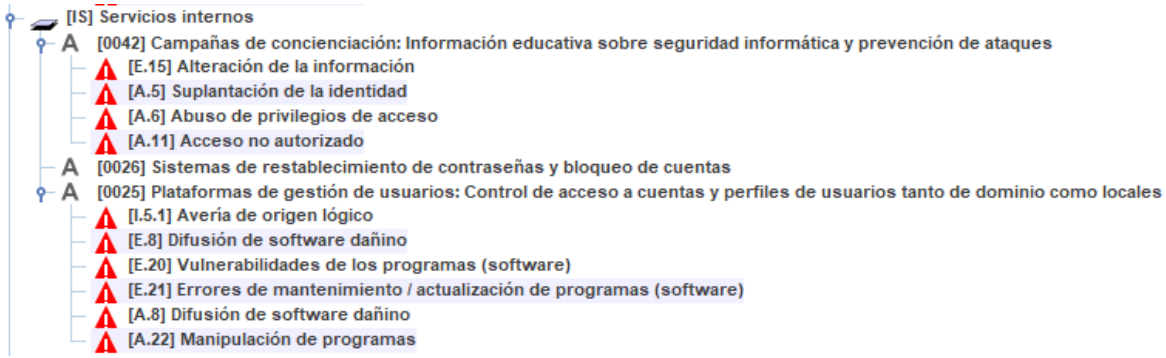


Figura 6 *Amenazas en equipamiento*

Figura 7 *Amenazas en servicios subcontratados*

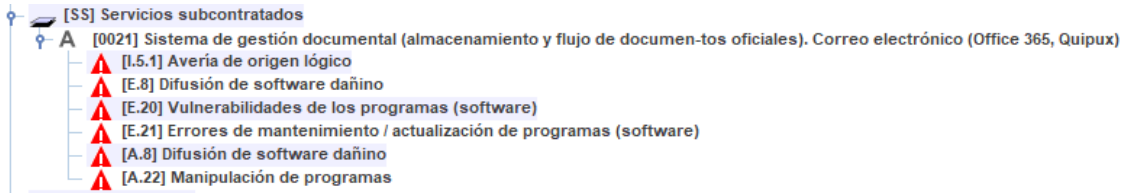


Figura 8 *Amenazas en personal*

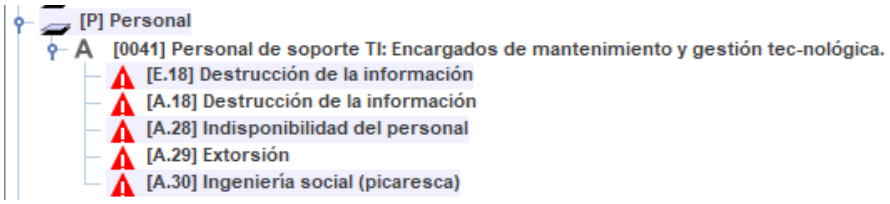
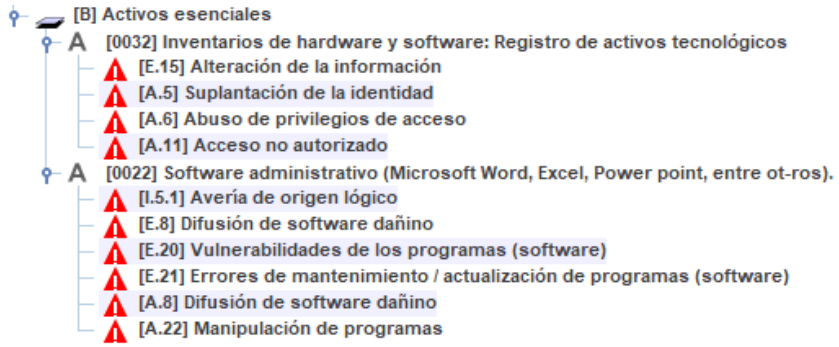


Figura 9 *Amenazas en activos esenciales*



A continuación, se presenta una tabla que detalla las vulnerabilidades y amenazas identificadas en los servicios proporcionados por el área de soporte técnico a los usuarios de la IES (institución de educación superior). Se toma como base las amenazas presentadas por el software pilar.

Tabla 1 *Amenazas y vulnerabilidades identificados en el área de soporte técnico*

Activos de información	Vulnerabilidades		Amenazas	
	Vulnerabilidad	Descripción	Amenaza	Descripción
Equipos de cómputo: PCs, laptops, AIO y estaciones de trabajo utilizadas por los usuarios.	Falta de actualizaciones y parches de seguridad.	Los equipos que ejecutan versiones desactualizadas de sistemas operativos y software son	Explotación de vulnerabilidades conocidas	Un atacante puede aprovechar fallos de seguridad ya identificados en sistemas desactualizados para ejecutar

		vulnerables a exploits conocidos.		código malicioso, obtener acceso no autorizado o comprometer la integridad, confidencialidad y disponibilidad de los datos
	Uso de configuraciones predeterminadas inseguras	Muchos equipos conservan configuraciones de fábrica.	Acceso no autorizado	Los atacantes pueden explotar configuraciones predeterminadas inseguras, como contraseñas por defecto o permisos excesivos
	Falta de autenticación multifactor (MFA)	Sin esta capa adicional de seguridad, el acceso a sistemas críticos se vuelve más vulnerable a ataques de fuerza bruta.		
	Desactivación de firewalls y protección antivirus	Algunos usuarios deshabilitan estas medidas de seguridad, dejando los equipos expuestos a amenazas.	Infección por malware	La desactivación de firewalls y protección antivirus permite que malware, ransomware u otras amenazas ingresen y se propaguen en el sistema sin ser detectadas, comprometiendo la seguridad y la integridad de los datos.
	Instalación de software no autorizado	La ejecución de programas descargados de fuentes no verificadas puede introducir malware y otras amenazas		
	Ejecución de archivos o enlaces sospechosos	Apertura de correos electrónicos o archivos adjuntos maliciosos que comprometen la seguridad del sistema.		

	Uso de dispositivos USB no seguros	Permite la propagación de malware cuando se insertan en equipos infectados		
	Uso de contraseñas débiles o reutilizadas	Facilita accesos no autorizados en caso de filtraciones de credenciales.	Ataques de denegación de servicio (DDoS) mediante botnets	Equipos comprometidos pueden ser utilizados para realizar ataques contra redes externas.
	Acceso físico no autorizado	La ausencia de mecanismos de control (bloqueo de sesión, almacenamiento seguro) permite que terceros manipulen los equipos.	Manipulación de dispositivos.	Un intruso puede acceder, modificar o robar información directamente desde los equipos
	Excesivos privilegios de usuario	Conceder derechos administrativos sin necesidad aumenta la posibilidad de errores humanos o ataques internos.	Escalamiento de privilegios.	Usuarios con permisos innecesarios pueden realizar acciones no autorizadas, intencionadas o accidentales.
	Riesgo de robo o extravío	Equipos portátiles y dispositivos de almacenamiento sin cifrado pueden ser robados y la información comprometida	Pérdida de datos sensibles.	Equipos perdidos o robados pueden contener información confidencial que podría ser accedida sin protección adecuada.
	Falta de cifrado en discos duros	La información almacenada sin cifrado es accesible fácilmente en caso de pérdida	Exposición de datos.	Información almacenada puede ser fácilmente accesible si el dispositivo cae en manos no autorizadas.

		o robo del equipo.		
Dispositivos periféricos: Impresoras, teclados, monitores, escáneres y otros dispositivos de cómputo.	Intercepción de datos en monitores y teclados inalámbricos	Dispositivos con conexiones Bluetooth o RF sin cifrar pueden ser espiados.	Robo de información.	Un atacante puede capturar datos sensibles transmitidos entre dispositivos inalámbricos sin cifrado, como contraseñas o contenido visualizado.
	Ataques de denegación de servicio (DoS) en periféricos	Un atacante puede enviar paquetes maliciosos a un dispositivo para deshabilitarlo o sobrecargar su funcionalidad	Interrupción de servicios.	Un atacante puede sobrecargar dispositivos periféricos, dejándolos inutilizables y afectando las operaciones de la red o del sistema.
	Acceso no autorizado a impresoras y escáneres en red	Muchos modelos no tienen autenticación y permiten que cualquier usuario acceda a documentos almacenados en la memoria del dispositivo	Exposición de documentos sensibles.	Usuarios no autorizados pueden recuperar o manipular documentos almacenados o enviados a dispositivos en red.
	Exposición a polvo, humedad o temperaturas extremas	Puede afectar el rendimiento y provocar fallos en dispositivos críticos.	Daño físico y fallos operativos.	Condiciones ambientales adversas pueden deteriorar los componentes de los dispositivos.
	Mantenimiento inadecuado	La falta de revisiones periódicas puede generar fallos en impresoras, escáneres, teclados, monitores, etc afectando la disponibilidad de servicios.	Degradación del rendimiento.	La falta de mantenimiento puede generar fallos en los dispositivos periféricos.

	Cableado desordenado o accesible	Permite la manipulación o desconexión intencional de dispositivos periféricos.	Manipulación o desconexión no autorizada.	Cables accesibles pueden ser manipulados intencionadamente o desconectados accidentalmente.
Sistema de gestión documental (almacenamiento y flujo de documentos oficiales). Correo electrónico (Office 365, Quipux).	Falta de cifrado en la transmisión y almacenamiento de documentos sensibles.	La ausencia de mecanismos de cifrado en la transmisión y almacenamiento de documentos sensibles expone la información a posibles ataques. Un atacante con acceso a la red o al sistema de almacenamiento puede interceptar, modificar o extraer datos confidenciales sin ser detectado.	Instalación de un plugin malicioso en el sistema de gestión documental	Existe la posibilidad de que un usuario descargue e instale un plugin malicioso para la lectura de archivos PDF en el sistema de gestión documental, como Quipux. Este software malintencionado podría ejecutar acciones no autorizadas, como la exfiltración de información confidencial, la alteración de documentos o la introducción de malware en la infraestructura del sistema.
	Acceso no autorizado	personas no autorizadas obtienen acceso a sistemas, documentos o correos electrónicos	Exposición o robo de información confidencial	Personas no autorizadas (como atacantes externos, empleados malintencionados o terceros) pueden acceder a sistemas, documentos o correos electrónicos que contienen información sensible

	Configuración inadecuada de filtros antispam y antimalware	Si los filtros de seguridad no están bien configurados, pueden permitir la entrega de correos maliciosos con enlaces fraudulentos o archivos infectados.	Distribución de malware a través de correos electrónicos	Un atacante puede adjuntar archivos maliciosos en correos electrónicos, lo que podría infectar equipos dentro de la red universitaria y comprometer sistemas internos.
	Uso de contraseñas débiles o reutilizadas	Si los usuarios utilizan contraseñas cortas, predecibles o las mismas en múltiples servicios, los atacantes pueden adivinarlas fácilmente mediante ataques de fuerza bruta o diccionario. Además, si una credencial filtrada en otro servicio se reutiliza en Outlook, puede ser explotada en ataques de credential stuffing.	Compromiso de cuentas por ataques de fuerza bruta o credential stuffing	Los atacantes pueden utilizar herramientas automatizadas para probar combinaciones de usuario y contraseña hasta encontrar credenciales válidas.

Administración de aplicaciones de seguridad: Software antivirus y antimalware (Consola de administración del antivirus ESET PROTECT).	Falta de monitoreo y alertas en la consola de administración	Si no se activan notificaciones de seguridad en la consola, los administradores pueden tardar en detectar infecciones, fallos en las actualizaciones o equipos sin protección activa.	Propagación de malware sin detección temprana	Sin un monitoreo efectivo, un malware podría extenderse en la infraestructura universitaria antes de que el equipo de seguridad lo identifique y responda, causando daños graves.
	Falta de actualizaciones del software antivirus y bases de datos de firmas	Si los equipos no reciben actualizaciones regulares del software y las firmas de virus, la protección contra amenazas emergentes se vuelve inefectiva, dejando expuestos a los sistemas.	Ataques de malware de día cero o variantes recientes	Un atacante podría aprovechar vulnerabilidades de software recientes o malware no detectado por bases de datos desactualizadas para infectar sistemas antes de que haya parches disponibles.
	Configuración inadecuada de la consola de administración (ESET PROTECT)	Si la consola de administración no está bien configurada, los administradores podrían no tener control total sobre los endpoints protegidos. Configuraciones débiles pueden permitir que ciertos equipos no reciban actualizaciones o que la protección en tiempo real esté deshabilitada.	Infección masiva por malware debido a protección inefectiva	Un atacante podría explotar la falta de actualizaciones o configuraciones deficientes del antivirus para propagar malware dentro de la red comprometiendo datos y sistemas críticos.

Instalación de aplicaciones de escritorio: (Sistemas Financieros, contables, Talento humano, sistema académico, entre otros)	Uso de versiones desactualizadas o sin parches de seguridad	Las versiones antiguas de software pueden contener vulnerabilidades conocidas que no han sido corregidas	Explotación de vulnerabilidades conocidas	Pueden ser blanco de ataques que aprovechan fallos ya documentados y sin corregir.
Plataformas de gestión de usuarios: Control de acceso a cuentas y perfiles de usuarios tanto de dominio como locales.	Falta de monitoreo y auditoría de accesos	Si no se registran los accesos y acciones en la gestión de usuarios, es difícil detectar actividades sospechosas o accesos indebidos.	Persistencia de atacantes dentro de la infraestructura universitaria	Un atacante que obtiene acceso al dominio podría permanecer en la red sin ser detectado por largos periodos, usando cuentas legítimas para evadir controles de seguridad.
	Sincronización de cuentas con servicios externos sin control de seguridad	Integración de Active Directory con plataformas como Google Workspace, Moodle o sistemas administrativos, lo que puede generar vulnerabilidades si la sincronización de credenciales no está bien asegurada.	Acceso no autorizado a múltiples servicios tras comprometer una cuenta	Un atacante que obtiene acceso a una cuenta en Active Directory podría usarla para ingresar automáticamente a otras plataformas vinculadas, aumentando el impacto del ataque.
Sistemas de restablecimiento de contraseñas y bloqueo de cuentas (desbloqueo a través de PowerShell para usuarios que se encuentran enrolados al dominio de la institución.)	Uso indebido de scripts de PowerShell sin restricciones	Los scripts utilizados para desbloquear cuentas pueden ejecutarse sin controles, permitiendo que cualquier usuario con acceso a la herramienta pueda manipular las cuentas del dominio.	Ejecución de comandos no controlados	Los scripts utilizados para desbloquear cuentas pueden ser manipulados o ejecutados sin autorización, permitiendo la alteración de credenciales o accesos dentro del dominio.

	Configuración inadecuada de políticas de bloqueo de cuentas	Si los bloqueos no están bien configurados, se pueden generar bloqueos recurrentes o facilitar el desbloqueo sin controles efectivos.	Bloqueo excesivo o insuficiente de cuentas	Si las cuentas se bloquean con demasiada facilidad, los usuarios pueden experimentar interrupciones frecuentes; si el bloqueo es insuficiente, se permite intentos repetidos de acceso sin control.
	Posibilidad de ataques de fuerza bruta o repetidos intentos de autenticación	Si el sistema permite múltiples intentos de autenticación sin penalización o registro, se pueden probar combinaciones de credenciales hasta encontrar la correcta.	Explotación de intentos de autenticación ilimitados	Si el sistema no restringe la cantidad de intentos fallidos, un atacante podría probar múltiples combinaciones de credenciales hasta obtener acceso.
	Falta de procedimientos de verificación antes del desbloqueo de cuentas	No contar con un protocolo de validación de identidad antes de desbloquear cuentas puede permitir el restablecimiento de contraseñas sin confirmar la legitimidad de la solicitud.	Restablecimiento de contraseñas sin validación de identidad	se pueden realizar modificaciones sin comprobar su autenticidad.
Elaboración de informes técnicos: Documentos sobre mantenimiento, adquisiciones y bajas de equipos.	Modificación no autorizada	Sin controles de integridad, los informes podrían ser alterados maliciosamente, afectando la toma de decisiones.	Alteración de la información,	Toma de decisiones erróneas, fraude o pérdida de confianza en la veracidad de los informes.
	Divulgación indebida	Envío accidental de informes a destinatarios incorrectos, comprometiendo información sensible.	Exposición de información sensible	Fugas de datos, incumplimiento normativo o uso indebido de la información.

Elaboración de inventarios de hardware y software: Registro de activos tecnológicos.	Falta de actualización y precisión en el inventario	Si el inventario no se mantiene actualizado, se pueden perder registros de dispositivos obsoletos o nuevos activos no documentados.	Pérdida de control sobre los activos tecnológicos	Activos obsoletos o desconocidos pueden quedar expuestos a vulnerabilidades sin protección.
	Falta de monitoreo y alertas sobre cambios en el inventario	La ausencia de herramientas de monitoreo automático puede hacer que los cambios no autorizados en los activos pasen desapercibidos.	Instalación de hardware o software malicioso sin detección	Atacantes internos o externos podrían introducir dispositivos o aplicaciones maliciosas sin que la organización lo note a tiempo.
	No identificación de dispositivos vulnerables o en desuso	Si el inventario no refleja firmware desactualizado o sistemas sin soporte (como Windows 7 u otros SO obsoletos), estos pueden ser explotados por atacantes.	Explotación de sistemas sin soporte o con vulnerabilidades conocidas	Los ciberdelincuentes pueden aprovechar vulnerabilidades en dispositivos no actualizados o en desuso para infiltrarse en la red.
	No gestionar la baja segura de activos	Los dispositivos retirados sin un proceso seguro pueden contener datos sensibles recuperables por atacantes.	Fuga de información por recuperación de datos en dispositivos retirados	Dispositivos desechados sin un borrado seguro pueden contener datos sensibles que pueden ser recuperados por terceros malintencionados.
	Uso de software sin licencia o no autorizado	Si el inventario no identifica software sin licencia, podría haber incumplimientos legales y exposición a acciones legales o multas	Riesgo legal y puertas traseras	Software pirata o no autorizado puede incluir malware, además de exponer la organización a sanciones legales.

	Falta de seguimiento y auditoría de los equipos asignados	No existen procedimientos claros para monitorear y verificar periódicamente el estado de los equipos entregados, lo que dificulta conocer su ubicación y uso actual.	Pérdida o extravío de dispositivos sin detección	Los equipos asignados pueden cambiar de ubicación o de usuario sin que se registre adecuadamente, dificultando su rastreo y administración.
	No revocar accesos ni recuperar equipos al finalizar la asignación	Cuando un usuario deja de utilizar un equipo, no se aplican procesos para asegurar que este sea devuelto ni que sus accesos sean revocados, permitiendo un uso no controlado del dispositivo.	Uso continuado de dispositivos por personas no autorizadas	Los usuarios que ya no deberían tener acceso a los equipos pueden seguir utilizándolos sin restricciones.
	Falta de trazabilidad en la asignación de equipos	No se mantiene un registro detallado y actualizado sobre qué usuario tiene asignado cada equipo, dificultando el seguimiento en caso de auditorías o incidentes.	Dificultad para identificar responsables en incidentes	No se puede determinar con precisión qué persona tiene asignado un equipo en un momento específico.
	No incluir información detallada del equipo en el acta	Las actas no especifican características clave del equipo entregado, como número de serie, modelo o configuraciones, lo que complica su identificación y administración	Confusión o fraude en la gestión de activos	Los dispositivos pueden ser intercambiados, reemplazados o reportados incorrectamente sin una referencia clara en la documentación.

		dentro del inventario.		
Personal de soporte TI: Encargados de mantenimiento y gestión tecnológica.	Accesos privilegiados sin control adecuado	El personal de soporte TI posee permisos avanzados en los sistemas, lo que les permite realizar configuraciones, cambios y modificaciones sin restricciones específicas.	Uso indebido de privilegios	Las cuentas con permisos elevados pueden ser utilizadas para realizar modificaciones en sistemas, acceder a información confidencial o alterar configuraciones sin restricciones.
	Falta de capacitación en seguridad informática	El equipo de soporte TI puede no contar con formación continua en ciberseguridad, actualizaciones de amenazas o mejores prácticas en la protección de información.	Aplicación de prácticas inadecuadas	El desconocimiento de procedimientos actualizados en ciberseguridad puede llevar a la implementación de medidas insuficientes o la omisión de controles esenciales.
	Exposición a ataques de ingeniería social	Los técnicos pueden ser contactados por actores externos o internos que buscan obtener información o acceso mediante manipulación psicológica.	Obtención de información mediante manipulación	Las personas con acceso a sistemas críticos pueden ser persuadidas para proporcionar datos o realizar acciones bajo pretextos engañosos.
	Falta de compromiso o participación	Si los empleados no toman en serio las campañas de concienciación o no participan activamente, el	Comportamientos inseguros y aumento del riesgo de brechas de seguridad	La falta de compromiso o participación puede llevar a seguir practicas inseguras en el entorno tecnológico.

		mensaje no será internalizado.		
	Falta de seguimiento y evaluación	Si no se mide la efectividad de las campañas, no se puede saber si los empleados están aplicando lo aprendido.	Mantenimiento de un bajo nivel de conciencia y preparación	Probabilidad de que se apliquen correctamente las medidas de seguridad, aumentando la vulnerabilidad a ataques como phishing o ingeniería social.

4.3 CATEGORIZACIÓN, EVALUACIÓN Y TRATAMIENTO DE RIESGOS

4.3.1 CATEGORIZACIÓN DE RIESGOS

Para llevar a cabo la categorización de riesgos, conforme a las vulnerabilidades y amenazas descritas en el apartado anterior del presente trabajo, se empleará una matriz de riesgos de tipo 5x5. En dicha matriz se establecerán tanto la probabilidad como el impacto asociado a cada vulnerabilidad.

Antes de la matriz de riesgos se definirán las escalas de probabilidad e impacto.

ESCALA DE PROBABILIDAD

La escala de probabilidad se define con cinco niveles que se detallan en la tabla que se muestra a continuación:

Tabla 2 *Escala de probabilidad*

Probabilidad		
Definición	valor	Descripción
Muy alta	5	Altamente probable
Alta	4	Probabilidad significativa
Media	3	probabilidad ocasional
Baja	2	Poco probable
Muy baja	1	Altamente improbable

ESCALA DE IMPACTO

La escala de impacto se define con cinco niveles que se detalla en la tabla que se muestra a continuación:

Tabla 3 *Escala de impacto*

Impacto		
Definición	Valor	Descripción
Muy alto	5	Interrupción total de servicios críticos. Pérdidas económicas significativas. Daño reputacional institucional.
Alto	4	Afecta de manera considerable la operación de procesos clave. Pérdidas económicas relevantes. Retrasos significativos en el cumplimiento de objetivos.
Medio	3	Afectación parcial de procesos o servicios. Costos de recuperación gestionables.
Bajo	2	Perturbaciones poco significativas. No compromete la operación general ni los activos críticos.
Muy bajo	1	Impacto insignificante o casi nulo. Efectos mínimos que se resuelven sin mayor intervención o consecuencias.

MAPA DE CALOR

Impacto / Probabilidad	Muy bajo 1	Bajo 2	Medio 3	Alto 4	Muy alto 5
Muy alta 5	5	10	15	20	25
Alta 4	4	8	12	16	20

Media 3	3	6	9	12	15
Baja 2	2	4	6	8	10
Muy baja 1	1	2	3	4	5

Se define la matriz 5x5 de riesgo con impacto probabilidad, además también se define el esquema de mapa de calor con las escalas definidas en los puntos anteriores.

VALORACIÓN DEL RIESGO

Una vez ha sido determinada la valorización de la matriz de riesgos con el impacto y la probabilidad, se define el nivel de exposición el riesgo. En el presente trabajo de titulación, se definieron cinco niveles de exposición a los riesgos y su respectiva ponderación:

Tabla 4 *valoración del riesgo de acuerdo con el mapa de calor*

Rango de valor	Nivel de riesgo	Descripción
15 - 25	Crítico	Nivel de riesgo inaceptable; demanda medidas inmediatas de mitigación o eliminación. Su ocurrencia puede tener consecuencias graves para la organización.
10 - 14	Alto	Riesgo significativo que requiere acciones específicas de control en el corto plazo.
5 - 9	Moderado	Riesgo tolerable; debe ser monitoreado y gestionado con medidas de mejora continua.
1 - 4	Bajo	Riesgo mínimo; puede ser aceptado con medidas preventivas básicas o sin intervención.

DETERMINACIÓN DEL NIVEL DE RIESGO POR EL IMPACTO Y PROBABILIDAD

En esta etapa, a cada vulnerabilidad identificada en los activos de información se le asignará una valoración correspondiente a la probabilidad de ocurrencia y al impacto potencial. Esta evaluación permitirá determinar el nivel de riesgo asociado a cada activo, facilitando así la priorización de acciones para su gestión y mitigación.

Tabla 5 *Determinación del riesgo basado en la probabilidad y el impacto*

ACTIVOS	VULNERABILIDADES	PROBABILIDAD	IMPACTO	RIESGO	Nivel de Riesgo
Equipos de cómputo: PCs, laptops, AIO y estaciones de trabajo utilizadas por los usuarios.	Falta de actualizaciones y parches de seguridad.	4	5	20	Critico
	Uso de configuraciones predeterminadas inseguras	4	4	16	Critico
	Falta de autenticación multifactor (MFA)	3	5	15	Critico
	Desactivación de firewalls y protección antivirus	3	4	12	Alto
	Instalación de software no autorizado	4	3	12	Alto
	Ejecución de archivos o enlaces sospechosos	3	4	12	Alto
	Uso de dispositivos USB no seguros	3	4	12	Alto
	Uso de contraseñas débiles o reutilizadas	5	3	15	Critico
	Acceso físico no autorizado	2	5	10	Alto
	Excesivos privilegios de usuario	3	4	12	Alto
	Riesgo de robo o extravío	3	4	12	Alto
	Falta de cifrado en discos duros	3	5	15	Critico
Dispositivos periféricos: Impresoras, teclados, monitores, escáneres y otros dispositivos de cómputo.	Intercepción de datos en monitores y teclados inalámbricos	1	4	4	Bajo
	Ataques de denegación de servicio (DoS) en periféricos	3	4	12	Alto
	Acceso no autorizado a impresoras y escáneres en red	2	3	6	Moderado
	Exposición a polvo, humedad o temperaturas extremas	3	5	15	Critico
	Mantenimiento inadecuado	2	3	6	Moderado

	Cableado desordenado o accesible	3	3	9	Moderado
Sistema de gestión documental (almacenamiento y flujo de documentos oficiales). Correo electrónico (Office 365, Quipux).	Falta de cifrado en la transmisión y almacenamiento de documentos sensibles.	4	5	20	Critico
	Acceso no autorizado	2	5	10	Alto
	Configuración inadecuada de filtros antispam y antimalware	3	5	15	Critico
	Uso de contraseñas débiles o reutilizadas	3	5	15	Critico
Administración de aplicaciones de seguridad: Software antivirus y antimalware (Consola de administración del antivirus ESET PROTECT).	Falta de monitoreo y alertas en la consola de administración	3	4	12	Alto
	Falta de actualizaciones del software antivirus y bases de datos de firmas	3	5	15	Critico
	Configuración inadecuada de la consola de administración (ESET PROTECT)	4	5	20	Critico
Instalación de aplicaciones de escritorio: (Sistemas Financieros, contables, Talento humano, sistema académico, entre otros)	Uso de versiones desactualizadas o sin parches de seguridad	3	5	15	Critico
Plataformas de gestión de usuarios: Control de acceso a cuentas y perfiles de usuarios tanto de dominio como locales.	Falta de monitoreo y auditoría de accesos	4	5	20	Critico
	Sincronización de cuentas con servicios externos sin control de seguridad	4	5	20	Critico
Sistemas de restablecimiento de contraseñas y bloqueo de cuentas (desbloqueo a través de PowerShell para usuarios que se encuentran enrolados al dominio de la institución.)	Uso indebido de scripts de PowerShell sin restricciones	3	2	6	Moderado
	Configuración inadecuada de políticas de bloqueo de cuentas	3	3	9	Moderado
	Posibilidad de ataques de fuerza bruta o repetidos intentos de autenticación	3	4	12	Alto
	Falta de procedimientos de verificación antes del desbloqueo de cuentas	3	2	6	Moderado
	Modificación no autorizada	2	3	6	Moderado

Elaboración de informes técnicos: Documentos sobre mantenimiento, adquisiciones y bajas de equipos.	Divulgación indebida	2	2	4	Bajo
Elaboración de inventarios de hardware y software: Registro de activos tecnológicos.	Falta de actualización y precisión en el inventario	2	2	4	Bajo
	Falta de monitoreo y alertas sobre cambios en el inventario	2	2	4	Bajo
	No identificación de dispositivos vulnerables o en desuso	4	5	20	Critico
	No gestionar la baja segura de activos	3	2	6	Moderado
	Uso de software sin licencia o no autorizado	4	2	8	Moderado
	Falta de seguimiento y auditoría de los equipos asignados	3	2	6	Moderado
	No revocar accesos ni recuperar equipos al finalizar la asignación	2	2	4	Bajo
	Falta de trazabilidad en la asignación de equipos	3	2	6	Moderado
	No incluir información detallada del equipo en el acta	3	2	6	Moderado
Personal de soporte TI: Encargados de mantenimiento y gestión tecnológica.	Accesos privilegiados sin control adecuado	3	3	9	Moderado
	Falta de capacitación en seguridad informática	3	2	6	Moderado
	Exposición a ataques de ingeniería social	2	2	4	Bajo
	Falta de compromiso o participación	3	2	6	Moderado
	Falta de seguimiento y evaluación	3	2	6	Moderado

4.3.2 EVALUACIÓN Y TRATAMIENTO DE RIESGOS

EVALUACIÓN DE RIESGOS

Para facilitar la comprensión, a cada sección de activos de información se le otorgará un código, de tal manera que será más fácil identificarlo al momento de realizar la priorización de riesgos.

Tabla 6 *Codificación de activos de información*

ACTIVOS DE INFORMACIÓN	CÓDIGO
Equipos de cómputo: PCs, laptops, AIO y estaciones de trabajo utilizadas por los usuarios.	AI001
Dispositivos periféricos: Impresoras, teclados, monitores, escáneres y otros dispositivos de cómputo.	AI002
Sistema de gestión documental (almacenamiento y flujo de documentos oficiales). Correo electrónico (Office 365, Quipux).	AI003
Administración de aplicaciones de seguridad: Software antivirus y antimalware (Consola de administración del antivirus ESET PROTECT).	AI004
Instalación de aplicaciones de escritorio: (Sistemas Financieros, contables, Talento humano, sistema académico, entre otros)	AI005
Plataformas de gestión de usuarios: Control de acceso a cuentas y perfiles de usuarios tanto de dominio como locales.	AI006
Sistemas de restablecimiento de contraseñas y bloqueo de cuentas (desbloqueo a través de PowerShell para usuarios que se encuentran enrolados al dominio de la institución.)	AI007
Elaboración de informes técnicos: Documentos sobre mantenimiento, adquisiciones y bajas de equipos.	AI008
Elaboración de inventarios de hardware y software: Registro de activos tecnológicos.	AI009
Personal de soporte TI: Encargados de mantenimiento y gestión tecnológica.	AI010

Con base en el nivel de riesgo obtenido en la tabla 5, el siguiente paso consiste en priorizar los riesgos identificados, de manera que se logre establecer un enfoque preciso respecto a cuáles riesgos críticos requieren atención inmediata y cuáles pueden ser gestionados en una etapa posterior.

Tabla 7 *Priorización de riesgos*

CÓDIGO ACTIVO DE INFORMACIÓN	VULNERABILIDAD	RIESGO	NIVEL DE RIESGO
AI001	Falta de actualizaciones y parches de seguridad.	20	Crítico
AI003	Falta de cifrado en la transmisión y almacenamiento de documentos sensibles.	20	Crítico
AI004	Configuración inadecuada de la consola de administración (ESET PROTECT)	20	Crítico
AI006	Falta de monitoreo y auditoría de accesos	20	Crítico
AI006	Sincronización de cuentas con servicios externos sin control de seguridad	20	Crítico
AI009	No identificación de dispositivos vulnerables o en desuso	20	Crítico
AI001	Uso de configuraciones predeterminadas inseguras	16	Crítico
AI001	Falta de autenticación multifactor (MFA)	15	Crítico
AI001	Uso de contraseñas débiles o reutilizadas	15	Crítico
AI001	Falta de cifrado en discos duros	15	Crítico
AI002	Exposición a polvo, humedad o temperaturas extremas	15	Crítico
AI003	Configuración inadecuada de filtros antispam y antimalware	15	Crítico
AI003	Uso de contraseñas débiles o reutilizadas	15	Crítico
AI004	Falta de actualizaciones del software antivirus y bases de datos de firmas	15	Crítico
AI005	Uso de versiones desactualizadas o sin parches de seguridad	15	Crítico
A001	Uso de dispositivos USB no seguros	12	Alto
AI007	Posibilidad de ataques de fuerza bruta o repetidos intentos de autenticación	12	Alto
AI001	Instalación de software no autorizado	12	Alto
AI004	Falta de monitoreo y alertas en la consola de administración	12	Alto

AI001	Desactivación de firewalls y protección antivirus	12	Alto
AI001	Ejecución de archivos o enlaces sospechosos	12	Alto
AI001	Excesivos privilegios de usuario	12	Alto
AI001	Riesgo de robo o extravío	12	Alto
AI002	Ataques de denegación de servicio (DoS) en periféricos	12	Alto
AI003	Acceso no autorizado	10	Alto
AI001	Acceso físico no autorizado	10	Alto
AI007	Configuración inadecuada de políticas de bloqueo de cuentas	9	Moderado
AI002	Cableado desordenado o accesible	9	Moderado
AI010	Accesos privilegiados sin control adecuado	9	Moderado
AI009	Uso de software sin licencia o no autorizado	8	Moderado
AI010	Falta de capacitación en seguridad informática	6	Moderado
AI009	No gestionar la baja segura de activos	6	Moderado
AI010	Falta de compromiso o participación	6	Moderado
AI009	No incluir información detallada del equipo en el acta	6	Moderado
AI009	Falta de trazabilidad en la asignación de equipos	6	Moderado
AI009	Falta de seguimiento y auditoría de los equipos asignados	6	Moderado
AI010	Falta de seguimiento y evaluación	6	Moderado
AI008	Modificación no autorizada	6	Moderado
AI007	Falta de procedimientos de verificación antes del desbloqueo de cuentas	6	Moderado
AI007	Uso indebido de scripts de PowerShell sin restricciones	6	Moderado
AI002	Acceso no autorizado a impresoras y escáneres en red	6	Moderado
AI002	Mantenimiento inadecuado	6	Moderado

AI009	Falta de monitoreo y alertas sobre cambios en el inventario	4	Bajo
AI008	Divulgación indebida	4	Bajo
AI009	No revocar accesos ni recuperar equipos al finalizar la asignación	4	Bajo
AI010	Exposición a ataques de ingeniería social	4	Bajo
AI009	Falta de actualización y precisión en el inventario	4	Bajo
AI002	Intercepción de datos en monitores y teclados inalámbricos	4	Bajo

TRATAMIENTO DE RIESGOS

Criterios de aceptación de riesgos

Con base en los riesgos priorizados en la tabla 6, se establece que aquellos clasificados con un nivel de riesgo bajo son aceptados por la IES. En contraste, los riesgos clasificados como moderados, altos o críticos no son considerados aceptables por la organización, y por tanto requieren medidas correctivas específicas.

Para los riesgos no aceptados, se procederá a un análisis detallado conforme a los lineamientos establecidos en las normas ISO/IEC 2700, con el objetivo de determinar los controles más adecuados para su tratamiento. La descripción detallada de dichos controles será presentada en el Capítulo 5 del presente documento.

Tabla 8 *Criterios para aceptación de riesgos*

Nivel de riesgo	Rango de valor	Cantidad	Criterio
Bajo	1 - 4	6	Aceptado
Moderado	5 - 9	16	No aceptado
Alto	10 - 14	11	No aceptado
Crítico	15 - 25	15	No aceptado

ROLES Y RESPONSABILIDADES

El análisis de riesgos desarrollado en este estudio se encuentra enfocado específicamente en el área de soporte técnico. En consecuencia, la definición de roles y responsabilidades se limita a los actores involucrados dentro de dicha área. A continuación, se detallan los roles internos considerados relevantes para la implementación y gestión de los controles de seguridad:

Tabla 9 *Roles y responsabilidades que se deben cumplir en el área de soporte técnico*

Rol	Responsabilidad
Director de ingeniería en sistemas	Supervisar y garantizar la implementación de políticas estratégicas de seguridad de la información, alineadas con las normas ISO/IEC 27001 e ISO 31000. Validar los planes de tratamiento de riesgos y aprobar los recursos necesarios para su ejecución.
Líder de soporte técnico	Coordinar la ejecución del plan de tratamiento de riesgos dentro del área de soporte técnico. Asignar tareas al equipo, monitorear el avance de las actividades y reportar los resultados al director de Ingeniería en Sistemas.
Analista de soporte técnico	Ejecutar actividades técnicas específicas para la mitigación de riesgos, tales como actualizaciones de sistemas, aplicación de controles de acceso, monitoreo de alertas y auditoría de dispositivos. Participar en la documentación de incidentes y mejoras.

Asistente de soporte técnico	Brindar apoyo operativo en la implementación de controles preventivos y correctivos. Realizar tareas como la revisión de configuraciones, seguimiento de inventario de equipos y asistencia en la capacitación básica de usuarios.

CAPÍTULO V

DEFINICIÓN DE UN CONJUNTO DE CONTROLES DE SEGURIDAD ESPECÍFICOS PARA MITIGAR LOS PRINCIPALES RIESGOS IDENTIFICADOS EN LOS SERVICIOS DE SOPORTE TÉCNICO DEL ÁREA DE TI

En el presente capítulo, se abordará los riesgos no aceptados que fueron identificados en el capítulo 4. Se hará uso de la ISO 27001:2017 para identificar que controles son aplicables a los riesgos obtenidos previamente.

5.1 IDENTIFICACIÓN DE CONTROLES DE SEGURIDAD APLICABLES

Como parte del análisis de riesgos aplicado a los activos de información de la institución, se identificaron diversas vulnerabilidades específicas por tipo de activo (hardware, software, infraestructura documental y personal). A fin de mitigar estas vulnerabilidades y alinear el tratamiento del riesgo con las mejores prácticas internacionales, se recurrió al Anexo A de la norma ISO/IEC

27001:2017, que contiene un conjunto de controles de seguridad organizacionales, técnicos y físicos.

Cada vulnerabilidad fue evaluada individualmente y se asignaron uno o más controles relevantes del Anexo A de la ISO 27001, según su capacidad para:

- Prevenir el riesgo (mediante políticas, restricciones o diseño seguro),
- Detectar eventos relacionados (mediante registros, monitoreo o auditorías), o
- Responder y corregir (mediante control de cambios, revisión de accesos o mantenimiento).

A continuación, se presentan los controles sugeridos para cada riesgo:

Tabla 10 *Riesgos con controles aplicables de la iso 27001*

CÓDIGO	VULNERABILIDAD	NIVEL DE RIESGO	CONTROLES ISO 27001 SUGERIDOS
AI001	Falta de actualizaciones y parches de seguridad.	Crítico	A.12.6.1 - Gestión de vulnerabilidades técnicas
AI003	Falta de cifrado en la transmisión y almacenamiento de documentos sensibles.	Crítico	A.13.2.1 - Políticas y procedimientos de intercambio de información
AI004	Configuración inadecuada de la consola de administración (ESET PROTECT)	Crítico	A.12.5.1 - Control de cambios
AI006	Falta de monitoreo y auditoría de accesos	Crítico	A.12.4.1 - Registro de eventos
AI006	Sincronización de cuentas con servicios externos sin control de seguridad	Crítico	A.9.2.1 Registro y cancelación del acceso de usuarios. A.9.2.6 Gestión de la identidad de los usuarios

AI009	No identificación de dispositivos vulnerables o en desuso	Crítico	A.8.1.2 - Propiedad de los activos. A.8.1.4 - Retiro de activos. A.8.3.1 - Gestión de activos removibles
AI001	Uso de configuraciones predeterminadas inseguras	Crítico	A.11.2.6 Utilización segura de los equipos. A.12.1.2 Cambio de procedimientos operativos
AI001	Falta de autenticación multifactor (MFA)	Crítico	A.9.4.2 - Control de autenticación
AI001	Uso de contraseñas débiles o reutilizadas	Crítico	A.9.4.3 - Uso de información secreta de autenticación
AI001	Falta de cifrado en discos duros	Crítico	A.10.1.1 - Política de uso del cifrado
AI002	Exposición a polvo, humedad o temperaturas extremas	Crítico	A.11.2.9 - Protección contra amenazas ambientales
AI003	Configuración inadecuada de filtros antispam y antimalware	Crítico	A.12.5.1 - Control de cambios
AI003	Uso de contraseñas débiles o reutilizadas	Crítico	A.9.4.3 - Uso de información secreta de autenticación
AI004	Falta de actualizaciones del software antivirus y bases de datos de firmas	Crítico	A.12.6.1 - Gestión de vulnerabilidades técnicas
AI005	Uso de versiones desactualizadas o sin parches de seguridad	Crítico	A.12.6.1 - Gestión de vulnerabilidades técnicas, A.14.2.3 - Protección de datos de prueba
A001	Uso de dispositivos USB no seguros	Alto	A.8.3.1 - Gestión de soportes extraíbles
AI007	Posibilidad de ataques de fuerza bruta o repetidos intentos de autenticación	Alto	A.9.4.2 – Procedimientos seguros de inicio de sesión
AI001	Instalación de software no autorizado	Alto	A.12.6.2 – Restricción en la instalación de software

AI004	Falta de monitoreo y alertas en la consola de administración	Alto	A.12.4.1 - Registro de eventos. A.12.1.2 – Gestión de cambios
AI001	Desactivación de firewalls y protección antivirus	Alto	A.13.1.1 - Controles de red
AI001	Ejecución de archivos o enlaces sospechosos	Alto	A.12.2.1 - Controles contra el código malicioso. A.7.2.2 - Concienciación, educación y capacitación en seguridad de la información
AI001	Excesivos privilegios de usuario	Alto	A.9.2.3 - Gestión de privilegios de acceso.
AI001	Riesgo de robo o extravío	Alto	A.11.2.6 - Seguridad de los equipos fuera de las instalaciones. A.11.1.1 - Perímetro de seguridad física
AI002	Ataques de denegación de servicio (DoS) en periféricos	Alto	A.13.1.1 – Controles de red
AI003	Acceso no autorizado	Alto	A.9.1.1 – Política de control de acceso.
AI001	Acceso físico no autorizado	Alto	A.11.1.1 – Perímetro de seguridad física
AI007	Configuración inadecuada de políticas de bloqueo de cuentas	Moderado	A.9.2.1 - Registro y baja de usuario.
AI002	Cableado desordenado o accesible	Moderado	A.11.2.3 - Seguridad del cableado. A.11.1.1 - Perímetro de seguridad física. A.11.2.4 - Mantenimiento de los equipos
AI010	Accesos privilegiados sin control adecuado	Moderado	A.9.2.3 - Gestión de privilegios de acceso. A.9.2.1 - Registro y baja de usuarios

AI009	Uso de software sin licencia o no autorizado	Moderado	A.8.1.1 - Inventario de activos.
AI010	Falta de capacitación en seguridad informática	Moderado	A.7.2.2 - Concienciación, educación y capacitación en seguridad de la información.
AI009	No gestionar la baja segura de activos	Moderado	A.8.1.4 – Devolución de activos.
AI010	Falta de compromiso o participación	Moderado	A.7.2.2 - Concienciación, educación y capacitación en seguridad de la información.
AI009	No incluir información detallada del equipo en el acta	Moderado	A.8.1.2 - Propiedad de los activos
AI009	Falta de trazabilidad en la asignación de equipos	Moderado	A.8.1.1 - Inventario de activos. A.8.1.2 - Propiedad de los activos
AI009	Falta de seguimiento y auditoría de los equipos asignados	Moderado	A.12.4.1 - Registro de eventos. A.8.1.1 - Inventario de activos. A.8.1.2 - Propiedad de los activos
AI010	Falta de seguimiento y evaluación	Moderado	A.8.1.1 - Inventario de activos
AI008	Modificación no autorizada	Moderado	A.9.1.1 - Política de control de acceso. A.12.4.1 - Registro de eventos
AI007	Falta de procedimientos de verificación antes del desbloqueo de cuentas	Moderado	A.9.2.1 - Registro y baja de usuarios.
AI007	Uso indebido de scripts de PowerShell sin restricciones	Moderado	A.12.1.1 - Documentación de procedimientos operacionales
AI002	Acceso no autorizado a impresoras y escáneres en red	Moderado	A.9.1.1 – Política de control de acceso.
AI002	Mantenimiento inadecuado	Moderado	A.11.2.4 - Mantenimiento de los equipos.

Esta sistematización permitió establecer un mapa claro de medidas concretas que la organización puede implementar para cada combinación de activo y riesgo, fortaleciendo así el sistema de gestión de seguridad de la información.

5.2 RELACIÓN DE CONTROLES CON LOS RIESGOS CRÍTICOS

En función de los riesgos clasificados como críticos en la Tabla 7 del Capítulo 4, se ha establecido una vinculación directa con controles de seguridad específicos orientados a mitigar tanto su impacto como la probabilidad de ocurrencia. Esta correspondencia se fundamenta en las buenas prácticas definidas por la norma ISO/IEC 27001:2017, e incluye tanto controles de carácter técnico como administrativo. Dado que los riesgos críticos representan las amenazas de mayor severidad para la organización, los controles sugeridos serán abordados en mayor profundidad, incorporando una descripción detallada de cada uno con el fin de facilitar su comprensión e implementación.

Tabla 11 *Descripción de controles en riesgos críticos*

Código	Vulnerabilidad	Nivel de Riesgo	Control Sugerido	Descripción del control
AI001	Falta de actualizaciones y parches de seguridad.	Crítico	A.12.6.1 - Gestión de vulnerabilidades técnicas	Se debe obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas para afrontar el riesgo asociado.
AI003	Falta de cifrado en la transmisión y almacenamiento de documentos sensibles.	Crítico	A.13.2.1 - Políticas y procedimientos de intercambio de información.	Deben establecerse políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación.

			A.10.1.1 – Política de uso de los controles criptográficos.	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para proteger la información.
AI004	Configuración inadecuada de la consola de administración (ESET PROTECT)	Crítico	A.14.2.5 - Principios de ingeniería de sistemas seguros	Principios de ingeniería de sistemas seguros se deben establecer, documentar, mantener y aplicarse a todos los esfuerzos de implementación de sistemas de información.
AI006	Falta de monitoreo y auditoría de accesos	Crítico	A.12.4.1 - Registro de eventos	Se deben registrar, proteger y revisar periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información
AI006	Sincronización de cuentas con servicios externos sin control de seguridad	Crítico	A.9.2.1 Registro y baja de usuario.	Debe implantarse un procedimiento formal de registro y retirada de usuarios que haga posible la asignación de los derechos de acceso.
			A.9.2.5 Revisión de los derechos de acceso de usuario.	Los propietarios de los activos deben revisar los derechos de acceso de usuario a intervalos regulares.
			A.13.1.1 – Controles de red	Las redes deben ser gestionadas y controladas para proteger la información de los sistemas
AI009	No identificación de dispositivos vulnerables o en desuso	Crítico	A.8.1.1 – Inventario de activos	La información y otros activos asociados a la información y a los recursos para el tratamiento de la información deben estar claramente identificados y debe elaborarse y mantenerse un inventario.
			A.8.1.2 - Propiedad de los activos.	Todos los activos que figuran en el inventario deben tener un propietario.
			A.8.1.4 - Devolución de activos.	Todos los empleados y terceras partes deben devolver todos los activos de la organización que estén en su poder al finalizar su empleo, contrato o acuerdo

			A.8.3.1 - Gestión de soportes extraíbles	Se debe implementar procedimientos para la gestión de soportes extraíbles de acuerdo con el esquema de clasificación adoptado por la organización.
AI001	Uso de configuraciones predeterminadas inseguras	Crítico	A.12.1.2 - Gestión de cambios	Los cambios en la organización, los procesos de negocios, instalaciones de tratamiento de información y los sistemas que afectan a la seguridad de la información deben ser controlados.
AI001	Falta de autenticación multifactor (MFA)	Crítico	A.9.4.2 - Procedimientos seguros de inicio de sesión.	Cuando así requiera en la política de control de acceso, el acceso a los sistemas y a las aplicaciones se debe controlar por medio de un procedimiento seguro de inicio de sesión.
AI001	Uso de contraseñas débiles o reutilizadas	Crítico	A.9.4.3 - Sistema de gestión de contraseñas	Los sistemas para la gestión de contraseñas deben ser interactivos y estableces contraseñas seguras y robustas.
AI001	Falta de cifrado en discos duros	Crítico	A.10.1.1 - Política de uso de los controles criptográficos	Se debe desarrollar e implementar una política sobre el uso de los controles criptográficos para proteger la información.
AI002	Exposición a polvo, humedad o temperaturas extremas	Crítico	A.11.2.1 - Emplazamiento y protección de equipos	Los equipos deben situarse o protegerse de forma que reduzcan los riesgos de las amenazas y los riesgos ambientales, así como las oportunidades de que se produzcan accesos no autorizados
AI003	Configuración inadecuada de filtros antispam y antimalware	Crítico	A.12.6.2 - Restricción en la instalación de software	Se deben establecer y aplicar reglas que rijan la instalación de software por parte de los usuarios.
			A.12.2.1 – Controles contra el código malicioso.	Se debe implementar los controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso, así como procedimientos adecuados de concienciación al usuario.

AI003	Uso de contraseñas débiles o reutilizadas	Crítico	A.9.4.3 - Sistema de gestión de contraseñas	Los sistemas para la gestión de contraseñas deben ser interactivos y estableces contraseñas seguras y robustas.
AI004	Falta de actualizaciones del software antivirus y bases de datos de firmas	Crítico	A.12.6.1 - Gestión de vulnerabilidades técnicas	Se debe obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas para afrontar el riesgo asociado.
AI005	Uso de versiones desactualizadas o sin parches de seguridad	Crítico	A.12.6.1 - Gestión de vulnerabilidades técnicas, A.14.2.3 - Protección de datos de prueba	Se debe obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas para afrontar el riesgo asociado.

5.3 DISEÑO DE POLÍTICAS Y CONTROLES ESPECÍFICOS

A partir de los controles definidos en el apartado anterior, se ha diseñado un conjunto de políticas y controles de seguridad específicos**,** orientados al área de soporte técnico y alineados con los lineamientos establecidos por las normas ISO/IEC 27001:2017**.** Estas políticas tienen como finalidad establecer directrices claras para la prevención, detección y respuesta ante incidentes de seguridad informática, contribuyendo así a una gestión eficaz de los riesgos identificados. Tal como se expuso previamente, se contempla el tratamiento de riesgos clasificados como críticos, altos y moderados. En función de ello, las políticas han sido estructuradas en dos secciones diferenciadas: una destinada exclusivamente a los riesgos críticos, dada su mayor nivel de severidad, y otra orientada a los riesgos de nivel alto y moderado.

Las políticas descritas a continuación se fundamentan en los controles establecidos en la norma ISO/IEC 27001:2017, y han sido adaptadas al contexto particular de la organización como medidas de referencia para su implementación.

POLÍTICA PARA EL TRATAMIENTO DE RIESGOS CRÍTICOS

Gestión de Vulnerabilidades Técnicas

Basado en A.12.6.1

Objetivo: Reducir la exposición a amenazas conocidas mediante la aplicación oportuna de actualizaciones y parches.

Controles personalizados:

- Se realizará un escaneo mensual de vulnerabilidades utilizando herramientas como OpenVAS, Nessus u otras aprobadas.
- Se establecerá un calendario de parches de seguridad para sistemas operativos, antivirus, navegadores, firmware de equipos y aplicaciones críticas.
- Las actualizaciones deberán ser aplicadas en un entorno de pruebas antes de ser desplegadas en producción.
- El área de soporte técnico será responsable de documentar y verificar cada aplicación de parche.

Cifrado en la Transmisión y Almacenamiento de Información

Basado en A.13.2.1 y A.10.1.1

Objetivo: Proteger la confidencialidad de la información crítica durante su almacenamiento y transmisión.

Controles personalizados:

- Todo documento que contenga datos personales, financieros o institucionales deberá almacenarse en medios cifrados.

- Se exigirá el uso de protocolos seguros como HTTPS, SFTP, o VPN con TLS 1.2 o superior.
- Se implementará BitLocker (Windows) o LUKS (Linux) para cifrado de discos duros en equipos portátiles y estaciones de trabajo con datos sensibles.
- Las claves de cifrado estarán bajo control de un custodio designado, y su gestión seguirá buenas prácticas de rotación periódica.

Configuración Segura de Consolas y Herramientas Administrativas

Basado en A.14.2.5

Objetivo: Evitar configuraciones por defecto inseguras en herramientas administrativas como consolas de antivirus o paneles web.

Controles personalizados:

- Se exigirá el cambio inmediato de credenciales por defecto en cualquier herramienta implementada.
- La consola de ESET PROTECT deberá tener autenticación multifactor activada, con auditoría de accesos habilitada.
- Las configuraciones serán revisadas cada trimestre para asegurar que no existan puertos abiertos innecesarios ni usuarios con privilegios innecesarios.
- Se documentarán todas las configuraciones iniciales y cambios aplicados con su justificación.

Monitoreo y Auditoría de Accesos

Basado en A.12.4.1 y A.12.4.3

Objetivo: Detectar accesos no autorizados o actividades anómalas mediante monitoreo constante.

Controles personalizados:

- Se habilitará el registro de eventos en servidores, equipos críticos y consolas de administración.
- Se utilizarán herramientas como Graylog, Splunk o ELK Stack para centralizar y analizar los registros.
- El sistema generará alertas automáticas ante:
    - Inicios de sesión fuera de horario.
    - Más de 5 intentos fallidos consecutivos de inicio de sesión.
    - Cambios de configuración no autorizados.
- Los registros se conservarán por un mínimo de 12 meses y serán revisados mensualmente.

Gestión Segura de Sincronización con Servicios Externos

Basado en A.13.1.1

Objetivo: Controlar las integraciones entre sistemas internos y servicios en la nube o externos.

Controles personalizados:

- Toda sincronización con servicios como Google Drive, OneDrive u otros requerirá autorización previa por parte del director de Ingeniería.
- Se implementará una revisión técnica de la API o canal de sincronización utilizado, asegurando que los datos estén cifrados.
- Se utilizarán mecanismos de autenticación segura (OAuth 2.0, tokens de acceso temporales).
- Se desactivará el acceso automático a cuentas externas cuando el personal cambie de área o se desvincule.

Gestión de Equipos Obsoletos y Baja Segura

Basado en A.8.1.3 y A.11.2.7

Objetivo: Evitar la exposición de información o vulnerabilidades a través de activos sin control o en desuso.

Controles personalizados:

- Todo equipo obsoleto o que no sea utilizado por más de 3 meses será etiquetado y evaluado para baja segura.
- Se aplicará software de borrado seguro (como DBAN o herramientas con estándares DoD 5220.22-M) antes de reutilizar o desechar equipos.
- La baja deberá ser firmada por el responsable de TI y registrada en el sistema de inventario.
- Se realizará un inventario físico y digital semestral para validar el estado de los activos y su trazabilidad.

POLITICA PARA EL TRATAMIENTO DE RIESGOS ALTOS Y MODERADOS

Gestión de Dispositivos USB y Soportes Extraíbles

Basado en A.8.3.1

Objetivo: Prevenir el uso no autorizado de dispositivos removibles que puedan introducir software malicioso o extraer información sensible.

Controles personalizados:

- Se deshabilitarán los puertos USB en estaciones de trabajo mediante políticas de grupo (GPO) o BIOS.
- El uso de dispositivos USB requerirá autorización formal por parte del área de soporte técnico.
- Solo se permitirá el uso de dispositivos cifrados y previamente registrados.
- Se mantendrá un registro detallado de cada uso, incluyendo usuario, número de serie y equipo conectado.

Procedimientos Seguros de Autenticación

Basado en A.9.4.2

Objetivo: Garantizar que los accesos a los sistemas estén protegidos frente a ataques de fuerza bruta o intentos repetitivos.

Controles personalizados:

- Bloqueo automático de cuentas tras 5 intentos fallidos durante un lapso de 15 minutos.
- Uso obligatorio de autenticación multifactor (MFA) para personal privilegiado.
- Contraseñas con un mínimo de 10 caracteres, incluyendo combinación de letras, números y símbolos.
- Caducidad de contraseñas cada 90 días y restricción para no repetir las últimas 5 claves usadas.

Monitoreo y Registro de Eventos en Consolas

Basado en A.12.4.1

Objetivo: Detectar actividades anómalas en herramientas de administración a través del registro y revisión de eventos.

Controles personalizados:

- Activación de logs en todas las consolas críticas de seguridad, antivirus y gestión de red.
- Uso de sistemas como Wazuh o ELK para centralizar y analizar los eventos.
- Configuración de alertas automáticas para actividades fuera de lo habitual.
- Conservación de registros por al menos 12 meses, con revisiones semanales por parte del analista técnico.

Control de Acceso a Impresoras y Escáneres en Red

Basado en A.9.1.2

Objetivo: Proteger los periféricos de red contra el uso no autorizado o manipulación indebida de documentos.

Controles personalizados:

- Asignación de contraseñas administrativas a impresoras y escáneres conectados a red.
- Acceso restringido a través de cuentas del dominio institucional.
- Registro de escaneos y restricciones de funciones inalámbricas o por USB no controladas.
- Ubicación de dispositivos con funciones sensibles en áreas con acceso limitado.

Mantenimiento Seguro de Equipos

Basado en A.11.2.4

Objetivo: Evitar riesgos durante o después de intervenciones técnicas en los activos de información.

Controles personalizados:

- Registro obligatorio de todas las actividades de mantenimiento en la plataforma de soporte.
- Supervisión directa en caso de intervención por terceros y firma de acuerdo de confidencialidad.
- Realización de respaldo completo antes de cualquier intervención crítica.
- Ejecución de pruebas de integridad y funcionalidad al finalizar cada mantenimiento.

DEFINICIÓN DE TAREAS POR ROLES EN SOPORTE TÉCNICO

La implementación de las políticas de seguridad orientadas al tratamiento de riesgos críticos, altos y moderados requiere una asignación clara de tareas y responsabilidades específicas entre los miembros del área de soporte técnico. Con base en los roles previamente definidos, a continuación, se establecen las funciones que cada uno de ellos deberá desempeñar en relación con los controles propuestos, con el fin de garantizar una ejecución coordinada, eficiente y alineada con los principios de seguridad de la información.

Director de Ingeniería en Sistemas

- Aprobar formalmente las políticas de seguridad de la información propuestas.
- Asignar recursos humanos, tecnológicos y presupuestarios para la implementación de controles.
- Participar en la validación de excepciones o situaciones no contempladas en los procedimientos estándar.
- Supervisar el cumplimiento global de la política y liderar revisiones anuales.

Líder de Soporte Técnico

- Coordinar la ejecución de los controles definidos en las políticas, tanto para riesgos críticos como para los niveles alto y moderado.
- Asignar tareas al personal técnico, verificando su cumplimiento y calidad.
- Aprobar solicitudes excepcionales (por ejemplo, uso de dispositivos USB o instalación de software).
- Consolidar y presentar informes mensuales sobre incidentes, auditorías, actualizaciones y cumplimiento de controles.

Analista de Soporte Técnico

- Aplicar configuraciones seguras en consolas administrativas, redes y estaciones de trabajo.
- Ejecutar tareas como instalación de parches, cifrado de dispositivos, bloqueo de puertos y validación de software.
- Realizar escaneos de vulnerabilidades, revisar registros de eventos, analizar alertas y proponer mejoras técnicas.
- Garantizar el registro adecuado de logs y respaldos de seguridad.

Asistente de Soporte Técnico

- Apoyar en la ejecución de tareas operativas como el seguimiento de mantenimiento, etiquetado de equipos en desuso, supervisión del uso de periféricos y control de acceso físico.
- Registrar información técnica y administrativa sobre intervenciones, dispositivos y configuraciones aplicadas.
- Colaborar en la preparación de reportes y mantener actualizados los inventarios de activos tecnológicos.
- Brindar capacitación básica a usuarios finales en buenas prácticas de seguridad informática.

REVISIÓN Y MEJORA CONTINUA

Esta política será revisada de forma periódica cada 12 meses o de manera inmediata en caso de presentarse un incidente relevante asociado a los riesgos abordados. Las propuestas de mejora serán evaluadas por el Líder de Soporte Técnico en coordinación con el director de Ingeniería en Sistemas, quienes tendrán la responsabilidad de actualizar y adaptar los controles implementados conforme a los cambios tecnológicos, operativos o normativos que pudieran surgir.

CONCLUSIONES

- La identificación de los activos de información y sistemas críticos del área de soporte técnico permitió establecer una base sólida para el análisis de riesgos. Se reconoció que estos activos, al estar directamente relacionados con la continuidad operativa de la institución, requieren una gestión especializada. La recopilación y clasificación de hardware, software, documentación y recursos humanos facilitó una comprensión estructurada del entorno tecnológico y su relevancia estratégica dentro de la universidad.

- A través del análisis de vulnerabilidades y amenazas, se evidenció que los activos del área de soporte técnico están expuestos a riesgos tanto internos como externos. Entre los principales hallazgos se destacan la ausencia de controles de acceso, la falta de actualización de sistemas, el uso de software no autorizado y la exposición a amenazas como malware, accesos no autorizados y errores humanos. Esta etapa fue fundamental para delimitar los factores que comprometen la confidencialidad, integridad y disponibilidad de la información institucional.

- La categorización y evaluación de los riesgos mediante el uso de una matriz de impacto y probabilidad permitió establecer un enfoque estructurado y cuantificable del nivel de exposición al que se encuentra la institución. Se logró priorizar los riesgos según su criticidad, destacándose un número significativo de riesgos clasificados como críticos, lo que evidencia la necesidad urgente de implementar medidas correctivas. Este análisis confirmó que, sin una adecuada gestión, los activos tecnológicos del soporte técnico están en una situación de vulnerabilidad que puede derivar en afectaciones operativas y reputacionales.

- A partir del análisis de riesgos realizado, se definió un conjunto de políticas y controles personalizados alineados con las normas ISO/IEC 27001. Estos controles fueron organizados en función del nivel de riesgo (crítico, alto o moderado) y adaptados al contexto institucional. Además, se asignaron responsabilidades específicas a cada rol del área de soporte técnico, con el fin de asegurar una implementación efectiva. Este diseño no solo permite mitigar riesgos existentes, sino que también constituye un marco de referencia para el fortalecimiento continuo de la seguridad informática dentro de la universidad.

- La aplicación de la norma ISO 31000 proporcionó un marco metodológico integral para la identificación, análisis, evaluación y tratamiento de riesgos en el área de soporte técnico de TI. Su enfoque estructurado y adaptable permitió desarrollar un proceso sistemático que facilitó la toma de decisiones informadas, basadas en criterios de impacto y probabilidad. Asimismo, la norma permitió priorizar los riesgos en función de su severidad y establecer lineamientos claros para su mitigación, fortaleciendo así la base conceptual y operativa del diseño de políticas de seguridad presentadas en este trabajo.

RECOMENDACIONES

- Implementar gradualmente las políticas diseñadas, comenzando por aquellas asociadas a riesgos críticos, asegurando su apropiación por parte del personal del área de soporte técnico y fomentando una cultura de seguridad institucional.

- Establecer mecanismos de monitoreo y revisión periódica de los controles implementados, con el fin de evaluar su efectividad y realizar ajustes oportunos en función de los cambios tecnológicos o nuevos riesgos identificados.

- Promover la capacitación continua del personal técnico, especialmente en temas de seguridad de la información, gestión de riesgos y cumplimiento de normativas, para garantizar una correcta aplicación de las políticas y reducir la exposición a amenazas internas y externas.

- Formalizar los procedimientos documentados derivados de las políticas, asegurando su difusión y accesibilidad dentro del área de TI, de manera que todos los miembros del equipo comprendan sus funciones, límites y responsabilidades.

- Ampliar el alcance del análisis de riesgos a otras áreas de la institución, replicando la metodología utilizada en este estudio, con el objetivo de fortalecer el sistema general de gestión de seguridad de la información en toda la universidad.

BIBLIOGRAFÍA

[1] J. Merchan-Lima, F. Astudillo-Salinas, L. Tello-Oquendo, F. Sanchez, G. Lopez-Fonseca, and D. Quiroz, “Information security management frameworks and strategies in higher education institutions: a systematic review,” Ann. Telecommun., vol. 76, no. 3, pp. 255–270, Apr. 2021, doi: 10.1007/s12243-020-00783-2.

[2] S. A. Grishaeva and V. I. Borzov, “Information Security Risk Management,” in 2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS), 2020, pp. 96–98. doi: 10.1109/ITQMIS51053.2020.9322901.

[3] M. B. Oliveira, A. Goldman, and J. Yoder, “Information Security Investments: How to Prioritize?,” in Proceedings of the 20th Brazilian Symposium on Information Systems, in SBSI ’24. New York, NY, USA: Association for Computing Machinery, 2024. doi: 10.1145/3658321.3658363.

[4] P. Manuja and R. S. Shekhawat, “IT Security Frameworks: Risk Management Analysis and Solutions,” in Proceedings of the 4th International Conference on Information Management & Machine Intelligence, in ICIMMI ’22. New York, NY, USA: Association for Computing Machinery, 2023. doi: 10.1145/3590837.3590881.

[5] L. H. Collante, Y. Escobar, F. Acosta, A. Pranolo, and A. Prasetya, “Preparation of the Information Security Management System Implementation Based on the NTC-ISO-IEC 27001:2013 Standard at the IUB University Institution,” in 2023 IEEE Colombian Caribbean Conference (C3), 2023, pp. 1–6. doi: 10.1109/C358072.2023.10436270.

[6] F. Alkhudhayr, S. Alfarraj, B. Aljameeli, and S. Elkhdiri, “Information Security:A Review of Information Security Issues and Techniques,” in 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), 2019, pp. 1–6. doi: 10.1109/CAIS.2019.8769504.

[7] B. Lundgren and N. Möller, “Defining Information Security,” Sci. Eng. Ethics, vol. 25, no. 2, pp. 419–441, Apr. 2019, doi: 10.1007/s11948-017-9992-1.

[8] M. Hentea, “Security Management,” in Building an Effective Security Program for Distributed Energy Resources and Systems, 2021, pp. 405–436. doi: 10.1002/9781119070740.ch11.

[9] H. S. Lallie, A. Thompson, E. Titis, y P. Stephens, «Analysing Cyber Attacks and Cyber Security Vulnerabilities in the University Sector», Computers, vol. 14, n.o 2, p. 49, feb. 2025, doi: 10.3390/computers14020049.

[10] H. L. Grob, G. Strauch, and C. Buddendick, “Applications for IT-Risk Management – Requirements and Practical Evaluation,” in 2008 Third International Conference on Availability, Reliability and Security, 2008, pp. 758–764. doi: 10.1109/ARES.2008.168.

[11] E. S. Mandrakov, D. A. Dudina, V. A. Vasiliev, and M. N. Aleksandrov, “Risk Management Process in the Digital Environment,” in 2022 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS), 2022, pp. 108–111. doi: 10.1109/ITQMIS56172.2022.9976622.

[12] D. Cruz, A. Arsenio, T. Gallego, A. José, and S. Henares, “Análisis de riesgos PID_00275346.”

[13] N. C. Pa and B. Anthony, “A model of mitigating risk for IT organisations,” in 2015 4th International Conference on Software Engineering and Computer Systems (ICSECS), 2015, pp. 49–54. doi: 10.1109/ICSECS.2015.7333082.

[14] B. Shahzad and S. A. Safvi, “Risk Mitigation And Management Scheme Based On Risk Priority”.

[15] M. L. Yeo, E. Rolland, J. R. Ulmer, and R. A. Patterson, “Risk Mitigation Decisions for IT Security,” ACM Trans Manage Inf Syst, vol. 5, no. 1, Apr. 2014, doi: 10.1145/2576757.

[16] G. Stoneburner, A. Goguen, and A. Feringa, “Risk management guide for information technology systems : recommendations of the National Institute of Standards and Technology,” National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-30, 2002. doi: 10.6028/NIST.SP.800-30.

[17] P. Y. Lartey, Y. Kong, F. B. M. Bah, R. J. Santosh, and I. A. Gumah, “Determinants of Internal Control Compliance in Public Organizations; Using Preventive, Detective, Corrective and Directive Controls,” Int. J. Public Adm., vol. 43, no. 8, pp. 711–723, Jun. 2020, doi: 10.1080/01900692.2019.1645689.

[18] A. Setyawan, Y. Giri Sucahyo, and A. Gandhi, “Design of Disaster Recovery Plan: State University in Indonesia,” in 2020 Fifth International Conference on Informatics and Computing (ICIC), Nov. 2020, pp. 1–5. doi: 10.1109/ICIC50835.2020.9288543.

[19] S. M. Hawkins, D. C. Yen, and D. C. Chou, “Disaster recovery planning: a strategy for data security,” Inf. Manag. Comput. Secur., vol. 8, no. 5, pp. 222–230, Dec. 2000, doi: 10.1108/09685220010353150.

[20] C. Beretas, “Information Systems Security, Detection and Recovery from Cyber Attacks,” Univers. Libr. Eng. Technol., vol. 01, no. 01, pp. 27–40, Jun. 2024, doi: 10.70315/uloap.ulete.2024.0101005.

[21] “EAR - Herramientas para el Análisis de Riesgos”, Ar-tools.com. [En línea]. Disponible en: https://www.ar-tools.com/es/index.html. [Consultado: 18-jun-2025].