UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

TÍTULO DEL TRABAJO DE TITULACIÓN

Mitigación de riesgos de la seguridad en la infraestructura de hardware del área de TIC de la Universidad Técnica Luis Vargas Torres basado en la metodología MAGERIT v. 3 y NIST Cybersecurity Framework.

Trabajo de Titulación previo a la obtención del Título de Magíster en

Computación con Mención en Seguridad Informática.

AUTOR: QUISPE MERA VICTOR EDUARDO.

DIRECTOR: MSC. CUZME RODRÍGUEZ FABIÁN GEOVANNY.

IBARRA - ECUADOR

2024

UNIVERSIDAD TÉCNICA DEL NORTE

Acreditada Resolución Nro. 173-SE-33-CACES-2020

REPÚBLICA DEL ECUADOR

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD	0804383495		
APELLIDOS Y NOMBRES	Quispe Mera Víctor Eduardo		
DIRECCIÓN	Esmeraldas, Sector Codesa, Propicia 4.		
EMAIL	vequispem@utn.edu.ec		
TELÉFONO FIJO	062015016	**MÓVIL**	0989678140
DATOS DE LA OBRA			
TÍTULO	Mitigación de riesgos de la seguridad en la infraestructura de hardware del área de TIC de la Universidad Técnica Luis Vargas Torres basado en la metodología MAGERIT v. 3 y NIST Cybersecurity Framework.		
AUTOR	Quispe Mera Víctor Eduardo		
FECHA	2023/11/06		
SOLO PARA TRABAJOS DE GRADO			
PROGRAMA DE POSGRADO	Computación con Mención en Seguridad Informática		
TÍTULO POR EL QUE OPTA	Magíster en Computación con Mención en Seguridad Informática		
TUTOR	Msc. Cuzme Rodríguez Fabián		

CONSTANCIA

El Quispe Mera Víctor Eduardo, manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de esta y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 14 días del mes de marzo del 2024

EL AUTOR

Quispe Mera Víctor Eduardo

C.I: 0804383495

CERTIFICACIÓN DIRECTOR

Ibarra, 13 de marzo del 2024

CERTIFICACIÓN DEL TRABAJO DE TITULACIÓN

Por medio del presente, yo, Msc. Cuzme Rodríguez Fabián, certifico que el Sr. Quispe Mera Víctor Eduardo, portador de la cédula de ciudadanía número 0804383495, ha trabajado en el desarrollo del proyecto de posgrado "Mitigación de riesgos de la seguridad en la infraestructura de hardware del área de TIC de la Universidad Técnica Luis Vargas Torres basado en la metodología MAGERIT v. 3 y NIST Cybersecurity Framework.", previo a la obtención del Magíster en Computación con Mención en Seguridad Informática, realizado con interés profesional y responsabilidad que certifico con honor de verdad.

Es todo en cuanto puedo certificar a la verdad.

Atentamente,

Firmado electrónicamente por:
FABIAN GEOVANNY
CUZME RODRIGUEZ

Fabián Geovanny Cuzme Rodríguez

DIRECTOR DE TRABAJO DE GRADO

Dedicatoria

El presente trabajo de investigación está destinado a mis amados padres, quienes me han guiado correctamente en cada paso a lo largo de mi vida, a quienes me inculcaron la importancia de lo académico, a quienes antepusieron mi bienestar y el de mis seis hermanos, a sus aspiraciones personales.

A mis hermanos, por ser un gran ejemplo a seguir, por enseñarme las virtudes de ser curioso e independiente.

A mis abuelos, que, aunque ya no están en este mundo, sé que desde el cielo celebran orgullosos cada logro de sus nietos.

También, dedico este proyecto a la mujer que amo, no habría avanzado en todo lo que he logrado hasta ahora sin su tenaz entusiasmo, hemos tenidos altos y bajos, pero si de algo estoy seguro es que no habría querido compartir todo esto con nadie más, y si la vida es amable conmigo me gustaría compartirla junto a ti.

Ing. Víctor Eduardo Quispe Mera.

Agradecimiento

Quiero expresar mi gratitud a Dios, quien con su bendición llena siempre mi vida y a toda mi familia por estar siempre presentes, quien me ha brindado momentos de claridad en las etapas más complicadas de mi vida, quien a pesar de saber de primera mano cuan imperfecto soy, siempre ha estado allí para ayudarme a seguir adelante.

A toda mi familia, por ser las personas más amorosas y respetables que he tenido cerca. A mis amigos cercanos y a todas las personas que directa e indirectamente me han apoyado en harás al cumplimiento de mis objetivos.

Los guardo en lo más profundo de mi corazón, por siempre.

Ing. Víctor Eduardo Quispe Mera.

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

Resumen

La seguridad de la información, es una de las principales necesidades de toda organización, y con el incremento de las nuevas tecnologías y de la virtualidad ha hecho que a su vez también se incrementan las amenazas, vulnerabilidades, incidentes y ataques a los sistemas de información. Debido a lo expuesto anteriormente se ha desarrollado un análisis para mitigar los riesgos de la seguridad en la infraestructura de hardware aplicado en el área de TIC de la Universidad Técnica Luis Vargas Torres de Esmeraldas basados en las metodologías MAGERIT v. 3 y NIST Security Framework, se ha considerado para la evaluación de riesgos la herramienta Pilar, cuya función es el análisis y la gestión de riesgos de un sistema de información siguiendo la metodología MAGERIT, que consta de cuatro fases; caracterización de los activos, de las amenazas, de las salvaguardas y estimación del estado del riesgo, de la misma forma la metodología NIST SP 800-30 está dividida en: prepararse para la evaluación, realizar la evaluación y comunicar los resultados, por ultimo mantener la evaluación de riesgos, a su vez se proponen controles adecuados tomando como referencia la normativa ISO/IEC 27001:2022, para contrarrestar los riesgos a los que se encuentran expuestos los activos de hardware.

Palabras claves: Activos de información, riesgo, amenaza, vulnerabilidades, salvaguardas, MAGERIT, Pilar, NIST Security Framework.

Abstract

Information security is one of the main needs of every organization, and with the increase in new technologies and virtuality, threats, vulnerabilities, incidents and attacks on information systems have also increased. Due to the above, an analysis has been developed to mitigate security risks in the hardware infrastructure applied in the ICT area of the Luis Vargas Torres de Esmeraldas Technical University based on the MAGERIT v methodologies. 3 and NIST Security Framework, the Pilar tool has been considered for risk assessment, whose function is the analysis and risk management of an information system following the MAGERIT methodology, which consists of four phases; characterization of assets, threats, safeguards and estimation of the risk state, in the same way the NIST SP 800-30 methodology is divided into: prepare for the evaluation, carry out the evaluation and communicate the results, finally maintain the risk assessment, in turn, appropriate controls are proposed, taking as reference the ISO/IEC 27001:2022 standard, to counteract the risks to which hardware assets are exposed. **Keywords**: Information assets, risk, threat, vulnerabilities, safeguards, MAGERIT, Pilar, NIST Security Framework.

Capítulo I

1. El Problema

Durante los últimos años, el mundo ha cambiado; los avances tecnológicos, la interconexión, el IoT, la inteligencia artificial, la inteligencia cognitiva, la globalización de la economía, el desarrollo de los mercados, las telecomunicaciones, los dispositivos de telecomunicación, el comercio electrónico, la era digital, la innovación de los procesos y modelos de negocio; no son solo conceptos, son una realidad, y con ello han aparecido nuevos y más riesgos de seguridad de información; año a año se observa como la percepción de riesgo de seguridad ha ido incrementando (Acosta J. , 2018).

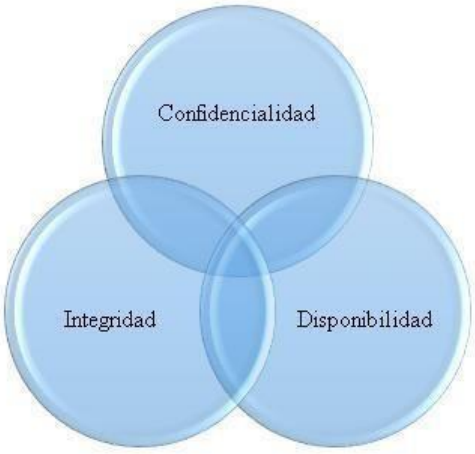
En consecuencia, en este capítulo se presenta el estudio de la problemática, donde se identifica el problema, los objetivos planteados en la investigación tanto el general como los específicos y la importancia de la misma.

1.1. Problema de Investigación

La ciberdelincuencia y fallos informáticos es uno de los focos de riesgos de las empresas y organismos públicos con una probabilidad alta e impacto alto en caso de materializarse (Lillo, 2019). Estos impactos pueden afectar en tres dimensiones, como se evidencia en la figura 1.

Figura 1

Tríada de la seguridad



***Nota**: La tríada de la seguridad está conformada por la confidencialidad, integridad y disponibilidad; todos estos garantizan una óptima gestión de la seguridad de la información, elaboración propia.*

Los riesgos de la información están presentes cuando confluyen dos elementos: amenazas y vulnerabilidades. Las amenazas y vulnerabilidades están íntimamente ligadas, y no puede haber ninguna consecuencia sin la presencia conjunta de éstas. Se pueden agrupar las amenazas en cuatro categorías, como son: el factor humano, los fallos en los sistemas de procesamiento de información, los desastres naturales, y los actos maliciosos. Algunos ejemplos de estas amenazas pueden ser: virus informáticos, robo o alteración de información, uso no autorizado de los sistemas, espionajes y ciberataques (Figueroa, Rodriguez, Bone, & Saltos, 2017).

De acuerdo con Villamar, los ciberataques han sido una gran problemática a lo largo de los años y se han incrementado conforme al crecimiento en el uso de la tecnología con múltiples plataformas tecnológicas que soportan multiplicidad de servicios. Un ciberataque se refiere a un individuo u organización que deliberadamente intenta dañar el sistema de información de un usuario, la complejidad y diversos de los ataques cibernéticos están aumentando y existen diferentes tipos de ataques para cada propósito malicioso (Arellano, 2022).

En el 2016, la compañía de seguridad informática ESET, informó que el 49 % de las empresas pequeñas y el 30 % de empresas medianas o grandes reportaron problemas de código malware, y de manera más vulnerable se encuentra el sector público (Chang, 2020). Una estadística en el 2016 por la empresa PwC señala que, del total de delitos económicos reportados a nivel global, el 32% correspondía a crimen cibernético y ocupaba el segundo lugar en la lista.

Uno de los delitos cibernéticos más recientes que afectó a varios países de América Latina, incluyendo en gran medida a Ecuador, fue la aplicación Pokémon GO. Se reportó que algunos usuarios por no poder descargar la aplicación oficial instalaron otras versiones que no contaban con la seguridad adecuada. Esto implicó un número considerable de ataques cibernéticos (Olmedo & Gavilanez, 2018).

Por último, según datos de Kaspersky Lab en su informe de amenazas en tiempo real, en junio del año 2017, Ecuador ocupó en América del Sur el primer lugar con el 2,8 % y el quinto lugar a nivel mundial en cuanto a ciberataques a sus redes. En Ecuador el 43 % de los ciudadanos tiene acceso a internet, sin embargo, la gran mayoría de estos, desconocen medidas de protección y prevención sobre las amenazas y peligros de su uso, debido a que carecen de una educación formal sobre el tema informático, siendo fácilmente víctimas de los ciberataques; por otro lado, las políticas de ciberseguridad en las empresas del Ecuador, tampoco se aplican de manera rigurosa (Chang, 2020).

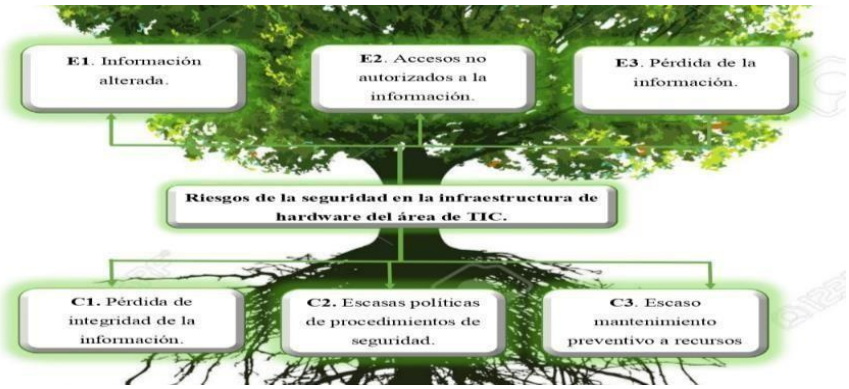
La Universidad Técnica Luis Vargas Torres de Esmeraldas, es una entidad autónoma de derecho público sin fines de lucro financiada por el Estado, creada mediante la Ley nº 70-16 el 4 de mayo de 1970, ubicada en la ciudad de Esmeraldas, provincia de Esmeraldas, al noreste de Ecuador. Su estructura está conformada por facultades, carreras, direcciones, unidades administrativas, académicas e investigativas. Una de las áreas administrativas, es la dirección de tecnologías de información y comunicación, quien es encargado de la operación y mantenimiento de los sistemas de información y de la infraestructura tecnológica, la seguridad de la información y las instalaciones, y el soporte a usuarios (Universidad Técnica Luis Vargas Torres, 2016).

Actualmente, presentan inconvenientes en la integridad, confidencialidad, y disponibilidad de la seguridad de la información dentro y fuera de la institución, desde la perspectiva de los estudiantes, a lo largo de los años se ha normalizado ciertos problemas en cuanto a disponibilidad de la información de los sitios webs, desde colapsos recurrentes hasta la pérdida de la información, en cuanto a los docentes se presentan errores durante el período de asignación de promedios trimestrales, adulteración de los registros de calificaciones.

Otro aspecto a considerar es al personal del área de TIC (tecnologías de la información y de la comunicación) al pasar el tiempo ha tenido problemas frecuentes en los registros académicos, desde alteración de notas por terceros, filtración de información institucional hasta el funcionamiento deficiente en infraestructura tecnológica. En la figura 2, se visualiza el árbol de problema, donde se identifica la naturaleza de la problemática a investigar.

Figura 2

Árbol de problemas



***Nota**: Se refleja tres causas con sus respectivos efectos, elaboración propia.*

En consecuencia, por todos estos posibles eventos de amenazas, es indispensable realizar un análisis de los riesgos para posteriormente incluir o adoptar métodos, medidas, procedimientos o normativas de seguridad que permitan salvaguardar la información, mitigar las amenazas y vulnerabilidades.

1.2 Interrogantes de la Investigación

- ¿Cuál es el impacto del análisis de riesgos de la seguridad en la infraestructura de hardware basados en la metodología MAGERIT v.3 y NIST Cybersecurity Framework en el área de TIC de la Universidad Técnica Luis Vargas Torres de la ciudad de Esmeraldas?
- ¿Mitigar los riesgos de seguridad en la infraestructura de hardware aplicando la metodología MAGERIT v.3 y NIST Cybersecurity Framework en el área de TIC garantizará la confidencialidad, disponibilidad e integridad de la información?

1.3. Objetivos de la Investigación

1.3.1. Objetivo General

- Mitigar los riesgos de la seguridad en la infraestructura de hardware del área de TIC de la Universidad Técnica Luis Vargas Torres de Esmeraldas basado en la metodología MAGERIT v. 3 y NIST Cybersecurity Framework.

1.3.2 Objetivos Específicos

- Identificar los riesgos de seguridad en los equipos informáticos del sistema de información del área de TIC.
- Determinar el nivel de impacto de acuerdo al proceso de gestión de riesgos del MAGERIT v.3 a través de la herramienta Pilar.
- Establecer medidas de protección que permitan reducir los riesgos de seguridad de acuerdo a la normativa ISO/IEC 27001:2022 y NIST Cybersecurity Framework.
- Evaluar las medidas de protección aplicadas en el área de TIC de la Universidad Técnica Luis Vargas Torres de la ciudad de Esmeraldas.

1.4 Justificación

La presente investigación se orienta en los Objetivos de Desarrollo Sostenible (ODS), estos son el corazón de la Agenda 2030 y muestran una mirada integral, indivisible y una colaboración internacional renovada. En conjunto, construyen una visión del futuro que queremos. En la figura 3, se muestran los 17 objetivos de desarrollo sostenible (Naciones Unidas, 2018).

Figura 3

Objetivos de desarrollo sostenible

***Nota**: Se hace referencia al objetivo 9, adaptado de Objetivos de desarrollo sostenible de Naciones Unidas, 2018, (https://repositorio.cepal.org/bitstream/handle/11362/40155/24/S1801141_es.pdf)*

Donde el objetivo 9, está orientado a construir infraestructuras resilientes, promover la industrialización inclusiva y sostenible y fomentar la innovación en América Latina y el Caribe, es esencial para fortalecer y actualizar las capacidades tecnológicas propias de la región; para reducir gradualmente su déficit de bienes con un mayor componente tecnológico, y aplicar una política que combine adecuadamente la demanda de nuevas capacidades con la educación y la formación profesional (Naciones Unidas, 2018).

Actualmente, los sistemas de información permiten la puesta en valor de la información y las tecnologías de la información implementadas por la empresa. El sistema de información integra esta información y tecnología con el componente humano y los procesos organizativos que conforman la organización. De esta forma, los sistemas de información engloban los equipos y programas informáticos, telecomunicaciones, bases de datos, recursos humanos y procedimientos (Alcamí, Carañana, & Herrando, 2011). Por tanto, es necesario implementar medidas de protección; como la ciberseguridad para la gestión adecuada de los sistemas de información.

La ciberseguridad, entendida como la prevención de ciberataques y la construcción de seguridad en la forma en que se protegen los sistemas TIC y datos. Se espera que las empresas y sus directorios protejan los datos y los activos digitales del robo y el fraude. También, se la puede considerar como una ciberdefensa, que se ocupa de la preparación para defender los intereses nacionales o atacar a los enemigos en el ciberespacio, involucrando tanto iniciativas militares como civiles, su objetivo es proteger la continuidad de la infraestructura y los servicios críticos, donde los ciberataques podrían causar daños considerables (Lehuedé, 2020).

Por otro lado, el objetivo de toda organización deberá estar enfocado en proteger los activos de la información teniendo como base a las siguientes dimensiones; disponibilidad, integridad, confidencialidad, y otras adicionales como; autenticidad, y trazabilidad, para cumplir con estos objetivos se puede aplicar metodologías de análisis y gestión de riesgos (Magerit, 2012).

Conforme con MAGERIT (2012), esta metodología persigue los siguientes objetivos; los objetivos directos, tienen por objeto concienciar a los responsables de las organizaciones

de información de la existencia de riesgos y la necesidad de gestionarlos, ofrecer un método sistemático para analizar los riesgos derivados del uso de las tecnologías de la información y comunicación (TIC), ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control. Mientras que, los objetivos indirectos, tienen como finalidad preparar a la organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda cada caso (Sanchez & Calispa, 2021).

Otro punto a considerar es el NIST SP 800-30 (Guía de Gestión de Riesgos de los Sistemas de Tecnología de la Información). Es un estándar desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST), fue formulado para la evaluación de riesgos de seguridad de la información especialmente a los sistemas de TI (Tecnología de la Información), proporciona una guía para la seguridad de las infraestructuras de la misma desde una perspectiva técnica (Macía, 2018).

Por consiguiente, la seguridad de la información es un alto factor de riesgo de ataques, por eso al aplicar metodologías de análisis de riesgos, igualmente es indispensable implementar medidas eficaces, como, por ejemplo, el cumplimiento de las normativas, entre ellas se encuentran la familia ISO.

La normativa ISO/IEC 27001:2022, es la norma más importante y principal de la familia ISO/IEC 27000, porque contiene los requisitos para la implantación del sistema de gestión de seguridad de la información (SGSI), cláusula 4 a 10 en las organizaciones y la única norma que se puede obtener la certificación (Toledo, 2022). En definitiva, el cumplimiento del estándar ISO/IEC 27001:2022, contribuirá a las instituciones para optimizar la gestión de riesgos, garantizando en todo momento la continuidad de las actividades de la organización, ya que se la considera como una estrategia de gestión de riesgos exitosa.

Adicionalmente, el proyecto de estudio también se guía en la línea de investigación N° 10 que se refiere al desarrollo, aplicación de software y cybersecurity (seguridad cibernética), aprobadas por el Honorable Consejo Universitario de la Universidad Técnica del Norte. (Universidad Técnica del Norte, 2023).

Capítulo II

2. Marco Referencial

En este capítulo, se presentan los antecedentes que son los estudios previamente realizados con anterioridad que aportan al desarrollo de la investigación; el marco teórico que son las bases teóricas que sustentan el proyecto y el marco legal que como su nombre lo indica es la fundamentación legal en la que se ampara el proyecto de investigación.

2.1 Antecedentes

La seguridad de la información a medida que pasan los años se ha convertido en un tema de vital importancia, debe ser protegida de forma adecuada, es por ello que son muchos los trabajos de investigación que abordan este tema desde diferentes enfoques, así se enumeran trabajos como se muestran a continuación:

En el estudio realizado por Luis Adrián Chóez Acosta (2020), implementa un plan de tratamiento de riesgos tecnológicos al centro de cómputo para una organización no gubernamental siguiendo la metodología MAGERIT, dentro de la metodología se efectúan técnicas de recolección y análisis de la información, en su resultado se evidencian los riesgos detectados a las que está expuesta la organización; las mismas que fueron controladas utilizando medidas preventivas y correctivas (Acosta L. A., 2020).

Otro ejemplo, corresponde a Ávila Torres Remigio (2021), de la Universidad Católica de Cuenca, quien realizó el "Análisis y evaluación de riesgos aplicado a EMAPAL-EP basado en la metodología de MAGERIT versión 3.0", el tipo de método empleado es el inductivo – deductivo para la obtención de los activos y amenazas presentes, con un enfoque descriptivo.

Su objetivo general es "Analizar los riesgos del área de TI en la empresa EMAPAL – EP, basado en la metodología MAGERIT v.3, para mitigar los riesgos; y elaborar un plan de tratamiento que permita mantenerlos en un nivel aceptable".

La finalidad de este trabajo de investigación es determinar una valoración cuantitativa del análisis y gestión de riesgos de la empresa, empleando la metodología MAGERIT, donde fue llevada a cabo en cinco fases, obteniendo como resultado 43 riesgos en nivel alto, 269 en

nivel medio y 88 riesgos en nivel bajo, para posteriormente elaborar un plan de tratamiento de los riesgos, haciendo uso de los estándares internacionales como el COBIT 5 o la familia ISO/IEC 27000, ISO/IEC 31000 (Torres, 2021).

Este estudio demostró la pertinencia de realizar un análisis de los riesgos, ya que permite mitigar o disminuir los riesgos presentes en una organización, ya que los más vulnerables a sufrir de ciberataques son los equipos de las empresas, la información como un recurso muy valioso, y los servicios que prestan.

Por tanto, este estudio se relaciona con el proyecto de investigación debido a que la metodología MAGERIT en complemento con los estándares internacionales garantizan, protegen, y mantienen la información de forma segura, detectando posibles amenazas para finalmente elaborar un plan de respuesta acorde con los resultados obtenidos.

También, Chiriboga Mera Teresa (2022), en su "Propuesta de un modelo híbrido basado en la metodología MAGERIT e ISO 27001 para controlar amenazas internas en la intranet de la Facultad de Informática y Electrónica, de la Universidad Politécnica de Chimborazo, el tipo de investigación es a nivel exploratorio, ya que propone incluir controles para contrarrestar las amenazas, además emplea el método deductivo debido al diagnóstico realizado, utilizó la observación y la lista de inventarios de los activos físicos y virtuales como técnica de recolección de datos.

El objetivo general del tema de estudio propone un modelo híbrido basado en la metodología MAGERIT e ISO 27001 para controlar amenazas internas en la intranet de la Facultad de Informática y Electrónica de la ESPOCH, llevando a cabo inicialmente un análisis de las etapas de cada una de las metodologías para formar una híbrida, luego un diagnóstico de las amenazas existentes, para elaborar y aplicar el modelo híbrido, y finalmente evaluar los resultados obtenidos tras la aplicación del modelo.

El modelo híbrido de la metodología MAGERIT y la ISO 27001 está formado por siete etapas, donde inicia con las actividades preliminares y continua con el análisis de riesgos, utilizando un escenario simulado en GNS3, demostrando que la reducción del nivel

de riesgo de ocurrencia de las amenazas en un 65.38%, logrando obtener un 95% de nivel de confianza con el análisis de los datos. (Mera, 2022)

Este trabajo se relaciona con la investigación planteada, ya que muestra que al aplicar la metodología de MAGERIT y el estándar ISO/IEC 27001, sirven en gran medida para la identificación, valoración, y tratamiento de los riesgos, permitiendo mantener seguro el sistema de información de las instituciones tanto públicas como privadas.

Víctor Félix Barrezueta Bermeo (2023), realiza un estudio sobre "Gestión de seguridad de la información", en el Gobierno provincial de Tungurahua, basado en los estándares de seguridad de la información ISO/IEC y la metodología MAGERIT, utilizando la herramienta Pilar en la que obtuvo riesgos críticos, y posteriormente propone un plan de mejora que permitirá mitigar las vulnerabilidades identificadas basado en la ISO/IEC 27001 (Bermeo, 2023).

2.2 Marco Teórico

2.2.1 Activo de Información

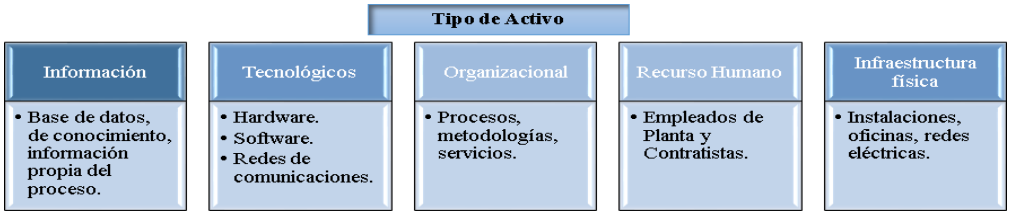
Para poder asegurar la TI (tecnología de la información) de la organización es necesario que se forme la cultura de seguridad de la información y gestión de riesgos, para lo cual es preciso que se defina un concepto esencial para la gestión de seguridad de la información y de riesgos "activo de información". Entiéndase activo de información como aquello que tiene valor y que forman parte del diario operar de las organizaciones y por tanto es necesario identificarlo, clasificarlo, analizar su nivel de tolerancia al riesgo y las contramedidas existentes y futuras que permitan asegurar que se encuentre disponible para los interesados (Leal, 2019).

Otra definición a considerar es la siguiente: es todo aquello que posea valor para el instituto, tales como: elementos de hardware, software, de procesamiento, almacenamiento y comunicaciones, bases de datos, información física y digital, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa, administrativa de la entidad (IGAC, 2018).

De acuerdo con la Agencia Nacional Digital, existen diferentes tipos de activos, en la cual los identifican y tipifican los activos de información como se observa en la figura 4 (Agencia Nacional Digital, 2020).

Figura 4

Tipo de activo



***Nota**: Adaptado de la Agencia Nacional Digital, por Quispe, V, E, 2020, (https://and.gov.co/sites/default/files/2022-05/Guia_De_Gestion_y_clasificacion_de_activos_de_informacon.pdf)*

2.2.2 Valoración de un Activo

La valoración del activo hace referencia a aquellas características que determinan la importancia que tiene un activo de información para un proceso de la institución, a través de una evaluación que se da al activo en términos de confidencialidad integridad y disponibilidad de la información (Daza, 2022). En la tabla 1, se refleja las valoraciones a considerar de un activo de información:

Tabla 1

Valoración de un activo

Dimensiones	Descripción
Confidencialidad	¿Qué daño causaría que lo conociera quien no debe? Esta valoración es típica de datos.
Integridad	¿Qué perjuicio causaría que estuviera dañado o corrupto? Esta valoración es típica de los datos, que pueden estar manipulados, ser total o parcialmente falsos o, incluso, faltar datos.

Disponibilidad	¿Qué perjuicio causaría no tenerlo o no poder utilizarlo? Esta valoración es típica de los servicios.
Autenticidad	¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa? Esta valoración es típica de servicios (autenticidad del usuario) y de los datos (autenticidad de quien accede a los datos para escribir o, simplemente, consultar).
Trazabilidad del acceso a los datos	¿Qué daño causaría no saber quién accede a qué datos y qué hace con ellos? Se reconocen habitualmente como dimensiones básicas la confidencialidad, integridad y disponibilidad.

Nota: *Adaptado de Metodología de análisis y gestión de riesgos de los sistemas de información libro I el método, por Quispe, V, E,2012, de Ministerio de hacienda y administraciones públicas, (p.24)*

En esta metodología se han añadido la autenticidad y el concepto de trazabilidad (del inglés, accountability), que a efectos técnicos se traducen en mantener la integridad y la confidencialidad de ciertos activos del sistema que pueden ser los servicios de directorio, las claves de firma digital, los registros de actividad (Magerit, 2012).

2.2.3 Riesgo

Dentro del ámbito de seguridad de la información, se considera al riesgo como la "Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información, se considera como una combinación de la probabilidad de un evento y sus consecuencias". El nivel de riesgo se puede "estimar y valorar cuantitativamente", como el producto del impacto, por la probabilidad de ocurrencia (Zevallos, 2019).

2.2.4 Tipos de Riesgo de Seguridad

Riesgo potencial. Riesgo sin tener en cuenta la aplicación de ningún tipo de salvaguarda.

Riesgo acumulado. Se calcula sobre un activo teniendo en cuenta el impacto acumulado sobre un activo y la frecuencia de la amenaza.

Riesgo repercutido. Se calcula sobre un activo teniendo en cuenta el impacto repercutido sobre un activo y la frecuencia de la amenaza (Sánchez, 2017).

Riesgo residual. Dado un cierto conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de riesgo que se denomina residual. Se dice que hemos modificado el riesgo, desde un valor potencial a un valor residual. El cálculo del riesgo residual es sencillo como no han cambiado los activos, ni sus dependencias, sino solamente la magnitud de la degradación y la probabilidad de las amenazas, se repiten los cálculos de riesgo usando el impacto residual y la probabilidad residual de ocurrencia (Magerit, 2012).

2.2.5 Impacto

Las organizaciones se ven afectadas cuando se origina una situación que infringe contra el mal funcionamiento de los servicios; estas secuelas reciben el nombre de impacto. Dicho de otra manera, el impacto es el alcance provocado o daño causado en caso de que se materialice una amenaza. (Luna & Simba, 2017). En una organización se puede detectar dos tipos de impacto los cuales son:

Impacto acumulado: Es el cálculo sobre un activo teniendo en cuenta; su valor acumulado y las amenazas a los que está expuesto, se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado y de la degradación causada.

Impacto repercutido: Es el cálculo sobre un activo teniendo en cuenta; su valor propio, y las amenazas a las que están expuestos los activos de los que depende. Se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor propio y de la degradación causada (Gonzaga, 2021).

2.2.6 Amenaza

Se define como una amenaza a cualquier acción o evento capaz de causar o no daño a los activos de una organización, mediante la modificación o destrucción de la información

lo cual puede ocasionar pérdidas materiales, económicas y de prestigio a la organización. Las amenazas surgen a partir de la existencia de vulnerabilidades, es decir que una amenaza sólo puede existir si existe una vulnerabilidad que pueda ser aprovechada, e independientemente de que se comprometa o no la seguridad de un sistema de información (Luna & Simba, 2017).

2.2.7 Clasificación de las Amenazas

Las amenazas en cada activo son diferentes según sus dimensiones, valoración de cada uno. Se las puede agrupar de la siguiente manera, como se observa en la figura 5.

Figura 5

Clasificación de las amenazas en un activo

***Nota**: Adaptado del trabajo de fin de master de Juan Salvador Díaz Pérez, 2020, (https://rua.ua.es/dspace/bitstream/10045/102087/1/Esquema_Director_de_Seguridad_para_Empresas_pymes_d_Diaz_Perez_Juan_Salvador.pdf)*

De origen natural. Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta como, por ejemplo; fuego, daño por agua.

Del entorno (origen industrial). Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.

Defectos en las aplicaciones. Problemas con origen el equipamiento propio por defectos en su diseño o en su implementación, fallos en las aplicaciones, hardware o equipos de transmisiones, producen consecuencias potencialmente negativas sobre el sistema. También se denominan vulnerabilidades técnicas.

Causadas por las personas de forma accidental. Errores accidentales de las personas que interactúan con la información. Las personas con acceso al sistema de información pueden ser causa de problemas no intencionados, por error o por omisión.

Causadas por las personas de forma deliberada. Errores deliberados de las personas que interactúan con la información. Las personas con acceso al sistema de información pueden de forma deliberada ser causa de problemas intencionados: acciones no autorizadas como uso de software o hardware no autorizados, funcionamiento incorrecto por abuso o robo de derechos de acceso o errores en el uso, falta de disponibilidad, información comprometida por robo de equipos, revelar secretos, espionaje, etc.

No todas las amenazas son susceptibles de afectar a todos los tipos de activos. Existe una cierta relación entre el tipo de activo y lo que le podría ocurrir. Además, tampoco afectan a todas las dimensiones (disponibilidad, integridad, confidencialidad, autenticidad o trazabilidad) por igual (Pérez, 2020).

2.2.8 Vulnerabilidad

Como menciona Torres (2021) una vulnerabilidad de seguridad es una falla o debilidad en un sistema de información que compromete su seguridad.

Es un "agujero" que puede ser causado por un error de configuración, falta de proceso o falla de diseño. Los ciberdelincuentes aprovechan las vulnerabilidades de los sistemas informáticos (como los sistemas operativos) para acceder a ellos y realizar actividades ilegales, robar información confidencial o interrumpir sus operaciones.

Las vulnerabilidades de seguridad son una de las principales razones por las que una empresa tiene un ataque informático en su sistema.

Es por eso, que los sistemas se deben actualizar a las últimas versiones, aplicaciones informáticas, sistemas de seguridad y sistemas operativos, ya que estas actualizaciones contienen muchas correcciones para las vulnerabilidades descubiertas (Zambrano, Vidal, & Vera, 2022).

2.2.9 Tipos de Vulnerabilidades

Las vulnerabilidades son el resultado de errores de programación (bugs), fallas en el diseño del sistema, incluidas en las limitaciones tecnológicas pueden ser explotadas por atacantes; a continuación, en la figura 6 se visualiza los tipos de vulnerabilidades en los activos de información.

Figura 6

Tipos de vulnerabilidades

***Nota**: Adaptado de Fundamentos de seguridad informática de Carlos Arturo Avenía Delgado, 2017, (https://core.ac.uk/download/pdf/326424171.pdf)*

Vulnerabilidades físicas. Debilidades en orden físico son las presentes en los entornos en los que la información se almacena o manipula. Ejemplos de este tipo de vulnerabilidad se pueden distinguir: instalaciones inadecuadas en el espacio de trabajo, la falta de recursos en los puestos de trabajo; disposición desordenada de los cables de alimentación y de red, la falta de identificación de personas y locales, entre otros.

Vulnerabilidades naturales. Debilidades naturales son los relacionados con las condiciones de la naturaleza que puedan poner en riesgo la información. A menudo, la humedad, el polvo y la contaminación pueden causar daños a los bienes.

Vulnerabilidades hardware. Posibles defectos de fabricación o la configuración de los equipos de la empresa que permitiría el ataque o alteración de la misma. Hay muchos elementos que representan debilidades de hardware. Entre ellos podemos mencionar: la falta de actualizaciones de acuerdo con las directrices de los fabricantes en los programas que se utilizan, y el mantenimiento inadecuado de los equipos.

Vulnerabilidades de software. Los puntos débiles que se producen en las aplicaciones permiten el acceso no autorizado a sistemas informáticos, incluso sin el conocimiento de un usuario o administrador de red.

Pueden ser proporcionadas por varias amenazas ya conocidas. Entre ellas están; una configuración incorrecta e instalación de programas informáticos, que pueden llevar a un mal uso de los recursos por usuarios maliciosos. A veces, la libertad de uso implica un mayor riesgo. Ejemplo: lectores de correo electrónico que permiten la ejecución de código malicioso, editores de texto que permiten la ejecución de los virus de macro, etc. Estas deficiencias ponen en riesgo la seguridad de los entornos tecnológicos.

Vulnerabilidades de medios de almacenaje. Si los medios de comunicación que almacenan información no se utilizan correctamente, el contenido de los mismos puede ser vulnerable a una serie de factores que pueden afectar la integridad, disponibilidad y confidencialidad de la información. Ejemplo: Los medios de almacenamiento pueden ser afectados por los puntos débiles que se pueden dañar o incluso dejarlos inservibles. Estas debilidades son: período de validez y defecto de fabricación, mal uso, ubicación de almacenamiento poco saludable de la humedad, el magnetismo o estática, moho, etc.

Vulnerabilidades de comunicación. Este tipo de debilidad se extiende a toda la información que transita por la red. Donde quiera que la información transite, ya sea a través de cable, satélite, fibra óptica u ondas de radio, tiene que haber seguridad. Los datos que viajan son un aspecto crucial al momento de aplicar la seguridad de la información.

Vulnerabilidades humanas. Esta categoría de vulnerabilidad está relacionada con el daño que pueden hacer las personas a la información y el entorno tecnológico que soporta**.**

La mayor vulnerabilidad es la falta de medidas de seguridad adecuadas para ser adoptada por cada elemento constituyente, principalmente miembros internos de la empresa. Dos debilidades humanas, por su grado de frecuencia son: la falta de formación específica para la ejecución de las actividades relacionadas con las funciones de cada uno, y la falta de conciencia sobre la seguridad a la rutina diarias de sus actividades, errores, omisiones (Delgado, 2017).

2.2.10 Salvaguardas

Consisten en medidas para tratar las posibles amenazas del sistema y reducir el riesgo total del mismo. Pueden ser procedimientos, como la documentación y gestión de incidentes, políticas de personal, soluciones técnicas o medidas de seguridad física de las instalaciones.

Las salvaguardas pueden ser preventivas si reducen la frecuencia de las amenazas, o paliativas, si reducen la degradación causada por las amenazas en los activos. Un caso especial de salvaguarda preventiva es aquélla que reduce la probabilidad de transmisión de fallos en la red de activos, disminuyendo la dependencia entre los activos terminales y los de soporte (Jiménez & Alfonso, 2015).

2.2.11 Tipos de Protección Prestados por las Salvaguardas

Hay que tener en cuenta los siguientes aspectos: tipo de activos a proteger, pues cada tipo se protege de una forma específica, dimensión o dimensiones de seguridad que requieren protección, amenazas de las que necesitamos protegernos, y si existen salvaguardas alternativas, para lo cual en la siguiente figura 7 se evidencia los tipos de protección prestados por las salvaguardas (Magerit, 2012).

Figura 7

Tipos de protección de salvaguardas

***Nota**: Adaptado de Magerit versión 3.0, libro I "Método", 2012, (https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html)*

A continuación, se describen cada uno de los tipos de protección de las salvaguardas de la figura 7.

Prevención. Es preventiva cuando reduce las oportunidades de que un incidente ocurra. Si la salvaguarda falla y el incidente llega a ocurrir, los daños son los mismos. Ejemplos: autorización previa de los usuarios, gestión de privilegios, planificación de capacidades, metodología segura de desarrollo de software, pruebas en pre-producción, segregación de tareas.

Disuasión. Es disuasoria cuando tiene un efecto tal sobre los atacantes que estos no se atreven o se lo piensan dos veces antes de atacar. Son salvaguardas que actúan antes del incidente, reduciendo las probabilidades de que ocurra; pero que no tienen influencia sobre los daños causados en caso de que el atacante realmente se atreva. Ejemplos: vallas elevadas, guardias de seguridad, avisos sobre la persecución del delito o persecución del delincuente.

Eliminación. Una salvaguarda elimina un incidente cuando impide que éste tenga lugar. Son salvaguardas que actúan antes de que el incidente se haya producido. No reducen los daños caso de que la salvaguarda no sea perfecta y el incidente llegue a ocurrir. Ejemplos: eliminación de cuentas estándar, de cuentas sin contraseña, de servicios innecesarios.

Minimización del impacto. Minimiza o limita el impacto cuando acota las consecuencias de un incidente. Ejemplos: desconexión de redes o equipos en caso de ataque, detención de servicios en caso de ataque, seguros de cobertura, cumplimiento de la legislación vigente.

Corrección. Es correctiva cuando habiéndose producido un daño, lo repara. Son salvaguardas que actúan después de que el incidente se haya producido y por tanto reducen los daños. Ejemplos: gestión de incidentes, líneas de comunicación alternativas, fuentes de alimentación redundantes.

Recuperación. Ofrece recuperación cuando permite regresar al estado anterior al incidente. Son salvaguardas que no reducen las probabilidades del incidente, pero acotan los daños en un periodo de tiempo. Ejemplo: copias de seguridad (back-up).

Monitorización. Son las salvaguardas que trabajan monitorizando lo que está ocurriendo o lo que ha ocurrido. Si se detectan cosas en tiempo real, podemos reaccionar atajando el incidente para limitar el impacto; si se detectan cosas a posteriori, podemos aprender del incidente y mejorar el sistema de salvaguardas de cara al futuro. Ejemplos: registros de actividad, registro de descargas de web.

Detección. Funciona detectando un ataque cuando informa de que el ataque está ocurriendo. Aunque no impide el ataque, sí permite que entren en operación otras medidas que atajen la progresión del ataque, minimizando daños. Ejemplos: antivirus, detectores de incendio.

Concienciación. Son las actividades de formación de las personas anexas al sistema que pueden tener una influencia sobre él. La formación reduce los errores de los usuarios, lo cual tiene un efecto preventivo. Adicionalmente, mejora las salvaguardas de todo tipo pues los que las operan lo hacen con eficacia y rapidez, potenciando su efecto o, al menos, disminuirlos por una mala operación. Ejemplos: cursos de concienciación, cursos de formación.

Administración. Se refiere a las salvaguardas relacionadas con los componentes de seguridad del sistema. Una buena administración evita el desconocimiento de lo que hay y por tanto impide considerar medidas de tipo preventivo. Ejemplos: inventario de activos, análisis de riesgos, plan de continuidad (Magerit, 2012).

2.2.12 Proceso de Análisis y Gestión del Riesgo

El análisis de riesgo es un proceso sistemático que permite definir los distintos niveles de exposición potencial de riesgos con los que conviven las organizaciones, con esto se busca identificar todos estos factores de riesgo, con el ánimo de generar procedimientos efectivos para el manejo de estos, buscando siempre eliminarlos y de no ser posible buscar mitigarlos hasta que el riesgo sea tolerable para la organización.

El objetivo general del análisis de riesgos, es identificar sus causas potenciales de los principales riesgos que amenazan el entorno informático.

Esta identificación se realiza en una determinada área para que se pueda tener información suficiente al respecto, optando así por un adecuado diseño e implantación de mecanismos de control con el fin de minimizar los efectos de eventos no deseados, en los diferentes puntos de análisis.

Otros objetivos específicos del proceso de análisis de riesgos son: analizar el tiempo, esfuerzo, recursos disponibles y necesarios para atacar los problemas; llevar a cabo un minucioso análisis de los riesgos y debilidades; identificar, definir y revisar los controles de seguridad; determinar si es necesario incrementar las medidas de seguridad; y la

identificación de los riesgos, los perímetros de seguridad y los sitios de mayor peligro, se pueden hacer el mantenimiento más fácilmente.

Los estándares más utilizados en la actualidad para la gestión del riesgo son: NIST RFM, Octave, y MAGERIT (Peña, 2019). En la figura 8, conforme con MAGERIT (2012), se describe los 8 pasos que intervienen en el análisis y gestión de riesgos.

Figura 8

Proceso de análisis y gestión de riesgos

***Nota**: Adaptado de Magerit versión 3.0, libro I "Método", 2012, (https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html)*

El análisis de riesgos determina impactos y riesgos. El resultado del análisis es sólo un análisis a partir de eso disponemos de información para tomar decisiones conociendo lo que queremos proteger (activos valorados=, de qué lo queremos proteger (amenazas valoradas) y qué hemos hecho por protegerlo (salvaguardas valoradas). Todo ello, sintetizado en los valores de impacto y riesgo (Magerit, 2012).

En consecuencia, en la siguiente figura 9, se resume las posibles decisiones que se pueden tomar tras haber estudiado los riesgos, indica que el estudio de riesgos dentro de sus opciones, refleja que el riesgo se evita, mitiga o se comparte.

Para lo cual el objetivo de la investigación de estudio consiste en la mitigación de los riesgos; al disminuir su probabilidad e impacto, al finalizar se debe realizar una monitorización continua y periódica. La caja 'estudio de los riesgos' pretende combinar el análisis con la evaluación.

Figura 9

Decisiones de tratamiento de los riesgos

***Nota**: Magerit v .3, Metodología de análisis y gestión de riesgos de los sistemas de información, libro I "Método", 2012, pág. 48, (https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html)*

2.2.13 Metodología MAGERIT

Es utilizada como método común para el marco de gestión de riesgos según los estándares ISO/IEC 27001. Esta metodología es sencilla y rápida de aplicar, proporciona buenos resultados sobre el estado del riesgo y puede utilizarse como base de apoyo al tomar decisiones para la mejora.

La metodología MAGERIT estipula los valores de los activos tomando en cuenta aspectos como la disponibilidad, integridad, confidencialidad, trazabilidad y autenticidad, con distintos grados de apreciación, como: muy alto, alto, medio, bajo, muy bajo y despreciable, en dicho método es comprobado el impacto estableciendo el valor de los activos, dicho acumulado es calculado por medio del valor del activo y las amenazas a las que se enfrenta, y dicha afectación resultante es tomada como el valor propio y las amenazas (Ramiro, 2020). Para el análisis de riesgos de sistemas de información se pueden emplear herramientas que soporten la metodología, como por ejemplo la herramienta Pilar.

2.2.14 Herramienta Pilar

PILAR, acrónimo de "Procedimiento Informático - Lógico para el Análisis de Riesgos", es una herramienta desarrollada bajo especificación del Centro Nacional de Inteligencia para soportar el análisis de riesgos de sistemas de información siguiendo la metodología MAGERIT.

La herramienta soporta todas las fases del método MAGERIT, también incorpora el "Catálogo de Elementos", permitiendo una homogeneidad en los resultados de análisis, sus resultados se presentan en varios formatos: informes RTF, gráficas y tablas para incorporar a hojas de cálculo, cabe destacar que hace uso de modelos cualitativos y cuantitativos (Magerit, 2012).

2.2.15 NIST Cybersecurity Framework

El marco de ciberseguridad del NIST (NIST CSF, NIST Cybersecurity Framework) consta de normas, pautas y mejores prácticas que ayudan a las organizaciones a mejor ar su gestión del riesgo de ciberseguridad, ya que está diseñado para ser flexible capaz de integrarse con los procesos de seguridad de cualquier organización, en cualquier sector.

De acuerdo con NIST (2018), las funciones proporcionan el nivel más alto de estructura para organizar actividades básicas de seguridad cibernética en categorías y subcategorías. Las cinco funciones son: identificar, proteger, detectar, responder y recuperar.

El marco de ciberseguridad del NIST incluye funciones, categorías, subcategorías y referencias informativas; ya que proporcionan planes de acción más concretos para departamentos o procesos específicos dentro de una organización. Las referencias informativas establecen una correlación directa entre las categorías, subcategorías y los controles de seguridad específicos de otros marcos. El NIST incluye al Center for Internet Security (CIS), COBIT 5, International Society of Automation, International Organization for Standardization, NIST SP 800-53, y NIST SP 800-30 (Yazmin, 2021).

2.2.16 NIST SP 800-30

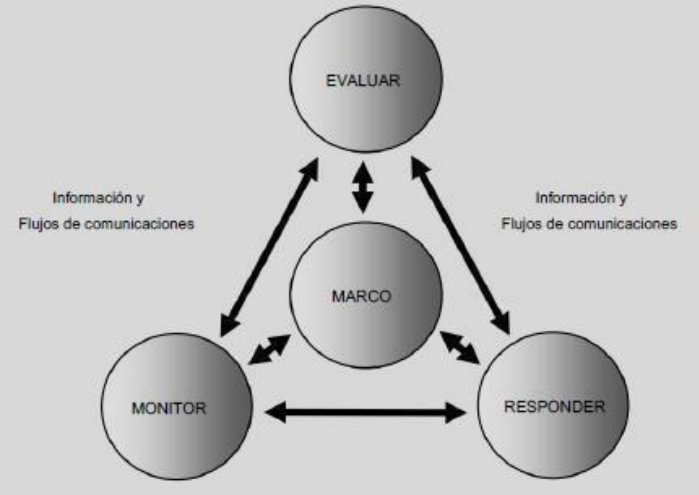
Es una metodología que fue elaborada para proporcionar una guía de evaluaciones de riesgos de los sistemas y organizaciones. Las evaluaciones de riesgos, llevadas a cabo en los tres niveles de la jerarquía de gestión de riesgos, son parte de un proceso general de gestión

de riesgos, proporcionando a los líderes un alto nivel de la información necesaria para determinar los cursos de acción adecuados en respuesta a los riesgos identificados (Omar & Vinicio, 2021).

La evaluación de riesgos es un componente clave de un proceso holístico de gestión de riesgos en toda la organización. Los procesos de gestión incluyen: enmarcar, evaluar, responder, y seguimiento del riesgo. La figura 10, ilustra los cuatro pasos en el proceso de gestión de riesgos, incluido el paso de la evaluación de riesgos y los flujos de información y comunicación necesarios para que el proceso funcione de manera efectiva (National Institute of Standards and Technology, 2012).

Figura 10

Evaluación de riesgos del proceso de gestión de riesgos



Nota: *National Institute of Standards and Technology, Guide for Conducting Risk Assessments 2012, pág. 4, (https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf)*

Correspondiente a los cuatro pasos del proceso de gestión de riesgos; enmarcar el riesgo describe el entorno en el que se toman las decisiones basadas en el riesgo; mientras que evaluar el riesgo su propósito es identificar amenazas, vulnerabilidades internas o externas de la organización, daños, y la probabilidad de que ocurra el daño; responder al riesgo aborda cómo las organizaciones responden al riesgo como por ejemplo, desarrollar cursos de acción, implementar respuestas de riesgos basados en los cursos de acción

seleccionados; y el seguimiento al riesgo verifica que se implementen las respuestas de riesgos planificadas y que se cumplan a lo largo del tiempo (National Institute of Standards and Technology, 2012).

Las organizaciones pueden utilizar una sola metodología de evaluación de riesgos o pueden emplear múltiples metodologías de evaluación, y la selección de una metodología específica depende, por ejemplo: del marco de tiempo para la planificación, la complejidad/madurez de la misión organizacional/procesos, la fase de los sistemas de información en el ciclo de vida del desarrollo de sistemas o la criticidad/sensibilidad de la información (National Institute of Standards and Technology, 2012).

2.2.17 Estándares Internacionales ISO/IEC 27001:2022

ISO/IEC 27001: 2022, es la norma ISO sobre sistema de gestión de seguridad de la información (SGSI). Las empresas que obtienen la certificación ISO/IEC 27001 cumplen con la protección de la información y los riesgos derivados de la necesidad por protección digital.

La ISO publicó los cambios el 15 de febrero de 2022, el nuevo título de ISO/IEC 27001:2022 es seguridad de la información, ciberseguridad y protección de la privacidad: controles de seguridad de la información, ahora proporciona una estructura de controles más transparentes que se pueden aplicar en toda la organización.

El número de categorías de control que se ha revisado ahora con 93 de 114 controles, distribuidos en cuatro categorías: organizacionales, personales, físicas y tecnológicas, de la cual 58 controles permanecen en su lugar con la actualización, 24 se han fusionado y 11 controles se han agregado (International Management Systems Marketing, 2022).

2.3. Marco legal

El desarrollo de la investigación, se sustentará en el cumplimiento de los siguientes reglamentos o normativas: el esquema nacional de seguridad, la ley de comercio electrónico, firmas electrónicas y mensaje de datos, la ley orgánica de transparencia y acceso a la información, y la ley orgánica y normas de control de la contraloría general del estado, a continuación, se detalla cada una de ellas.

2.3.1 Esquema Nacional de Seguridad

El análisis de riesgos puede venir requerido por precepto legal. Tal es el caso del Real Decreto 3/2010, del 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. En el Capítulo II, Principios Básicos, se dice:

Artículo 6. Gestión de la seguridad basada en los riesgos.

1. El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado.

2. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad.

El mismo Real Decreto 3/2010, en el Capítulo III, Requisitos Mínimos, establece en el:

Artículo 13. Análisis y gestión de los riesgos.

1. Cada organización que desarrolle e implante sistemas para el tratamiento de la información y las comunicaciones realizará su propia gestión de riesgos.

2. Esta gestión se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema. Sin perjuicio de lo dispuesto en el Anexo II, se empleará alguna metodología reconocida internacionalmente.

3. Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, que en su Artículo 1, Objeto de la Ley, dice así:

2. Las Administraciones Públicas utilizarán las tecnologías de la información de acuerdo con lo dispuesto en la presente Ley, asegurando la disponibilidad, el acceso, la

integridad, la autenticidad, la confidencialidad y la conservación de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias.

La Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, en su artículo 9 (Seguridad de los datos) expresa que:

El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural (Magerit, 2012).

En Ecuador, los siguientes documentos establecen normas para garantizar la seguridad de la información, entre ellos existen: la ley de comercio electrónico, firmas electrónicas y mensaje de datos, la ley orgánica de transparencia y acceso a la información pública, la ley orgánica y normas de control de la contraloría general del estado.

2.3.2 Ley de Comercio Electrónico, Firmas Electrónicas y Mensaje de Datos

En el capítulo I, principios generales, expide lo siguiente:

Art. 5.- Confidencialidad y reserva. - Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta ley y demás normas que rigen la materia.

Art. 9.- Protección de datos. - Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros. La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta ley, los cuales podrán ser utilizados o transferidos únicamente

con autorización del titular u orden de autoridad competente (Asamblea Nacional de Ecuador, 2021).

2.3.3 Ley Orgánica de Transparencia y Acceso a la Información Pública

En el título segundo, de la información pública y su difusión, expide la presente:

Art. 6.- Información Confidencial. - Se considera información confidencial aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales, especialmente aquellos señalados en los artículos 23 y 24 de la Constitución Política de la República. El uso ilegal que se haga de la información personal o su divulgación dará lugar a las acciones legales pertinentes.

Art. 10.- Custodia de la Información.- Es responsabilidad de las instituciones públicas, personas jurídicas de derecho público y demás entes señalados en el artículo 1 de la presente Ley, crear y mantener registros públicos de manera profesional, para que el derecho a la información se pueda ejercer a plenitud, por lo que, en ningún caso se justificará la ausencia de normas técnicas en el manejo y archivo de la información y documentación para impedir u obstaculizar el ejercicio de acceso a la información pública, peor aún su destrucción. Los documentos de una institución que desapareciere pasarán bajo inventario al Archivo Nacional y en caso de fusión interinstitucional, será responsable de aquello la nueva entidad (Nacional, 2004).

2.3.4 Ley Orgánica y Normas de Control de la Contraloría General del Estado

Mediante el acuerdo No. 004-CG-2023, tiene por objeto dar a conocer las normas de control interno para las entidades, organismos del sector público y de las personas jurídicas de derecho privado que dispongan de recursos públicos, manifiesta que:

300-01 Identificación y análisis de riesgos: Es imprescindible identificar y analizar, tanto cuantitativa como cualitativamente, los riesgos que enfrenta una entidad en la búsqueda de sus objetivos y la protección de sus recursos.

Algo fundamental para la evaluación de riesgos, incluyendo el riesgo de fraude y corrupción, es la existencia de un proceso permanente para identificar el cambio de

condiciones gubernamentales, económicas, industriales, regulatorias y operativas, respecto de una situación inicial.

300-02 Valoración de los riesgos: La administración debe valorar los riesgos a partir de dos perspectivas, probabilidad e impacto, siendo la probabilidad la posibilidad de ocurrencia, mientras que el impacto representa el efecto frente a su ocurrencia. Se consideran factores de alto riesgo potencial los programas o actividades complejas, el manejo de dinero en efectivo, la alta rotación y crecimiento del personal, el establecimiento de nuevos servicios, sistemas de información rediseñados, crecimientos rápidos, nueva tecnología, formas de gestionar la documentación de sustento, competencia profesional, entre otros.

300-03 Respuesta al riesgo: La consideración del manejo del riesgo y la selección e implementación de una respuesta son parte integral de la administración de los riesgos. Los modelos de respuestas al riesgo pueden ser: evitar, reducir, compartir y aceptar.

300-04 Plan de mitigación de riesgos: En el plan de mitigación de riesgos se desarrollará una estrategia de gestión, que incluya su proceso e implementación. Se incluirán las actividades de control establecidas para manejar los riesgos, metas, cronogramas, indicadores de eficacia y efectividad y responsables por áreas relacionadas (Contraloria General del Estado, 2023).

2.3.5 Código Orgánico Integral Penal (COIP)

La Asamblea Nacional de acuerdo con el artículo 84 de la Constitución, tiene la obligación de adecuar, formal y materialmente, las leyes y demás normas jurídicas a los derechos previstos en la Constitución e instrumentos internacionales. En ejercicio de sus atribuciones constitucionales y legales expide el siguiente:

Sección Tercera: Delitos contra la seguridad de los activos de los sistemas de información y comunicación.

Art. 229.- Revelación ilegal de base de datos. - La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del

secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años.

Art. 230.- Interceptación ilegal de datos. - Será sancionada con pena privativa de libertad de tres a cinco años:

1. La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.

2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.

3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.

4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior.

Art. 231.- Transferencia electrónica de activo patrimonial. - La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años.

Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona.

Art. 232.- Ataque a la integridad de sistemas informáticos. - La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años.

Art. 233.- Delitos contra la información pública reservada legalmente. - La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años. La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años.

Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información, será sancionado con pena privativa de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis meses, siempre que no se configure otra infracción de mayor gravedad.

Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones. – La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años (Código Orgánico Integral Penal, 2014).

2.3.6 Ley Orgánica de Protección de Datos Personales

En uso de la atribución que le confiere el número 6 del artículo 120 de la Constitución de la República, expide la siguiente:

Art. 38.-Medidas de seguridad en el ámbito del sector público. -El mecanismo gubernamental de seguridad de la información deberá incluir las medidas que deban implementarse en el caso de tratamiento de datos personales para hacer frente a cualquier riesgo, amenaza, vulnerabilidad, accesos no autorizados, pérdidas, alteraciones, destrucción o comunicación accidental o ilícita en el tratamiento de los datos conforme al principio de seguridad de datos personales.

Art. 40.-Análisis de riesgo, amenazas y vulnerabilidades. -Para el análisis de riesgos, amenazas y vulnerabilidades, el responsable y el encargado del tratamiento de los datos personales deberán utilizar una metodología que considere, entre otras:

- Las particularidades del tratamiento;
- Las particularidades de las partes involucradas; y,
- Las categorías y el volumen de datos personales objeto de tratamiento.

Art. 41.-Determinación de medidas de seguridad aplicables. -Para determinar las medidas de seguridad, aceptadas por el estado de la técnica, a las que están obligadas el responsable y el encargado del tratamiento de los datos personales, se deberán tomar en consideración, entre otros:

- Los resultados del análisis de riesgos, amenazas y vulnerabilidades;
- La naturaleza de los datos personales;
- Las características de las partes involucradas; y,
- Los antecedentes de destrucción de datos personales, la pérdida, alteración, divulgación o impedimento de acceso a los mismos por parte del titular, sean accidentales e intencionales, por acción u omisión, así como los antecedentes de transferencia, comunicación o de acceso no autorizado o exceso de autorización de tales datos.

El responsable y el encargado del tratamiento de datos personales deberán tomar las medidas adecuadas y necesarias, de forma permanente y continua, para evaluar, prevenir, impedir, reducir, mitigar y controlar los riesgos, amenazas y vulnerabilidades, incluidas las que conlleven un alto riesgo para los derechos y libertades del titular, de conformidad con la normativa que emita la Autoridad de Protección de Datos Personales.

Art. 42.-Evaluación de impacto del tratamiento de datos personales. -El responsable realizará una evaluación de impacto del tratamiento de datos personales cuando se haya identificado la probabilidad de que dicho tratamiento, por su naturaleza, contexto o fines, conlleve un alto riesgo para los derechos y libertades del titular o cuando la Autoridad de Protección de Datos Personales lo requiera (Ley orgánica de protección de datos personales, 2021).

Capítulo III

3. Marco Metodológico

3.1 Descripción del Área de Estudio

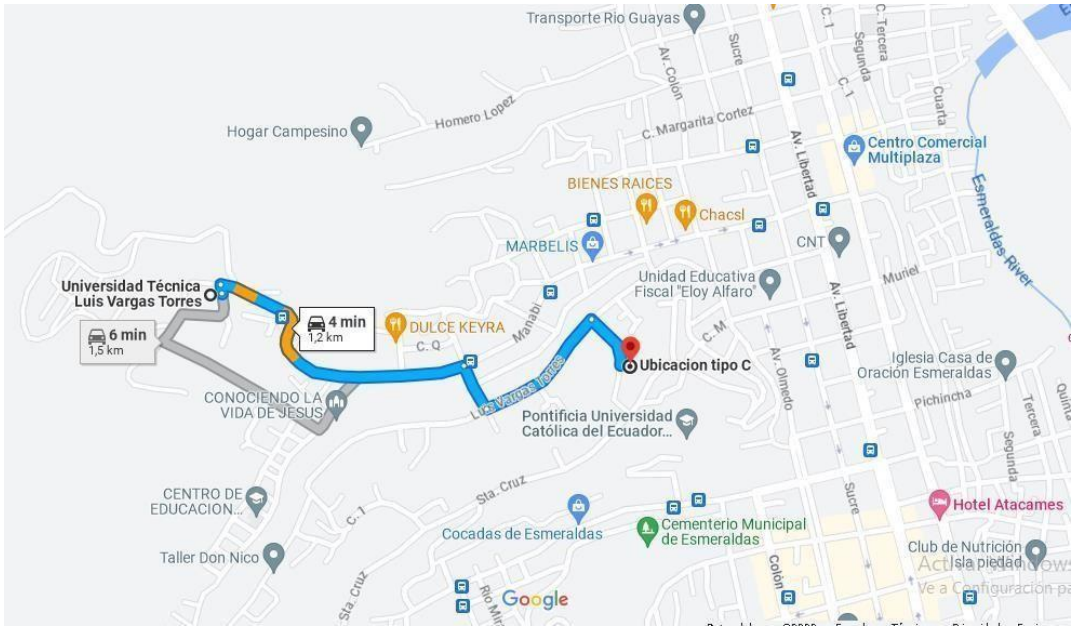
El presente trabajo de investigación se desarrolló en la Universidad Técnica Luis Vargas Torres de Esmeraldas, donde el área de estudio es el personal del área de TIC, orientada en el campo de seguridad.

3.1.1 Ubicación

La Universidad Técnica Luis Vargas Torres de Esmeraldas. Es una entidad autónoma de derecho público sin fines de lucro financiada por el Estado, está ubicada en la ciudad de Esmeraldas, provincia de Esmeraldas, al noroeste de Ecuador. En la figura 11, se visualiza el mapa de ubicación de la institución.

Figura 11

Ubicación del área de estudio



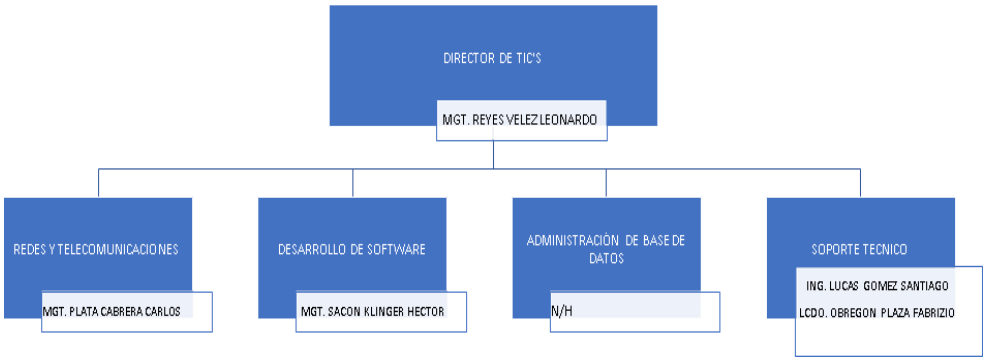
***Nota**: Se observa la ubicación del área a investigar, adaptado del mapa de Google, 2023.*

3.1.2 Organigrama Funcional

En la figura 12, se muestra la estructura del área de TIC, distribuida de la siguiente manera: l Director, y cuatro puestos de trabajo que son: Redes y comunicaciones, Desarrollo de Software. Administración de Base de Datos y Soporte Técnico.

Figura 12

Organigrama del Área de TIC.



***Nota**: Elaborado por el Ing. Leonardo Reyes, director de TIC, 2023.*

3.2 Enfoque y Tipo de Investigación

El objeto fundamental del tema de estudio es la investigación cualitativa, la cual permite recoger descripciones a través de la aplicación de técnicas e instrumentos como la observación y la entrevista, con el fin de obtener información en forma de narraciones, grabaciones, notas de campo, registros escritos, transcripciones de audio y video, fotografías, entre otros. El investigador está en constante interacción con los participantes y con los datos, para de esta forma encontrar las respuestas (Neill & Suárez, 2018).

Dentro de la investigación cualitativa podemos encontrar diversas técnicas como: la observación, la observación participante, la entrevista, la entrevista grupal, el cuestionario, el grupo de discusión (Juan, 2017).

Por consiguiente, el desarrollo del trabajo de investigación tuvo un enfoque cualitativo, debido a que el tamaño de la muestra es pequeño, por tal razón, el método de recolección de datos fue basado en la interacción personal, donde se aplicó entrevistas estructuradas y no estructuradas, además se utilizó la observación.

El tipo de investigación que se llevó a cabo se sustenta bajo tres modalidades:

Investigación documental

Según Alfonso (1995), la investigación documental es un procedimiento científico, un proceso sistemático de indagación, recolección, organización, análisis e interpretación de información o datos en torno a un determinado tema. Al igual que otros tipos de investigación, este conduce a la construcción de conocimientos (Ojeda & Palacios, 2018).

La investigación documental permitió estudiar trabajos de investigación, libros, artículos web, blogs, sitios web, entre otros, con la finalidad de recopilar, y organizar la información y a partir de la lectura y análisis realizar la construcción de la base teórica del área a investigar.

Investigación de campo

De acuerdo con Fidias G. Arias (2012), la investigación de campo es aquella que consiste en la recolección de datos directamente de los sujetos investigados, o de la realidad donde ocurren los hechos (datos primarios), sin manipular o controlar variable alguna, es decir, el investigador obtiene la información, pero no altera las condiciones existentes. La investigación de campo, al igual que la documental, se puede realizar a nivel exploratorio, descriptivo y explicativo (Arias, 2012).

Conforme a lo mencionado anteriormente, a través de la observación se recogió datos e información en el área de TIC de la Universidad Técnica Luis Vargas Torres de Esmeraldas que permitió el avance de cada una de las etapas del proyecto.

Investigación Aplicada

Este tipo de investigación recurre a los conocimientos ya alcanzados en la investigación básica para encaminarlos al cumplimiento de objetivos específicos; por tanto, este tipo de investigación considera todo el conocimiento existente en un área concreta, que será aplicado en el intento de solucionar problemas específicos.

Los resultados de la investigación aplicada pretenden, en primer lugar, enfocarse en la validación de posibles implementaciones de productos, prototipos o modelos

materializados en los niveles de transferencias y madurez tecnológicas (Maldonado.J., Macho.L.K., & Casallas.E., 2023).

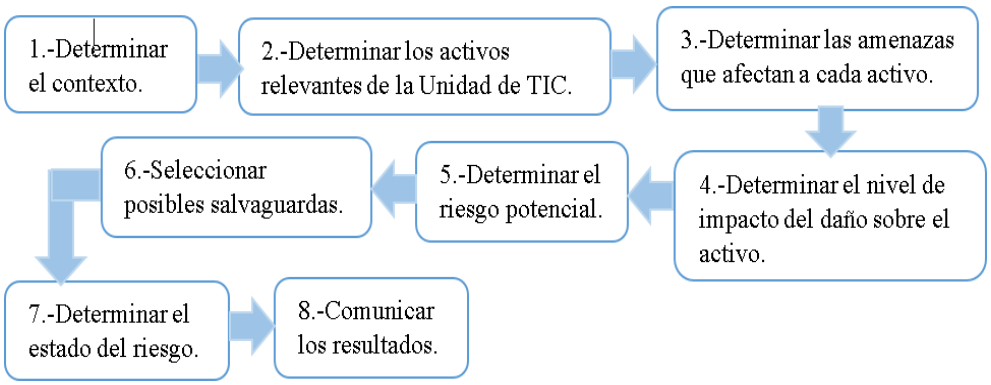
A partir de este tipo de investigación, se determinó aplicar los procedimientos de las metodologías MAGERIT v. 3 y NIST SP 800-30.

3.3 Procedimiento de la Investigación

La siguiente figura 13, recoge los procesos del análisis y gestión de riesgos del procedimiento a investigar, cuyos pasos se detallan de cada uno a continuación:

Figura 13

Proceso del análisis de riesgos



***Nota**: EL proceso a realizarse consta de 8 fases, adaptado de Magerit versión 3.0, libro I "Método", 2012, (https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html)*

3.3.1 Determinar el contexto

Esta actividad consistió en el levantamiento de información inicial, es decir, define el alcance y límites para la gestión del riesgo que se llevó a cabo en la Unidad de TIC, de la Universidad Técnica Luis Vargas Torres de Esmeraldas.

3.3.2 Determinar los activos relevantes de la Unidad de TIC.

Para la realización de esta actividad se contó con la información de todos los activos de hardware con los que dispone el departamento de TIC, para ello fue necesario la obtención de un inventario tecnológico.

De acuerdo a la UNE (acrónimo de Una Norma Española), considera un activo como un componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos (Magerit, 2012).

Se debe precisar que los activos de información son diferentes dependiendo del riesgo, vulnerabilidades o salvaguardas que presentan de acuerdo a sus características, para lo cual se los categoriza de acuerdo al apéndice 2, en la tabla 2, conforme al catálogo de elementos del libro II del MAGERIT.

Tabla 2

Descripción del inventario de activos

Equipos informáticos (Hardware)												
								Dimensiones				
Nº	Cantidad	Nombre	Descripción	Unidad responsable	Persona responsable	Ubicación	D	I	C	A	T

Nota: *En la dimensión de activos se dará el valor de acuerdo a la integridad (I), Confidencialidad (C), Autenticidad (A), y Trazabilidad (T), Adaptado de Metodología de análisis y gestión de riesgos de los sistemas de información libro II catálogo de elementos, por Quispe, V, E,2012, de Ministerio de hacienda y administraciones públicas, (p.60)*

3.3.3 Determinar las amenazas que afectan a cada activo.

De acuerdo a la UNE 71504:2008 (acrónimo de Una Norma Española), se considera una amenaza como una causa potencial de un incidente que puede causar daños a un sistema de información o a una organización.

Dentro del capítulo 5 del catálogo de elementos de la guía II del libro de MAGERIT, presenta una relación de amenazas típicas que se pueden clasificar de la siguiente manera: de origen natural, del entorno (origen industrial), defectos de las aplicaciones, causadas por las personas de forma accidental, causadas por las personas de forma deliberada (Magerit, 2012).

En este proceso, se realizará una valoración de las amenazas detectadas en cada activo, como se muestra a continuación, en la tabla 3.

Tabla 3

Descripción del tipo de amenaza en cada activo

(Código de activo) Descripción del tipo de amenaza	
Tipos de activos:	Dimensiones:
Que pueden ser afectados por ese tipo de amenaza	Pueden verse afectadas por ese tipo de amenaza, ordenadas de más a menos relevante.
Descripción: Detalles de la amenaza, lo que puede ocurrir a activos del tipo indicado con las consecuencias indicadas, es decir, se describe el tipo de amenaza existente sobre cada activo.	

Nota: *Se describe la amenaza por cada activo según las dimensiones afectadas de acuerdo al Libro II, adaptado de Metodología de análisis y gestión de riesgos de los sistemas de información, por Quispe, V, E,2012, de Ministerio de hacienda y administraciones públicas, (p.25)*

Una vez que se ha determinado que una amenaza puede perjudicar a un activo, con los valores cualitativos en la tabla 4, se valora su influencia en el activo en dos sentidos: degradación y probabilidad.

Tabla 4

Valoración de una amenaza sobre un activo

MA	Muy alta	Casi seguro	Fácil

A	Alta	Muy alto	Medio
M	Media	Posible	Difícil
B	Baja	Poco probable	Muy difícil
MB	Muy baja	Muy raro	Extremadamente difícil

***Nota**: Degradación, cuan perjudicado resultaría el valor del activo, adaptado de Metodología de análisis y gestión de riesgos de los sistemas de información, Libro I, 2012, por Quispe, V, E, de Ministerio de hacienda y administraciones públicas, (p.27)*

Adicionalmente, en la tabla 5, se utiliza la escala de valoración para determinar la frecuencia de cada amenaza que afecta en cada activo.

Tabla 5

Valoración de una amenaza sobre un activo

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

***Nota**: Probabilidad, cuan probable o improbable es que se materialice la amenaza, adaptado de Metodología de análisis y gestión de riesgos de los sistemas de información, Libro I, 2012, por Quispe, V, E, de Ministerio de hacienda y administraciones públicas, (p.27).*

3.3.4 Determinar el nivel de impacto del daño sobre el activo.

Se considera el nivel de impacto conociendo el valor de los activos en las dimensiones y la degradación, en este proceso se puede obtener el impacto acumulado y el impacto repercutido. El impacto acumulado se puede calcular por las amenazas a las que esté expuesto y de su valor acumulado, mientras que el impacto repercutido se basa teniendo en cuenta su valor propio y las amenazas a las que están expuestos.

3.3.5 Determinar el riesgo potencial.

Una vez identificado el impacto sobre las amenazas de los activos, el riesgo aumenta con el impacto y la probabilidad, para lo cual se calculará el riesgo acumulado y el riesgo repercutido (Magerit, 2012).

3.3.6 Seleccionar posibles salvaguardas.

Las salvaguardas pueden ser preventivas, si reducen la frecuencia de las amenazas, o paliativas, si reducen la degradación causada por las amenazas en los activos. Un caso especial de salvaguarda preventiva es aquélla que reduce la probabilidad de transmisión de fallos en la red de activos, disminuyendo la dependencia entre los activos terminales y los de soporte (Jiménez & Alfonso, 2015).

Las salvaguardas permiten reducir la probabilidad de las amenazas y además limitan el daño causado. Para seleccionar salvaguardas, de acuerdo al MAGERIT, se debe tomar en cuenta los siguientes aspectos: tipos de activos a proteger, dimensiones de seguridad, amenazas, si hay salvaguardas alternativas. Se debe considerar los tipos de protección: prevención, disuasión, eliminación, minimización del impacto, corrección, recuperación, monitorización, detección, concienciación, y administración (Magerit, 2012).

3.3.7 Determinar el estado del riesgo.

Se realiza una estimación del impacto residual y riesgo residual, y una vez procesados todos los datos de las actividades anteriores, se vuelven a repetir los cálculos con las nuevas medidas y procedimientos aplicados.

3.3.8 Comunicar los resultados.

Explicar en forma breve y clara sobre los procedimientos llevados a cabo y sobre los resultados obtenidos al personal del área de TIC, teniendo en cuenta que toda medida, políticas de seguridad de la información, normativas, reglamentos vigentes o procedimientos sugeridos debe estar apoyada por el departamento de TIC (Magerit, 2012).

3.4 Consideraciones Bioéticas

Para el desarrollo y ejecución de cada una de las actividades plasmadas en el cronograma, el Jefe del área de TIC emitirá un documento de respaldo que indique la autorización para acceder a la información, catálogo de inventarios, visitas técnicas necesarias para el cumplimiento de la investigación. Asimismo, se le notificará al personal del área de TIC, todo en cuanto al procedimiento a efectuar.

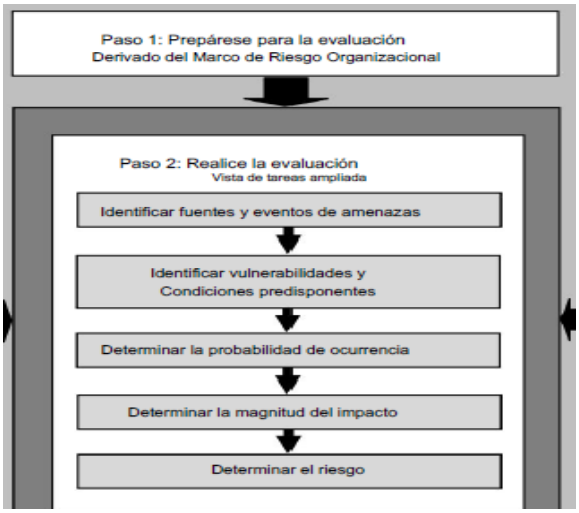
3.5 Identificación de los Riesgos en los Equipos de Hardware del Área de TIC

3.5.1 Proceso de Gestión de la Metodología NIST SP 800-30

En la figura 14, se ilustra los pasos básicos del proceso de evaluación y se destaca las tareas específicas que se llevó a cabo, y son las siguientes: prepararse para la evaluación, realizar la evaluación y comunicar los resultados, por ultimo mantener la evaluación de riesgos, a continuación, se detalla cada una de estas tareas.

Figura 14

Proceso de evaluación de riesgos



***Nota*:** *Adaptado de National Institute of Standards and Technology, Guide for Conducting Risk Assessments 2012, pág 23, (https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf)*

Paso 1. Prepararse para la Evaluación

Incluye las siguientes tareas: identificar el propósito y el alcance de la evaluación, identificar las suposiciones y restricciones asociadas con la evaluación, identificar las fuentes

de información que se utilizaron como insumos y se identificó el modelo de riesgo y los enfoques analíticos (National Institute of Standards and Technology, 2012)**.**

Tarea 1.1 Identificar el propósito

Conforme con MinTic (Ministerio de Tecnologías de la Información y las Comunicaciones) en Colombia, el propósito de la gestión de riesgo puede ser:

- Dar soporte al modelo de seguridad de la información al interior de la entidad.
- Preparación de un plan de respuestas a incidentes.
- Descripción de los requisitos de seguridad de la información para un producto, servicio o un mecanismo (MINTIC, 2016).

Es por ello, que el análisis de riesgos de la seguridad en la infraestructura de hardware del área de TIC de la Universidad Técnica Luis Vargas Torres de Esmeraldas se realizó debido a los problemas que se han suscitado a medida del tiempo, con la finalidad de mitigar los riesgos a los que están expuestos los activos de hardware y una vez obtenidos los resultados, adoptar medidas necesarias para proteger la seguridad de la información, potenciando al logro de los objetivos de la Institución.

Tarea 1.2 Identificar el alcance

El desarrollo de la investigación se llevó a cabo en el equipamiento de hardware, una vez recolectada la información, que se detalla en la tabla 6, donde indica el registro de los activos que fueron identificados correspondientes al departamento de TIC.

Tabla 6

Identificación del alcance

N°	Cantidad	Nombre	Descripción	Ubicación
A01	1	Servidor	Servidor de base de datos	Centro de datos

			Servidor de aplicaciones	
			Servidor de antivirus – virtual	
			Servidor de archivos – Virtual	
A02	5	Computadores	Computadores personales	Área de TIC
A03	1		Computadores de soporte	Área de TIC
A04	1		Computador servidor	Centro de datos
A05	2	Almacenamiento de datos	Discos duros locales	Área de TIC
A06	1		Discos duros externos	Área de TIC
A07	1	Periféricos de impresión	Impresora monocromática	Área de TIC
A08	1	Soporte de red	Router – Mikrotik	Centro de datos
A09	3		Switch – Cisco	Centro de datos
A10	3		UPS	Centro de datos
A11	8		Transceiver	Centro de datos
A12	1		NVR	Centro de datos
A13	1		PBX IP	Centro de datos
A14	5	Central telefónica	Teléfonos IP	Área de TIC
A15	1	Sistema de control de acceso	Biométrico	Área de TIC

A16	1	Equipo de videovigilancia	Cámara IP, Hik – Vision	Área de TIC
A17	1	Equipo eléctrico	Generador eléctrico	Centro de datos
A18	1	Equipo de climatización	Aire acondicionado	Área de TIC

***Nota**: Se evidencia 18 activos del área de TIC con su respectiva ubicación, elaboración propia.*

Tarea 1.3 Identificar las suposiciones y restricciones

El área de TIC cuenta con activos primarios, que se refiere a la información y actividades que realiza, y con activos de soporte; entre ellos la infraestructura de hardware, redes y comunicaciones, soporte de información, aplicaciones informáticas, instalaciones, y talento humano. En este proceso los activos que van a estar sometidos al análisis y mitigación de la gestión de riesgo, son 18 activos de infraestructura de hardware, debido a los permisos otorgados por la Universidad Técnica Luis Vargas Torres de Esmeraldas.

Tarea 1.4 Identificar fuentes de información

El medio por el cual se procedió a obtener la información fue a través de la observación, aplicación de encuestas y entrevistas en el departamento de TIC, para lo cual en la figura 12, se encuentra el organigrama estructural, donde constan las diferentes áreas: director de TIC, soporte técnico, administración de base de datos, desarrollo de software, redes y telecomunicaciones; el mismo que brinda los servicios tecnológicos con el fin de cumplir los objetivos de la institución.

Tarea 1.5 Identificar modelo de riesgo y enfoque analítico

El proceso de evaluación de riesgos de la publicación especial 800-30 incluye: una visión general de alto nivel de proceso de evaluación, las actividades necesarias para prepararse y realizar una evaluación de riesgos, las actividades necesarias para comunicar los resultados, compartir información relacionada con los riesgos y para mantener los resultados de una evaluación de riesgos (National Institute of Standards and Technology, 2012).Conforme al enfoque analítico se utilizó las siguientes técnicas: observación, encuestas y entrevistas.

Paso 2. Realizar la Evaluación

La realización de la evaluación de riesgo incluye las siguientes tareas específicas: identificar las fuentes de amenazas relevantes, los eventos de amenazas que producen esas fuentes y las vulnerabilidades que podrían ser expuestas por fuentes de amenazas, la probabilidad y el impacto adverso.

Tarea 2.1 Identificar fuentes de amenazas

En la guía para la dirección de evaluaciones de riesgos; la publicación NIST 800 -30 ofrece posibles fuentes de amenazas la cual detalla en su apéndice D. En consecuencia, para determinar si las fuentes de amenazas son relevantes para la organización y si están dentro del alcance, se evaluó de acuerdo a la capacidad, intención y objetivos del adversario; la cual se usó las tablas propuestas en la guía. En la tabla 7, se observa la escala de evaluación asignada según la capacidad, intención y orientación del adversario, obtenidos en los resultados de los anexos 2.1.

Tabla 7

Identificación de amenazas adversariales

Identificador	Activo	Origen de la amenaza	Capacidad	Intención	Orientación
A01	Servidor	Insider de confianza	Moderado	Moderado	Alto
A02	Computador personal	Insider privilegiado	Moderado	Moderado	Alto
A04	Computador servidor	Insider privilegiado	Moderado	Moderado	Moderado
A15	Biométrico	Información confidencial	Moderado	Moderado	Moderado

***Nota**: Adaptado de National Institute of Standards and Technology, Guide for Conducting Risk Assessments 2012, (https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf)*

Por otro lado, en la tabla 8, se muestra el origen de la amenaza y la escala de evaluación donde se obtuvo nueve activos en nivel moderado y cinco activos en nivel bajo conforme a las amenazas no adversariales asignadas de acuerdo con la gama de efectos obtenidos en los resultados de los anexos 2.1.

Tabla 8

Identificación de amenazas no adversariales

Identificador	Activo	Origen de la amenaza	Rango de efectos
A03	Computadores de soporte	Estructural	Bajo
A05	Discos duros locales	Accidental	Moderado
A06	Discos duros externos	Accidental	Moderado
A07	Impresora monocromática	Accidental	Bajo
A08	Router – Mikrotik	Estructural	Moderado
A09	Switch – Cisco	Estructural	Moderado
A10	UPS	Estructural	Moderado
A11	Transceiver	Estructural	Moderado
A12	NVR	Estructural	Moderado
A13	PBX IP	Estructural	Bajo
A14	Teléfonos IP	Accidental	Bajo
A16	Cámara IP, Hik – Vision	Accidental	Bajo
A17	Generador eléctrico	Ambiental	Moderado

A18	Aire acondicionado	Estructural	Moderado

***Nota*:** *Adaptado de National Institute of Standards and Technology, Guide for Conducting Risk Assessments 2012, pág 68, (https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf)*

Tarea 2.2 Identificar eventos de amenazas

En la identificación de eventos de amenazas potenciales, se determinó la relevancia de los eventos y las fuentes de amenazas que podrían iniciar los eventos. Una sola fuente de amenaza puede potencialmente iniciar múltiples eventos de amenaza (National Institute of Standards and Technology, 2012).

Basados en los criterios definidos por la metodología NIST SP 800-30, se definieron los eventos de amenazas asociados por el tipo de fuente de amenazas adversariales y no adversariales anteriormente descritas en las tablas 7 y 8. Para determinar la relevancia de los eventos de amenazas se utilizó los valores como se indica en la figura 15.

Figura 15

Relevancia de los eventos de amenaza

TABLA E-4: RELEVANCIA DE LOS EVENTOS DE AMENAZA

Valor	Descripción
Confirmado	La organización ha visto el evento de amenaza o TTP.
Esperado	El evento de amenaza o TTP ha sido visto por los compañeros o socios de la organización.
Anticipado	El evento de amenaza o TTP ha sido informado por una fuente confiable.
Predicho	El evento de amenaza o TTP ha sido predicho por una fuente confiable.
Posible	El evento de amenaza o TTP ha sido descrito por una fuente algo creíble.
N / A	El evento de amenaza o TTP no es aplicable actualmente. Por ejemplo, un evento de amenaza o TTP podría asumir tecnologías específicas, arquitecturas o procesos que no están presentes en la organización, misión/proceso comercial, segmento de EA o sistema de información; o condiciones predisponentes que no están presentes (p. ej., ubicación en una llanura aluvial). Alternativamente, si la organización está utilizando información detallada o específica sobre amenazas, un evento de amenaza o TTP podría considerarse inaplicable porque la información indica que no se espera que ningún adversario inicie el evento de amenaza o use el TTP.

***Nota*:** *National Institute of Standards and Technology, Guide for Conducting Risk Assessments 2012, pág 26, (https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf)*

En la tabla 9, se visualiza los eventos de amenazas de los activos con su respectiva relevancia, que determina si el evento de amenaza ha sido visto, informado, predicho,

descrito o no se aplica en la actualidad por el personal del departamento de TIC, la cual se determinó a través de las observaciones y de entrevistas dirigidas al personal de TIC.

Tabla 9

Relevancia de los eventos de amenaza

Identificador	Activo	Evento de amenaza	Origen de la amenaza	Relevancia
A01	Servidor	-Ataques de phishing. -Ataque simple de denegación del servicio. -Errores de mantenimiento/actualización de equipos. -Ingeniería social. -Alteración y fuga de la información.	Insider de confianza	Confirmado
A02	Computadores personales	-Ataques de phishing. -Obtención de información confidencial y no autorizada. -Errores de usuarios. -Errores de configuración, actualización. -Alteración y fuga de la información. -Uso no previsto. -Abuso de uso de privilegios de acceso.	Insider privilegiado	Confirmado

A03	Computadores de soporte	-Ataques de phishing. -Alteración o destrucción de la información. -Pérdida de equipos. -Errores de usuarios. -Alteración y fuga de la información. -Errores de configuración, actualización.	Estructural	N/A
A04	Computador servidor	-Ataques de phishing. -Errores de mantenimiento/actualización de equipos. -Suplantación de la identidad del usuario. -Pérdida de equipos. -Errores del administrador. -Manipulación de la configuración. -Alteración y fuga de la información. -Abuso de uso de privilegios de acceso.	Insider privilegiado	Confirmado
A05	Discos duros locales	-Error de disco. -Error de disco generalizado. -Errores de mantenimiento/actualización de equipos. -Deficiencia en los protocolos de almacenamiento. -Pérdida o robo de equipo.	Accidental	Confirmado

		-Alteración y destrucción de la información.		
A06	Discos duros externos	-Errores de mantenimiento/actualización de equipos. -Deficiencia en los protocolos de almacenamiento. -Alteración y destrucción de la información. -Pérdida o robo de equipo.	Accidental	Confirmado
A07	Impresora monocromática	-Daños por agua. -Avería de origen físico o lógico. -Errores de mantenimiento/actualización de equipos. -Errores de usuario y de configuración.	Accidental	N/A
A08	Router – Mikrotik	-Errores de mantenimiento/actualización de equipos. -Ataque destructivo. -Abuso de privilegios. -Acceso no autorizado. -Robo de quipo.	Estructural	N/A
A09	Switch - Cisco	-Errores de mantenimiento/actualización de equipos. -Acceso no autorizado.	Estructural	N/A

		-Errores de usuario y de configuración.		
		-Robo de quipo.		
A10	UPS	-Errores de mantenimiento/actualización de equipos.	Estructural	Posible
		-Condiciones inadecuadas de temperatura o humedad.		
		-Corte de suministro eléctrico.		
A11	Transceiver	-Errores de mantenimiento/actualización de equipos.	Estructural	N/A
		-Acceso no autorizado.		
		-Errores de usuario y de configuración.		
A12	NVR	-Errores de mantenimiento/actualización de equipos.	Estructural	N/A
		-Errores de usuario y de configuración.		
A13	PBX IP	-Errores de mantenimiento/actualización de equipos.	Estructural	N/A
		-Errores de usuario y de configuración.		
A14	Teléfonos IP	-Errores de los usuarios.		
		-Errores de configuración.		
		-Errores de mantenimiento/actualización de equipos.	Accidental	N/A
		-Robo de equipos.		
		-Uso no previsto.		

A15	Biométrico	-Errores de mantenimiento/actualización de equipos. -Errores de monitorización. -Errores de usuario y de configuración. Obtención de información confidencial y no autorizada.	Información confidencial	Posible
A16	Cámara IP, marca Hik – Vision	-Errores de mantenimiento/actualización de equipos. -Errores de monitorización. -Errores de usuario y de configuración. -Acceso no autorizado.	Accidental	N/A
A17	Generador eléctrico	-Corte del suministro eléctrico. -Avería de origen físico o lógico. -Errores de mantenimiento, de los usuarios, de configuración.	Ambiental	Confirmado
A18	Aire acondicionado	-Condiciones inadecuadas de temperatura o humedad. -Errores de mantenimiento/actualización de equipos. -Avería de origen físico o lógico.	Estructural	Confirmado

***Nota*:** *Adaptado de National Institute of Standards and Technology, Guide for Conducting Risk Assessments 2012, pág 76, (https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf)*

Tarea 2.3 Identificar vulnerabilidades

Se procedió a estimar las vulnerabilidades presentes que pueden ser explotadas por una o varias fuentes de amenazas en los activos de hardware que dieron como resultado de las encuestas aplicadas y de la observación en el departamento de TIC. En consecuencia, en el anexo 2.3, se estima el nivel de gravedad de las vulnerabilidades, es decir, mientras más alto es su gravedad más puede resultar en una vulnerabilidad a materializarse, en la tabla 10, se analiza las vulnerabilidades detectadas.

Tabla 10

Vulnerabilidades detectadas

Identificador	Activo	Vulnerabilidades	Encuesta al director de TIC	Encuesta al personal de TIC	Gravedad
A01	Servidor	No existe control de los accesos físicos realizados al servidor.	N° 3		Alto
A02	Computadores personales	Pérdida y alteración de la información.		N° 3	Alto
A03	Computadores de soporte	Falta de mantenimiento preventivo.		N° 19	Bajo
A04	Computador servidor	Carece de métodos de detección de intrusos (hardware).	N° 18		Alto
A05	Discos duros locales	No se evidencian bitácoras para el ingreso al departamento.		N° 5	Moderado

A06	Discos duros externos	No se evidencian bitácoras para el ingreso al departamento.	N°5	Moderado
A07	Impresora monocromática	Se imprimen documentos de otros departamentos.	N° 15	Bajo
A08	Router – Mikrotik	Falta de mantenimiento preventivo.	N°18	Bajo
A09	Switch – Cisco	Falta de mantenimiento preventivo.	N°18	Bajo
A10	UPS	Falta de mantenimiento preventivo.	N°18	Moderado
A11	Transceiver	Falta de mantenimiento preventivo.	N°18	Bajo
A12	NVR	Falta de mantenimiento preventivo.	N°18	Bajo
A13	PBX IP	Falta de mantenimiento preventivo.	N°18	Bajo
A14	Teléfonos IP	Falta de políticas de uso definidas.		Bajo
A15	Biométrico	Ausencia de un eficiente control en el mantenimiento.	N° 17	Alto
A16	Cámara IP, Hik – Vision	Las contraseñas se cambian cada 3 meses.	N° 21	Bajo
A17	Generador eléctrico	Energía eléctrica insuficiente.		Moderado

A18	Aire acondicionado	Falta de sensores de monitoreo de temperatura y humedad.	N° 14	Moderado

***Nota*:** *Adaptado de National Institute of Standards and Technology, Guide for Conducting Risk Assessments 2012, pág 78, (https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf)*

Tarea 2.4 Determinar probabilidad

Se evaluó la probabilidad de que puedan iniciarse los eventos de amenazas de forma adversarial y no adversarial en cada uno de los activos del departamento de TIC, resultados reflejados en el anexo 2.4. En la tabla 11, se indica la probabilidad de iniciación de los eventos de amenaza adversarial en los siguientes activos y se procedió a evaluar los eventos de amenazas que puedan resultar en impactos adversos.

Tabla 11

Probabilidad de iniciación del evento de amenaza (adversarial)

Identificador	**Activo**	**Vulnerabilidad** **Fuente de información**	**Probabilidad de iniciación**	**Probabilidad resultar en impacto**
A01	Servidor	No existe control de los accesos físicos realizados al servidor.	Alto	Alto
A02	Computadores personales	Pérdida y alteración de la información.	Alto	Alto
A04	Computador servidor	Carece de métodos de detección de intrusos (hardware).	Alto	Alto
A15	Biométrico	Ausencia de un eficiente control en el mantenimiento.	Alto	Alto

***Nota*:** *Adaptado de National Institute of Standards and Technology, Guide for Conducting Risk Assessments 2012, pág. 82, (https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf)*

También, en la tabla 12 se indica la probabilidad de iniciación de los eventos de amenazas no adversariales en los activos y se procedió a evaluar los eventos de amenazas que resultan en impactos adversos.

Tabla 12

Probabilidad de iniciación del evento de amenaza (no adversarial)

Identificador	Activo	Vulnerabilidad Fuente de información	Probabilidad de iniciación	Probabilidad resultar en impacto
A03	Computadores de soporte	Falta de mantenimiento preventivo.	Moderado	Moderado
A05	Discos duros locales	No se evidencian bitácoras para el ingreso al departamento.	Bajo	Bajo
A06	Discos duros externos	No se evidencian bitácoras para el ingreso al departamento.	Bajo	Bajo
A07	Impresora monocromática	Se imprimen documentos de otros departamentos.	Bajo	Bajo
A08	Router – Mikrotik	Falta de mantenimiento preventivo.	Moderado	Bajo
A09	Switch – Cisco	Falta de mantenimiento preventivo.	Moderado	Bajo
A10	UPS	Falta de mantenimiento preventivo.	Moderado	Bajo
A11	Transceiver	Falta de mantenimiento preventivo.	Moderado	Bajo

A12	NVR	Falta de mantenimiento preventivo.	Moderado	Bajo
A13	PBX IP	Falta de mantenimiento preventivo.	Moderado	Bajo
A14	Teléfonos IP	Falta de políticas de uso definidas.	Bajo	Bajo
A16	Cámara IP, Hik – Vision	Las contraseñas se cambian cada 3 meses.	Bajo	Bajo
A17	Generador eléctrico	Energía eléctrica insuficiente.	Moderado	Moderado
A18	Aire acondicionado	Falta de sensores de monitoreo de temperatura y humedad.	Moderado	Moderado

***Nota*:** *Adaptado de National Institute of Standards and Technology, Guide for Conducting Risk Assessments 2012, pág. 82, (https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf)*

Adicionalmente, en la tabla 13, se visualiza la probabilidad general que se obtuvo de los resultados de la probabilidad de iniciación del evento de amenaza (no adversarial y adversarial) más la probabilidad de evento de amenazas que resultan en impactos adversos, obtenidos de los resultados en el anexo 2.4.1.

Tabla 13

Probabilidad general

Identificador	Activo	Probabilidad general
A01	Servidor	Alto
A02	Computadores personales	Alto
A03	Computadores de soporte	Moderado
A04	Computador servidor	Alto

A05	Discos duros locales	Bajo
A06	Discos duros externos	Bajo
A07	Impresora monocromática	Bajo
A08	Router – Mikrotik	Bajo
A09	Switch – Cisco	Bajo
A10	UPS	Bajo
A11	Transceiver	Bajo
A12	NVR	Bajo
A13	PBX IP	Bajo
A14	Teléfonos IP	Bajo
A15	Biométrico	Alto
A16	Cámara IP, marca Hik – Vision	Bajo
A17	Generador eléctrico	Moderado
A18	Aire acondicionado	Moderado

***Nota*:** *Adaptado de National Institute of Standards and Technology, Guide for Conducting Risk Assessments 2012, pág. 82, (https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf)*

Tarea 2.5 Determinar el impacto

En la siguiente tabla 14, se muestra el tipo de impacto que existe por cada activo, y a su vez el cálculo del impacto máximo que se detectó en cada uno de ellos, resultados obtenidos en el anexo 2.5.

Tabla 14

Impacto de eventos de amenaza

Identificador	Activo afectado	Tipo de impacto	Impacto máximo
A01	Servidor	Daño a las personas	Alto
A02	Computadores personales	Daño a las personas	Alto
A03	Computadores de soporte	Daño a los activos	Bajo
A04	Computador servidor	Daño a las personas	Alto
A05	Discos duros locales	Daño a los activos	Moderado
A06	Discos duros externos	Daño a los activos	Moderado
A07	Impresora monocromática	Daño a operaciones	Moderado
A08	Router – Mikrotik	Daño a operaciones	Bajo
A09	Switch – Cisco	Daño a operaciones	Bajo
A10	UPS	Daño a operaciones	Bajo
A11	Transceiver	Daño a operaciones	Bajo
A12	NVR	Daño a operaciones	Bajo
A13	PBX IP	Daño a operaciones	Bajo
A14	Teléfonos IP	Daño a operaciones	Bajo
A15	Biométrico	Daño a operaciones	Alto
A16	Cámara IP, marca Hik – Vision	Daño a operaciones	Bajo
A17	Generador eléctrico	Daño a operaciones	Moderado
A18	Aire acondicionado	Daño a operaciones	Moderado

***Nota*:** *Adaptado de National Institute of Standards and Technology, Guide for Conducting Risk Assessments 2012, pág. 85, (https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf)*

Tarea 2.6 Determinar el riesgo

En la tabla 15, se obtuvo el nivel de riesgo por cada activo; que es el resultado de la probabilidad que resultan en impactos adversos más el resultado del impacto máximo, obtenidos en el anexo 2.6.

Tabla 15

Nivel de riesgo

Identificador	Activo	Nivel de riesgo
A01	Servidor	Alto
A02	Computadores personales	Alto
A03	Computadores de soporte	Bajo
A04	Computador servidor	Alto
A05	Discos duros locales	Bajo
A06	Discos duros externos	Bajo
A07	Impresora monocromática	Bajo
A08	Router – Mikrotik	Bajo
A09	Switch – Cisco	Bajo
A10	UPS	Bajo
A11	Transceiver	Bajo

A12	NVR	Bajo
A13	PBX IP	Bajo
A14	Teléfonos IP	Bajo
A15	Biométrico	Alto
A16	Cámara IP, marca Hik – Vision	Bajo
A17	Generador eléctrico	Moderado
A18	Aire acondicionado	Moderado

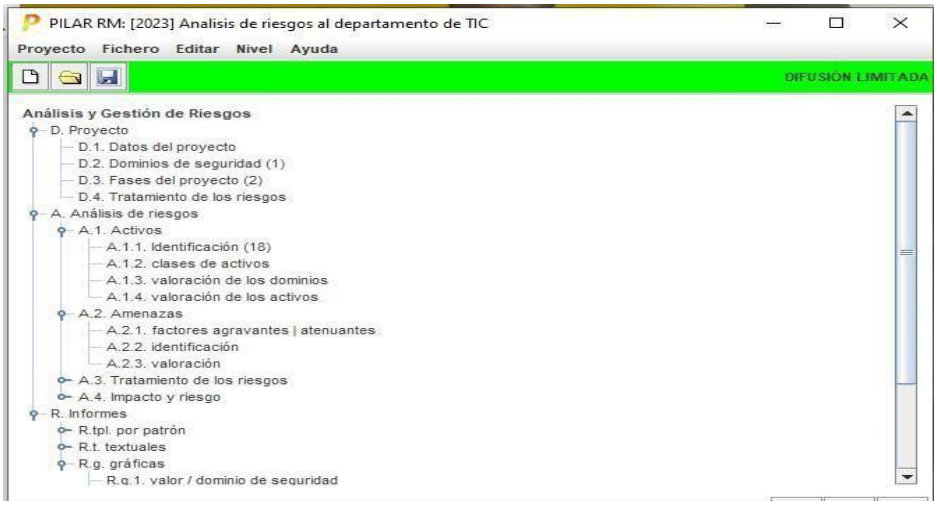
***Nota*:** *Adaptado de National Institute of Standards and Technology, Guide for Conducting Risk Assessments 2012, pág. 87, (https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf)*

3.5.2 Proceso de Gestión de la Metodología MAGERIT v.3

Para la realización del análisis y gestión de riesgos se utilizó la herramienta Pilar versión 2023.1.1, en la siguiente figura 16 se refleja las tareas con sus respectivas subtareas a seguir.

Figura 16

Análisis y gestión de riesgos



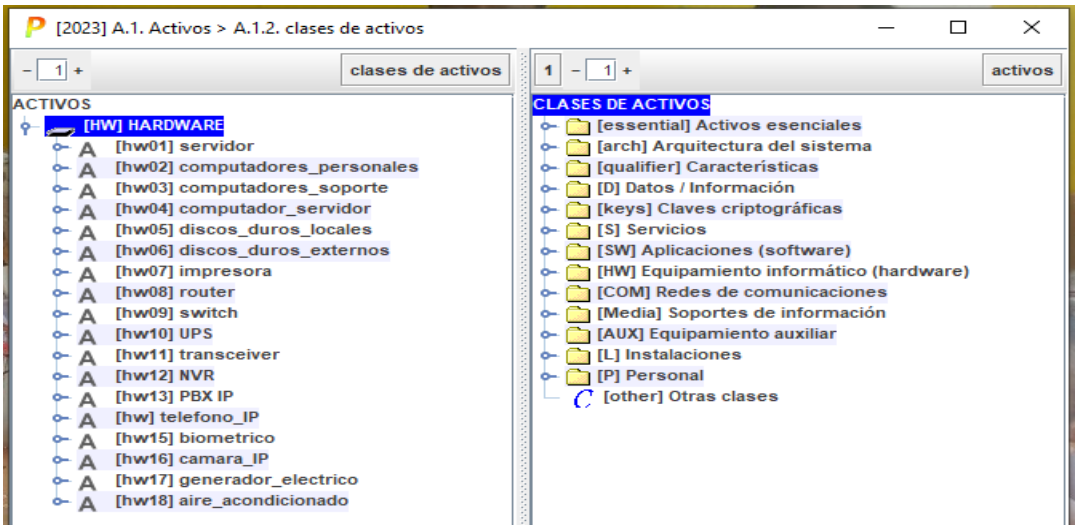
***Nota**: Adaptado de la herramienta pilar, versión 2023.1.1*

MAR.1.1 Identificación de Activos

En la identificación de activos, se creó una capa destinada a los activos de hardware donde se ingresaron los activos por un código, nombre y fuente de información y se seleccionó a la clase de activo que corresponde, como se plasma en la siguiente figura 17.

Figura 17

Clases de activos



***Nota**: Adaptado de la herramienta pilar, versión 2023.1.1*

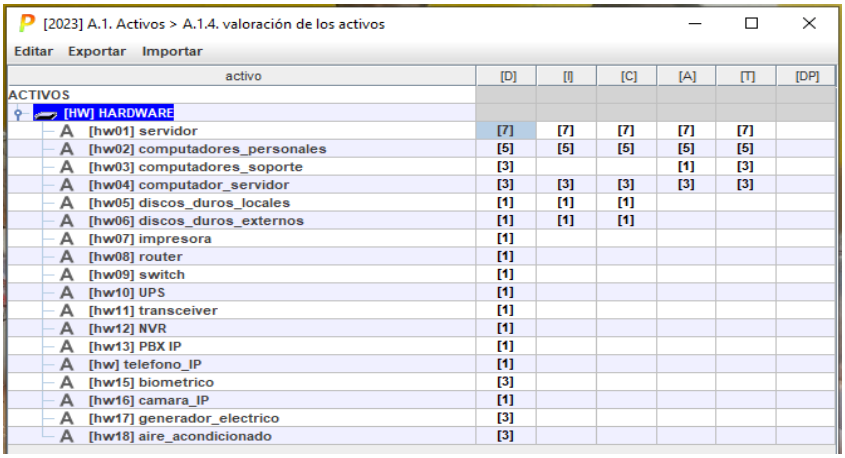
MAR.1.3 Valoración de los Activos

Una vez realizada la caracterización de los activos del departamento de TIC, se procedió a realizar la valoración de cada uno de ellos en cuanto a: disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.

En la siguiente figura 18, en la opción valoración de los activos se ingresó los valores obtenidos del anexo MAR.1.3, en los casos que no se especifica ninguna valoración, Pilar lo determinó como un activo que no tiene requisitos significativos en esa dimensión.

Figura 18

Valoración de activos



***Nota**: Adaptado de la herramienta pilar, versión 2023.1.1*

MAR.2 Caracterización de las amenazas

Esta actividad busca identificar las amenazas relevantes sobre el sistema a analizar, caracterizándolas por las estimaciones de ocurrencia (probabilidad) y daño causado (degradación).

Antes de la identificación de amenazas se determinó los factores agravantes, que son una serie de calificativos que se asigna en los dominios; calificativos que fueron utilizados para establecer el perfil de vulnerabilidad; es decir, para ajustar el perfil de amenazas posibles, como se indica en la siguiente figura 19.

Figura 19

Factores agravantes

***Nota**: Adaptado de la herramienta pilar, versión 2023.1.1*

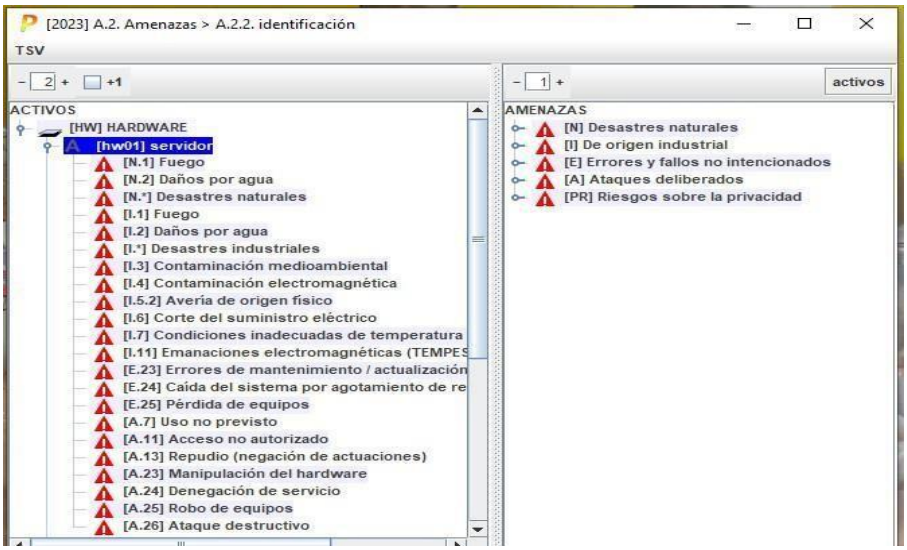
MAR.2.1 Identificación de las Amenazas

El siguiente paso, consistió en identificar las causas potenciales que pueden causar daños a los activos de hardware del departamento. Las amenazas típicas que se pueden encontrar son: desastres naturales, de origen industrial, errores y fallos no intencionados, ataques deliberados y riesgos sobre la privacidad, la cual están detallados en los anexos MAR. 2.0 y MAR.2.1.

Al identificar los activos a la clase de activos Hardware, Pilar asigna automáticamente a todos los activos las mismas posibles amenazas que pueden materializarse, como se presenta en la figura 20 y en la figura 21.

Figura 20

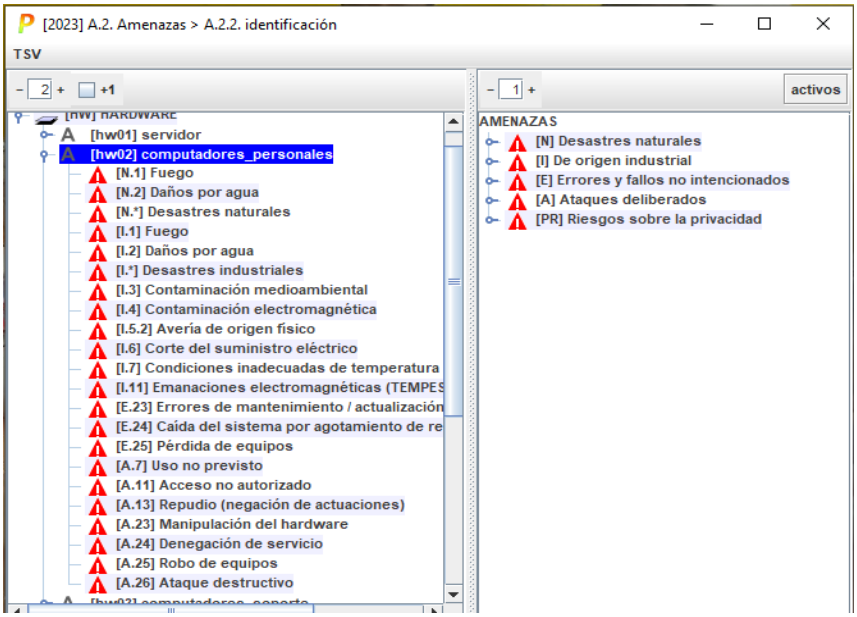
Identificación de amenazas en el servidor



***Nota**: Adaptado de la herramienta pilar, versión 2023.1.1*

Figura 21

Identificación de amenazas a los computadores personales



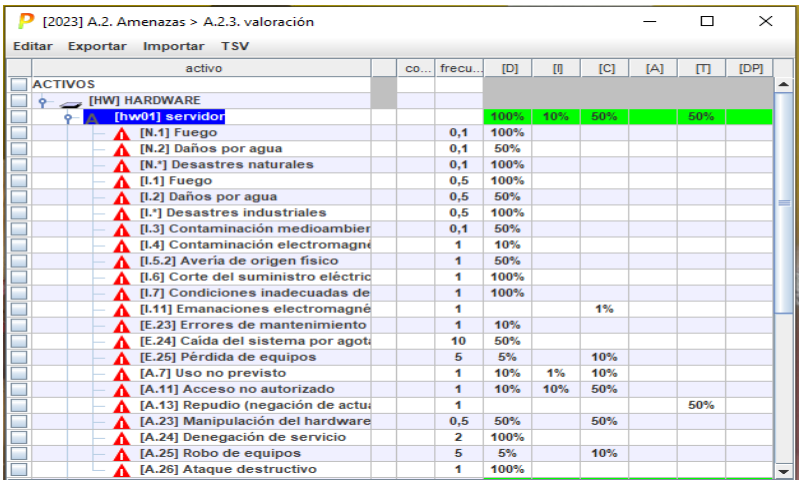
***Nota**: Adaptado de la herramienta pilar, versión 2023.1.1.*

MAR.2.2 Valoración de las Amenazas

Una vez identificadas las amenazas, se evaluó el daño que puede tener sobre cada activo. Pilar, calculó automáticamente la frecuencia de ocurrencia de cada amenaza por activo en las dimensiones de: disponibilidad, integridad, confidencialidad, y trazabilidad, como se puede ver en la siguiente figura 22.

Figura 22

Valoración de amenazas en el servidor

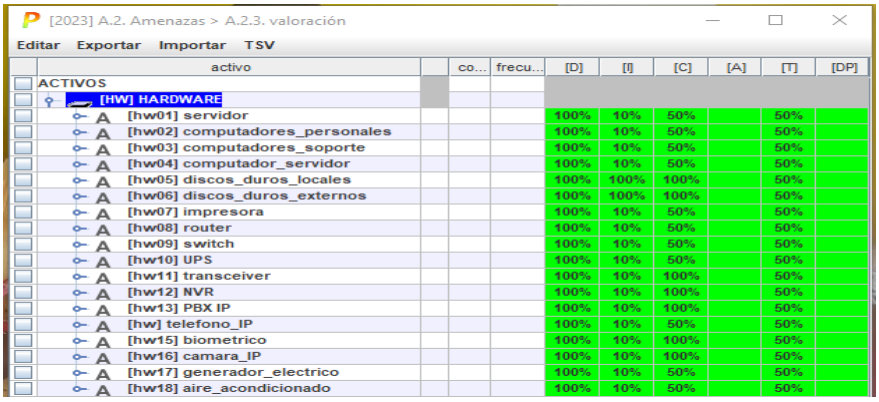


***Nota**: Adaptado de la herramienta pilar, versión 2023.1.1*

Posteriormente, en la siguiente figura 23 se evidencia la valoración de amenazas en cuanto a disponibilidad, integridad, confidencialidad y trazabilidad de todos los activos y de forma más detallada sobre cada activo se puede evidenciar en el anexo MAR. 2.2.

Figura 23

Valoración de amenazas en todos los activos



activo	co...	frecu...	[D]	[I]	[C]	[A]	[T]	[DP]
ACTIVOS								
[HW] HARDWARE								
[hw01] servidor			100%	10%	50%		50%	
[hw02] computadores_personales			100%	10%	50%		50%	
[hw03] computadores_soporte			100%	10%	50%		50%	
[hw04] computador_servidor			100%	10%	50%		50%	
[hw05] discos_duros_locales			100%	100%	100%		50%	
[hw06] discos_duros_externos			100%	100%	100%		50%	
[hw07] impresora			100%	10%	50%		50%	
[hw08] router			100%	10%	50%		50%	
[hw09] switch			100%	10%	50%		50%	
[hw10] UPS			100%	10%	50%		50%	
[hw11] transceiver			100%	10%	100%		50%	
[hw12] NVR			100%	10%	100%		50%	
[hw13] PBX IP			100%	10%	100%		50%	
[hw] telefono_IP			100%	10%	50%		50%	
[hw15] biometrico			100%	10%	100%		50%	
[hw16] camara_IP			100%	10%	100%		50%	
[hw17] generador_electrico			100%	10%	50%		50%	
[hw18] aire_acondicionado			100%	10%	50%		50%	

***Nota**: Adaptado de la herramienta pilar, versión 2023.1.1*

3.6 Nivel de Impacto del Proceso de Gestión de Riesgos del MAGERIT en Pilar

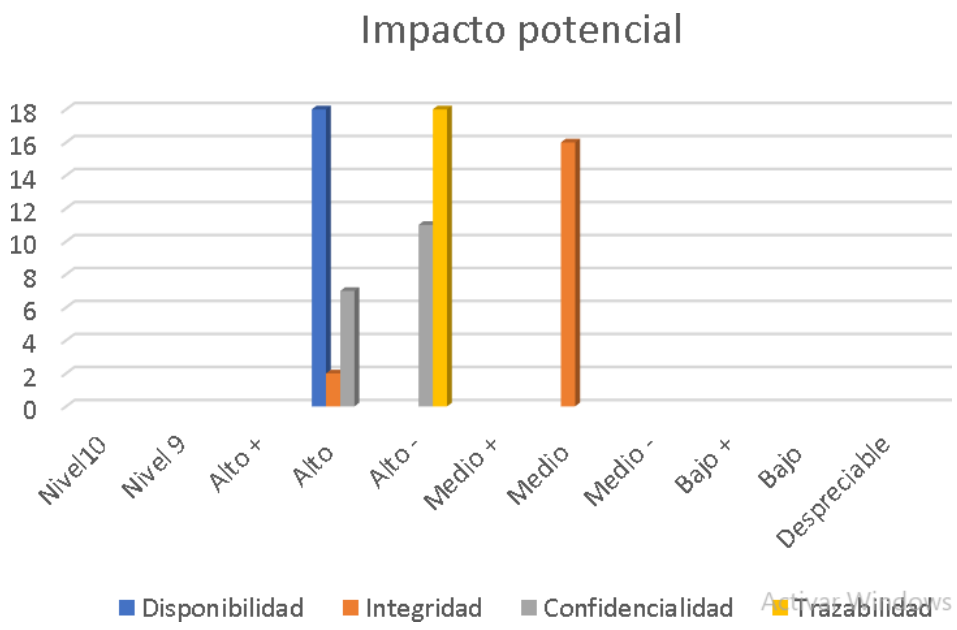
En esta actividad se procesaron todos los datos recopilados de las actividades anteriores, en esta actividad se realizó la estimación de impacto y riesgo potencial tanto acumulado como repercutido.

MAR.2.3 Impacto Potencial

Al obtener los resultados de la valoración de los activos, su frecuencia y degradación que causan las amenazas, se puede calcular el impacto potencial que tuvieron en cada uno de los activos del departamento de TIC. Pilar, calculó el impacto acumulado, donde el mayor componente afectado es la disponibilidad, confidencialidad en la cual todos los activos tiene un alto nivel de impacto, la cual se detalla en la siguiente figura 24.

Figura 24

Impacto potencial



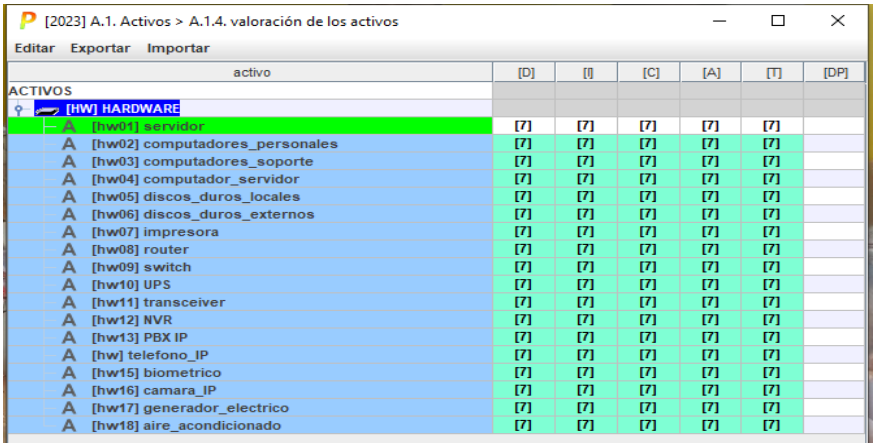
***Nota**: Elaboración propia*

Impacto potencial acumulado

El impacto acumulado se calculó en función de cada dimensión: disponibilidad, integridad, confidencialidad, y trazabilidad; una vez obtenido la valoración acumulada del activo que se plasma en la siguiente figura 25, donde el valor acumulado de cada activo se obtuvo de forma automática en la herramienta Pilar más las amenazas a las que se encuentran expuestos.

Figura 25

Valor acumulado de activos

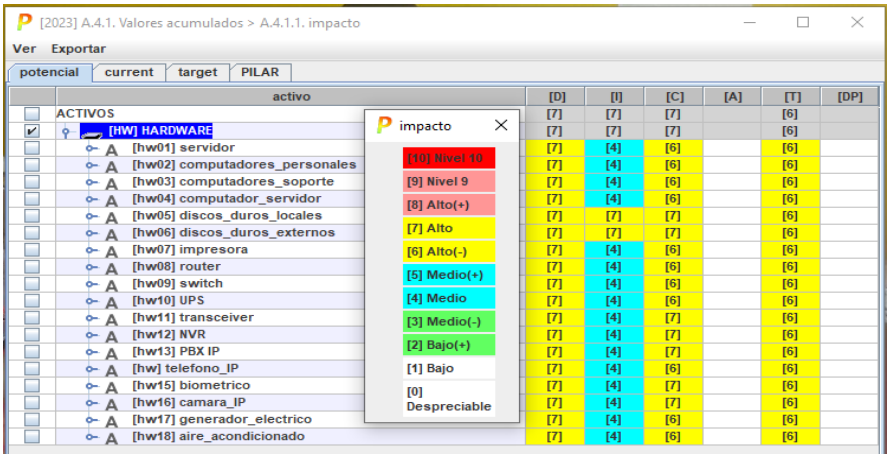


***Nota**: Adaptado de la herramienta pilar, versión 2023.1.1*

Al obtener su valor acumulado se evidenció el nivel de impacto de acuerdo a los resultados, donde la disponibilidad, confidencialidad y trazabilidad tuvo un nivel alto con una valoración de 7 a 6 en todos los activos; y la integridad un nivel medio con una valoración de 4, como se describe en la siguiente figura 26.

Figura 26

Valores acumulados del nivel de impacto



***Nota**: Adaptado de la herramienta pilar, versión 2023.1.1*

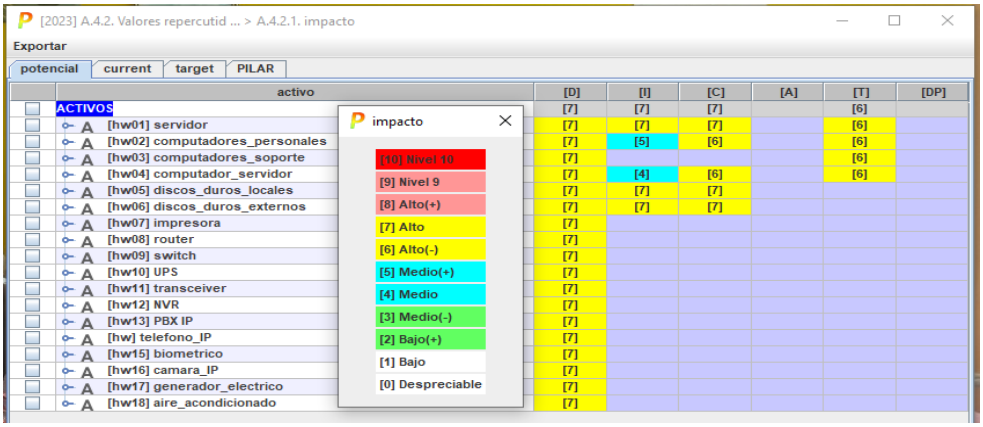
Impacto potencial repercutido

El impacto repercutido se calculó en función de cada dimensión: disponibilidad, integridad, confidencialidad, y trazabilidad; una vez identificado su valor propio de cada

activo más las amenazas a los que se encuentran propensos. En la siguiente figura 27, se evidenció el nivel de impacto, conforme a la leyenda se obtuvo un nivel alto con una valoración de 7 a 6 en todos los activos en disponibilidad, tres activos en integridad, cinco activos en confidencialidad, cuatro activos en trazabilidad; y un nivel medio con una valoración de 5 a 4 en dos activos en la dimensión de integridad.

Figura 27

Valores repercutidos del nivel de impacto



Nota: Adaptado de la herramienta pilar, versión 2023.1.1

MAR.2.4 Riesgo Potencial

La finalidad de esta actividad tiene como propósito determinar el riesgo potencial al que están sometidos los activos, en la figura 28 se observa los resultados obtenidos; donde todos los activos alcanzan niveles críticos, muy alto y alto en disponibilidad, integridad, confidencialidad y trazabilidad, posteriormente se detalla el nivel de riesgo acumulado y repercutido en función de la disponibilidad, integridad, confidencialidad y trazabilidad, valores obtenidos en la herramienta Pilar.

Figura 28

Riesgo potencial

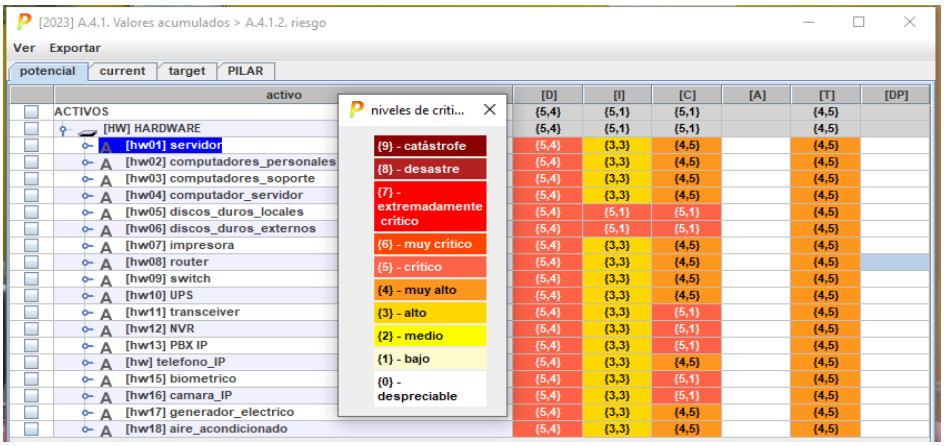
***Nota**: Elaboración propia*

Riesgo potencial acumulado

En esta actividad se obtuvo el resultado del riesgo acumulado al calcular el nivel de impacto acumulado de cada activo más la frecuencia de cada amenaza. En la siguiente figura 29, se observa los resultados teniendo como consecuencia un nivel crítico en todos los activos en función de la disponibilidad; muy alto en confidencialidad en once activos, en trazabilidad a todos los activos, y alto en función de la integridad en dieciséis activos.

Figura 29

Valores acumulados del riesgo



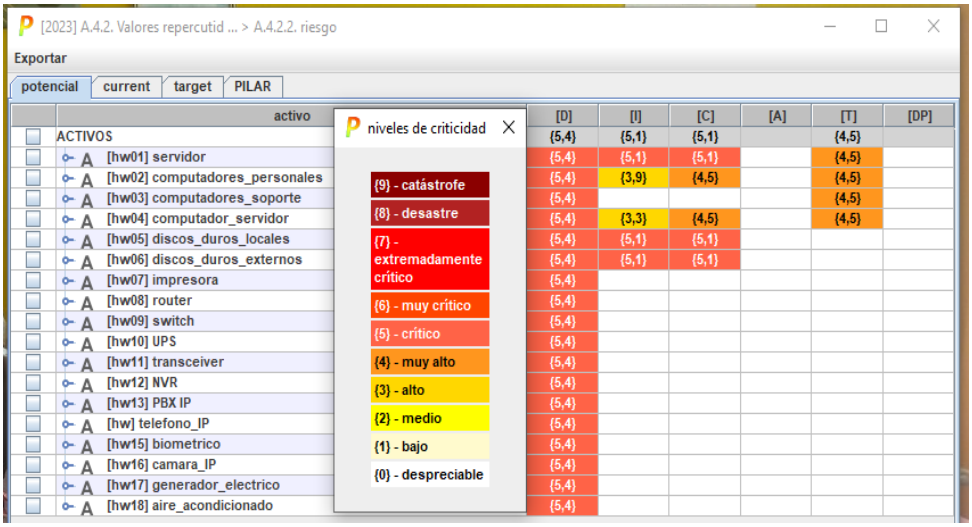
Nota: Adaptado de la herramienta pilar, versión 2023.1.1

Riesgo potencial repercutido

Se calculó el riesgo repercutido a partir del valor de impacto repercutido y la frecuencia de amenazas sobre cada uno de los activos, y se obtuvo como resultados de acuerdo la leyenda que todos los activos tienen un nivel crítico en función de la disponibilidad, en integridad y confidencialidad en tres activos; muy alto en la dimensión de trazabilidad en cuatro activos; y alto con dos activos en integridad, como se detalla en la siguiente figura 30.

Figura 30

Valores repercutidos del riesgo



***Nota**: Adaptado de la herramienta pilar, versión 2023.1.1*

3.7 Medidas de Protección de la Normativa ISO/IEC 27001:2022 y NIST Cybersecurity Framework

3.7.1 Proceso de Gestión de la Metodología NIST SP 800-30

Paso 3. Comunicación e Intercambio de Información de Evaluación de Riesgos

Comunicar los resultados y compartir la información consta de las siguientes tareas: comunicar los resultados de la evaluación de riesgos; y compartir información desarrollada en la ejecución de la evaluación de riesgos, para apoyar otros riesgos de actividades de gestión.

Tarea 3.1 Comunicar los resultados. La finalidad de esta actividad es comunicar los resultados de la evaluación de riesgos al Director de TIC, quien es el encargado de tomar decisiones conforme a los resultados obtenidos.

Tarea 3.2 Compartir información relacionada con riesgos. Una vez finalizada la evaluación del riesgo con el personal del departamento de TIC, se sugirió los controles de seguridad de la información enumerados en la ISO/IEC 27001:2022 acorde a los riesgos, con el objeto de mitigar los mismos.

Donde, la ISO/IEC 27001:2022, tiene 93 controles distribuidos de la siguiente manera: 37 controles organizacionales, 8 controles de personas, 14 controles físicos y 34 controles tecnológicos. En la tabla 16, se proponen las medidas sugeridas en base a la normativa.

Tabla 16

Medidas a implementar sobre los resultados

Id	Activo	Nivel de	Vulnerabilidad	Medidas sugeridas
A01	Servidor	Alto	No existe control de los accesos físicos realizados al servidor.	Control físico: 7.2 Entrada física. Control organizacional: 5.15 Control de acceso. Control físico: 7.4 Monitoreo de seguridad física.
A02	Computadores personales	Alto	Pérdida y alteración de la información.	Controles organizacionales: 5.34 Privacidad y protección de la información de identificación personal. Controles tecnológicos: 8.12 Prevención de fuga de datos.

					Controles tecnológicos: 8.16 Actividades de seguimiento.
A03	Computadores de soporte	Bajo	Falta de mantenimiento preventivo.		Control físico: 7.5 Protección contra daños físicos y amenazas ambientales. 7.13 Mantenimiento de equipo.
A04	Computador servidor	Alto	Carece de métodos de detección de intrusos (hardware).		Control organizacional: 5.21 Gestión del control de seguridad de la información. Controles de personas: 6.8 Informes de eventos de seguridad de la información. Controles de personas: 6.3 Conciencia de seguridad de la información..
A05	Discos duros locales	Bajo	No se evidencian bitácoras para el ingreso al departamento.		Control físico: 7.3 Seguridad de oficinas, habitaciones o instalaciones
A06	Discos duros externos	Bajo	No se evidencian bitácoras para el ingreso al departamento.		Control físico: 7.3 Seguridad de oficinas, habitaciones o instalaciones.
A07	Impresora monocromát	Bajo	Se imprimen documentos de otros departamentos.		Controles organizacionales: 5.10 Uso aceptable de la información y otros activos asociados.
A08	Router – Mikrotik	Bajo	Falta de mantenimiento preventivo.		Control físico: 7.5 Protección contra daños físicos y amenazas ambientales. 7.13 Mantenimiento de equipo.

A09	Switch – Cisco	Bajo	Falta de mantenimiento preventivo.	Control físico: 7.5 Protección contra daños físicos y amenazas ambientales. 7.13 Mantenimiento de equipo.
A10	UPS	Bajo	Falta de mantenimiento preventivo.	Control físico: 7.5 Protección contra daños físicos y amenazas ambientales. 7.13 Mantenimiento de equipo.
A11	Transceiver	Bajo	Falta de mantenimiento preventivo.	Control físico: 7.5 Protección contra daños físicos y amenazas ambientales. 7.13 Mantenimiento de equipo
A12	NVR	Bajo	Falta de mantenimiento preventivo.	Control físico: 7.5 Protección contra daños físicos y amenazas ambientales. 7.13 Mantenimiento de equipo
A13	PBX IP	Bajo	Falta de mantenimiento preventivo.	Control físico: 7.5 Protección contra daños físicos y amenazas ambientales. 7.13 Mantenimiento de equipo
A14	Teléfonos IP	Bajo	Falta de políticas de uso definidas.	Controles organizacionales: 5.10 Uso aceptable de la información y otros activos asociados.
A15	Biométrico	Alto	Ausencia de un eficiente control en el mantenimiento.	Control físico: 7.5 Protección contra daños físicos y amenazas ambientales. 7.13 Mantenimiento de equipo

A16	Cámara IP, marca Hik – Vision	Bajo	Las contraseñas se cambian cada 3 meses.	Controles físicos: 7.13 Mantenimiento de equipo Controles tecnológicos: 8.9 Control de gestión de configuración.
A17	Generador eléctrico	Moderado	Energía eléctrica insuficiente.	Control físico: 7.5 Protección contra daños físicos y amenazas ambientales. 7.12 Seguridad del cableado. 7.13 Mantenimiento de equipo.
A18	Aire acondicionado	Moderado	Falta de sensores de monitoreo de temperatura y humedad.	Control físico: 7.5 Protección contra daños físicos y amenazas ambientales. 7.13 Mantenimiento de equipo. Controles tecnológicos: 8.27 Arquitectura de sistemas seguros y principios de ingeniería.

Adaptado de National Institute of Standards and Technology, Guide for Conducting Risk Assessments 2012, (https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf), elaboración propia.

Paso 4. Mantener la Evaluación de Riesgos

El último paso, es mantener la evaluación, el objetivo de este paso es verificar el cumplimiento y determinar la eficacia de las respuestas a los riesgos; para el cumplimiento de estas medidas sugeridas, es necesario proponer diversas actividades que mitiguen la amenaza, cabe destacar que una amenaza puede ser controlada por varios tipos de salvaguardas, a continuación, se detalla por cada activo.

Servidor

- Control físico 7.2 Entrada física: Limitar y restringir el acceso mediante sistemas de identificación y métodos de verificación como tarjetas personales, y sistemas biométricos.

- Control organizacional 5.15 Control de acceso: Implementar políticas de seguridad para el acceso físico.
- Control físico 7.4 Monitoreo de seguridad física: Monitorear los accesos autorizados a través de vigilancia IP.

Computadores personales

- Controles organizacionales 5.34 Privacidad y protección de la información de identificación personal: Implementar y seguimiento de acuerdos de confidencialidad, y aseguramiento de respaldos de la información a diario.
- Controles tecnológicos 8.12 Prevención de fuga de datos: Implementar hardware DLP (prevención de pérdida de datos) para supervisar la red y evitar que usuarios no autorizados copien o compartan información privada.
- Controles tecnológicos: 8.16 Actividades de seguimiento: Desarrollar un plan de seguimiento y monitoreo de equipos de hardware.

Computadores de soporte

- Controles físicos: 7.13 Mantenimiento de equipo: Elaborar y ejecutar un plan actividades de mantenimiento preventivo y correctivo, además llevar un registro de incidentes.
- Control físico: 7.5 Protección contra daños físicos y amenazas ambientales: Establecimiento de un protocolo de ubicación correcta para los equipos de hardware y la instalación de detectores de humo, alarmas contra incendios, extintores.

Computador servidor

- Control organizacional: 5.21 Gestión del control de seguridad de la información: Implementar sistemas de prevención de intrusos (IPS).
- Controles de personas: 6.8 Informes de eventos de seguridad de la información: Elaborar un plan de detección y respuesta a incidentes.
- Controles de personas: 6.3 Conciencia de seguridad de la información. - Compromiso y concienciación en medidas de seguridad por parte de los empleados.

Discos duros externos, discos duros locales

- Control físico 7.3 Seguridad de oficinas, habitaciones o instalaciones: Implementar de registro de actividades mediante bitácoras que registre la fecha y el motivo de las personas que ingresan.

Impresora monocromática

- Controles organizacionales: 5.10 Uso aceptable de la información y otros activos asociados. Implementar políticas de seguridad de los dispositivos que pueden conectarse.

PBX IP, NVR, Transceiver, UPS, Switch, y Router

- Control físico: 7.5 Protección contra daños físicos y amenazas ambientales: Establecimiento de un protocolo de ubicación correcta para los equipos de hardware y la instalación de detectores de humo, alarmas contra incendios, extintores.
- Controles físicos: 7.13 Mantenimiento de equipo: Elaborar y ejecutar un plan actividades de mantenimiento preventivo y correctivo, además llevar un registro de incidentes.

Teléfonos IP

- Controles organizacionales: 5.10 Uso aceptable de la información y otros activos asociados: Diseñar políticas del uso y acceso del hardware.

Biométrico

- Control físico: 7.5 Protección contra daños físicos y amenazas ambientales: Diseñar un sistema de gestión de seguridad y establecer un plan de monitoreo y seguimiento del equipo.
- Controles físicos: 7.13 Mantenimiento de equipo: Elaborar y ejecutar un plan actividades de mantenimiento preventivo y correctivo, además llevar un registro de incidentes.

Cámara IP, marca Hik – Vision

- Controles físicos: 7.13 Mantenimiento de equipo: Elaborar y ejecutar un plan actividades de mantenimiento preventivo y correctivo, además llevar un registro de incidentes.
- Controles tecnológicos: 8.9 Control de gestión de configuración. Cambiar las contraseñas cada 90 días como mínimo e implementación del cifrado hash para el almacenamiento de contraseñas.

Generador eléctrico

- Control físico: 7.5 Protección contra daños físicos y amenazas ambientales: Establecimiento de un protocolo de ubicación correcta para los equipos de hardware y la instalación de detectores de humo, alarmas contra incendios, extintores.
- Controles físicos: 7.12 Seguridad del cableado. Revisar las conexiones eléctricas, cables, contactos.
- Controles físicos: 7.13 Mantenimiento de equipo: Realizar un mantenimiento preventivo o correctivo, establecer un plan de renovación de equipos de hardware por vida útil.

Aire acondicionado

- Control físico: 7.5 Protección contra daños físicos y amenazas ambientales: establecer un plan de emergencia antes desastres industriales.
- Controles físicos: 7.13 Mantenimiento de equipo: Elaborar y ejecutar un plan actividades de mantenimiento preventivo y correctivo, además llevar un registro de incidentes.
- Controles tecnológicos: 8.27 Arquitectura de sistemas seguros y principios de ingeniería: Implementar sensores de monitoreo de temperatura y humedad.

3.7.2 Proceso de Gestión de la Metodología MAGERIT v.3

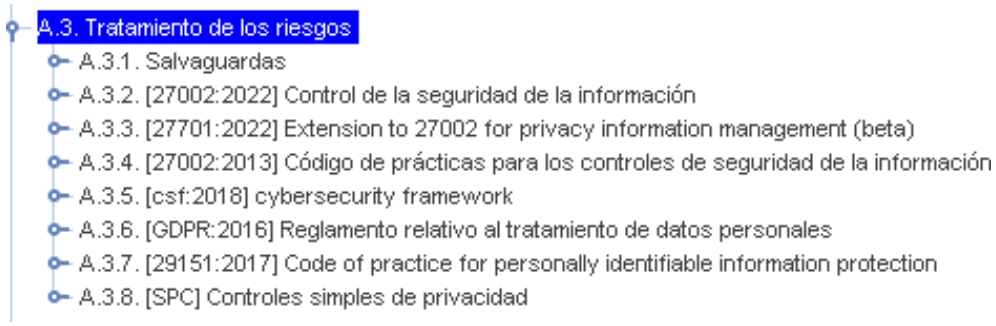
MAR.3 Caracterización de las Salvaguardas

Esta actividad busca identificar las salvaguardas que se pueden desplegar en los activos a analizar, clasificándolas por su eficacia frente a las amenazas que tienen como finalidad la mitigación. En la siguiente figura 31, en la opción “Tratamiento de los riesgos”

se despliegan varias opciones, donde se seleccionó la alternativa A.3.1, la cual mostró las salvaguardas que dispone la herramienta Pilar.

Figura 31

Tratamiento a los riesgos



Nota: Adaptado de la herramienta pilar, versión 2023.1.1

MAR.3.1 Identificación de las Salvaguardas Pertinentes

Esta actividad consistió en identificar las salvaguardas convenientes para determinar qué necesitamos proteger y saber si tenemos un sistema de protección a la altura de nuestras necesidades.

Una vez identificados y valoradas la amenazas en la herramienta Pilar, en el tratamiento de los riesgos la opción A.3.1 Salvaguardas como se indica en la figura 32 se identificaron todas las salvaguardas existentes en la biblioteca estándar de Pilar, la cual posteriormente se evaluó el nivel de madurez de cada salvaguarda; teniendo como base el nivel de madurez de las salvaguardas desde L0 a L5, que se evidencia en la siguiente tabla 17.

Tabla 17

Nivel de madurez de salvaguardas

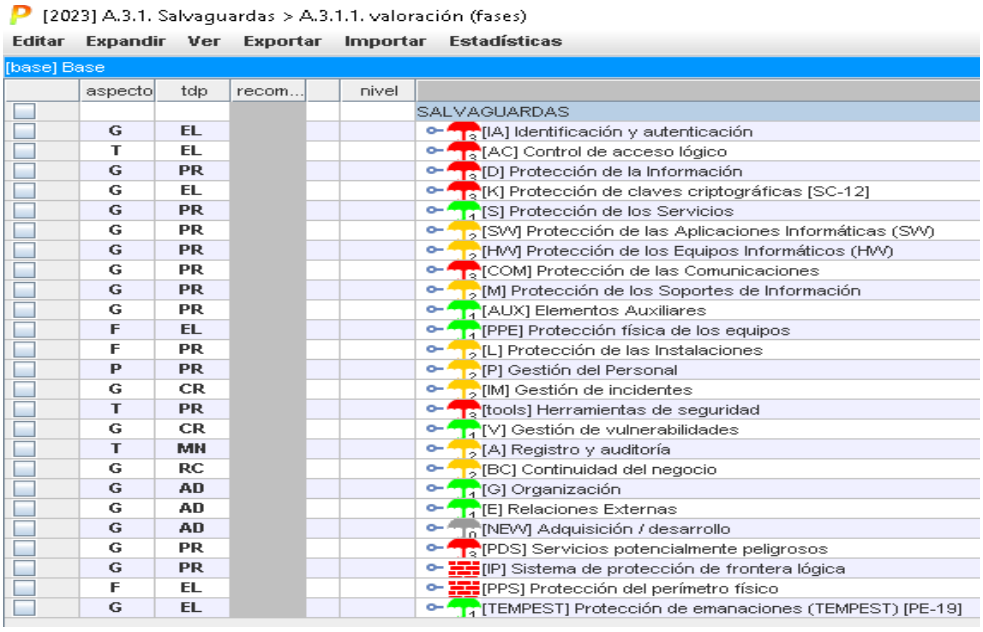
Factor	Nivel	Madurez	Estado
0%	L0	Inexistente	Inexistente

	L1	Inicial	Iniciado
	L2	Reproducible, pero intuitivo	Parcialmente realizado
	L3	Proceso definido	En funcionamiento
	L4	Gestionado y medible	Monitorizado
100%	L5	Optimizado	Mejora continua

Nota: Eficacia de la protección de las salvaguardas, adaptado de Metodología de análisis y gestión de riesgos de los sistemas de información, Libro I, 2012, por Quispe, V, E, de Ministerio de hacienda y administraciones públicas, (p.34).

Figura 32

Salvaguardas



***Nota**: Adaptado de la herramienta pilar, versión 2023.1.1*

MAR.3.2 Valoración de las Salvaguardas

En esta actividad se determinó las salvaguardas pertinentes que dependen de la valoración de las amenazas, Pilar recomendó las siguientes salvaguardas: identificación y autenticación, protección de los equipos informáticos (HW), protección a los elementos

auxiliares, protección de las instalaciones, gestionar los incidentes, emplear herramientas de seguridad, donde su nivel de madurez de las salvaguardas es de L2 que significa que está parcialmente realizado y L3 que indica en funcionamiento, como se ilustra en la figura 33.

Figura 33

Valoración de salvaguardas

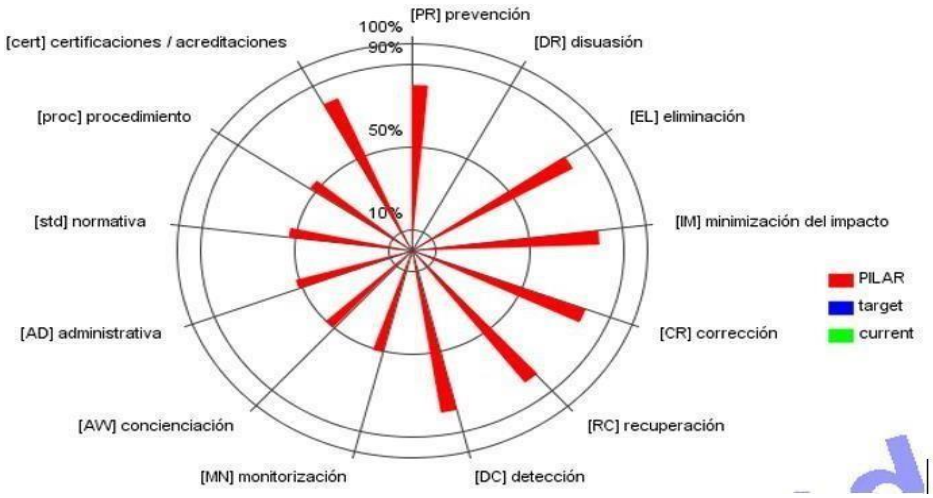
asp...	tdp	rec...	nivel	salvaguarda	du...	fue...	base	co...	cur...	tar...	PIL...
				SALVAGUARDAS							L2-...
G	EL			[IA] Identificación y autenticación							n.a.
T	EL			[AC] Control de acceso lógico	¿...?						n.a.
G	PR			[D] Protección de la Información							n.a.
G	EL			[K] Protección de claves criptográficas [SC-12]							n.a.
G	PR			[S] Protección de los Servicios							n.a.
G	PR			[SW] Protección de las Aplicaciones Informáticas (SW)							n.a.
G	PR	4		[HW] Protección de los Equipos Informáticos (HW)							L2-...
G	PR			[COM] Protección de las Comunicaciones							n.a.
G	PR			[M] Protección de los Soportes de Información							n.a.
G	PR	5		[AUX] Elementos Auxiliares							L2-...
F	EL	5		[PPE] Protección física de los equipos							L3
F	PR			[L] Protección de las Instalaciones							n.a.
P	PR			[P] Gestión del Personal							n.a.
G	CR	4		[IM] Gestión de incidentes							L2-...
T	PR	4		[tools] Herramientas de seguridad							L2-...
G	CR			[V] Gestión de vulnerabilidades							n.a.
T	MN	4		[A] Registro y auditoría							L2-...
G	RC	3		[BC] Continuidad del negocio							L2-...
G	AD	4		[G] Organización							L2-...
G	AD	3		[E] Relaciones Externas							L2-...
G	AD	4		[NEW] Adquisición / desarrollo							L2-...
G	PR			[PDS] Servicios potencialmente peligrosos							n.a.
G	PR			[IP] Sistema de protección de frontera lógica							n.a.
F	EL			[PPS] Protección del perímetro físico							n.a.
G	EL	3		[TEMPEST] Protección de emanaciones (TEMPEST) [PE-19]							L2

Nota: Adaptado de la herramienta pilar, versión 2023.1.1

A su vez, Pilar, también sugirió los tipos de protección que se pueden aplicar, de acuerdo a la probabilidad medidas de: prevención, disuasión, eliminación; por el nivel de impacto medidas de: minimización del impacto, corrección, recuperación; por su administración medidas de: detección, monitorización, concienciación, administrativa, normativa, procedimientos y acreditación de certificaciones. En la figura 34 se manifiesta el nivel de porcentaje que tienen cada una de ellas al aplicarlas.

Figura 34

Grado de eficacia de los tipos de protección



***Nota**: Adaptado de la herramienta pilar, versión 2023.1.1*

En la siguiente figura 35, los controles de la norma ISO/IEC 27002: 2022, la cual sugirió la herramienta Pilar son los siguientes: 21 controles organizacionales, 1 control a personas, 6 controles físicos y 7 controles de soporte de almacenamiento con un grado de madurez de L2 a L3, donde L2 que significa que está parcialmente realizado y L3 que indica en funcionamiento para más detalles véase los anexos MAR 3.2.

Figura 35

Controles de seguridad de la información ISO/IEC 27002: 2022

control	PILAR
[27002:2022] Control de la seguridad de la información	L2 (L2-L3)
[5] Organización /PR CR DC	L2 (L2-L3)
[5.1] Políticas para la seguridad de la información /PR	L2
[5.2] Roles y responsabilidades en seguridad de la información /PR	L2
[5.3] Segregación de tareas /PR	n.a.
[5.4] Responsabilidades de la dirección /PR	L2 (n.a.)
[5.5] Contacto con las autoridades /PR CR	L2
[5.6] Contacto con grupos de interés especial /PR CR	L2
[5.7] Inteligencia de amenazas /PR CR DC	L2 (L3)
[5.8] Seguridad de la información en la gestión de proyectos /PR	L2
[5.9] Inventario de información y otros activos asociados /PR	L2
[5.10] Uso aceptable de la información y activos asociados /PR	L2
[5.11] Devolución de activos /PR	L2 (n.a.)

***Nota**: Adaptado de la herramienta pilar, versión 2023.1.1*

De igual manera en la figura 36, se visualizan las salvaguardas de NIST cybersecurity framework, con un nivel de eficacia de grado 4, que se detalla a continuación:

En la función de Identificar se seleccionó 26 controles distribuidos de la siguiente manera: 3 controles en gestión de activos, 5 controles en entorno empresarial, 3 controles en gobernanza, 6 controles en evaluación de riesgos, 3 controles en estrategia de gestión de riesgos, y 6 controles en riesgo estratégico administrativo.

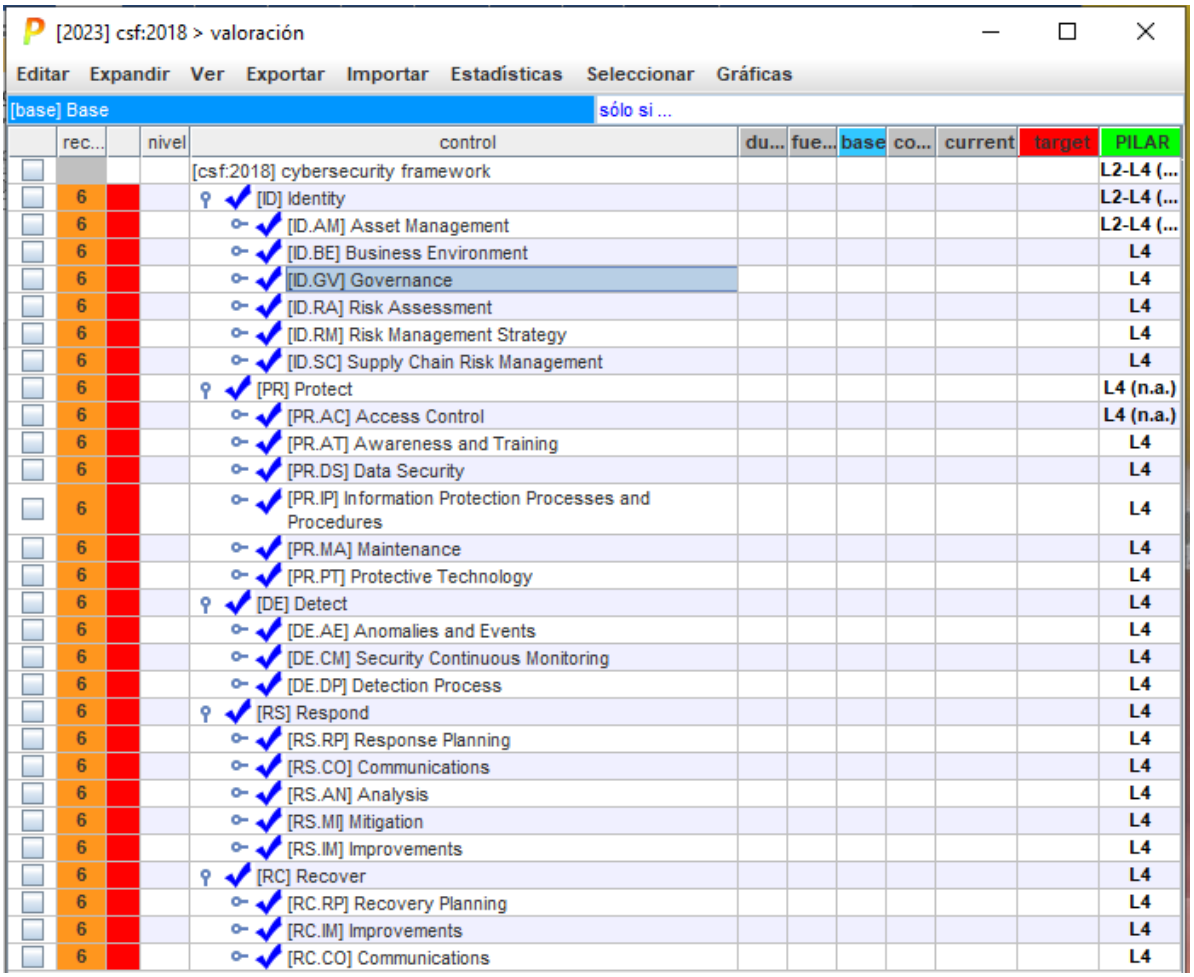
Mientras que la función de Proteger tiene 30 controles que son los siguientes: 3 controles en la subcategoría de control de acceso, 6 controles en concienciación y formación, 8 controles en seguridad en datos, 6 controles en procesos y procedimientos de la protección de la información, 2 controles en mantenimiento, y 5 controles en tecnología de protección.

Asimismo, en la función de Detectar existen 18 controles, que se detalla a continuación: 5 controles en anomalías y eventos, 8 controles en monitoreo continuo de seguridad, 5 controles en proceso de detección.

Respecto a la función de Responder se toman 16 controles en la que hay 1 control en planificación de la respuesta, 5 controles en comunicaciones, 5 controles en análisis, 3 controles en mitigación, 2 controles en mejoras.

Finalmente, en la función de Recuperar se eligieron 6 controles que son los siguientes: 1 control en planificación de recuperación, 2 controles en mejoras, 3 controles en comunicación, para más detalles véase los anexos MAR 3.2.

Figura 36. *Controles de NIST Cybersecurity Framework*



rec...		nivel	control	du...	fue...	base	co...	current	target	PILAR
			[csf:2018] cybersecurity framework							L2-L4 (...
6			[ID] Identity							L2-L4 (...
6			[ID.AM] Asset Management							L2-L4 (...
6			[ID.BE] Business Environment							L4
6			[ID.GV] Governance							L4
6			[ID.RA] Risk Assessment							L4
6			[ID.RM] Risk Management Strategy							L4
6			[ID.SC] Supply Chain Risk Management							L4
6			[PR] Protect							L4 (n.a.)
6			[PR.AC] Access Control							L4 (n.a.)
6			[PR.AT] Awareness and Training							L4
6			[PR.DS] Data Security							L4
6			[PR.IP] Information Protection Processes and Procedures							L4
6			[PR.MA] Maintenance							L4
6			[PR.PT] Protective Technology							L4
6			[DE] Detect							L4
6			[DE.AE] Anomalies and Events							L4
6			[DE.CM] Security Continuous Monitoring							L4
6			[DE.DP] Detection Process							L4
6			[RS] Respond							L4
6			[RS.RP] Response Planning							L4
6			[RS.CO] Communications							L4
6			[RS.AN] Analysis							L4
6			[RS.MI] Mitigation							L4
6			[RS.IM] Improvements							L4
6			[RC] Recover							L4
6			[RC.RP] Recovery Planning							L4
6			[RC.IM] Improvements							L4
6			[RC.CO] Communications							L4

Nota: Adaptado de la herramienta pilar, versión 2023.1.

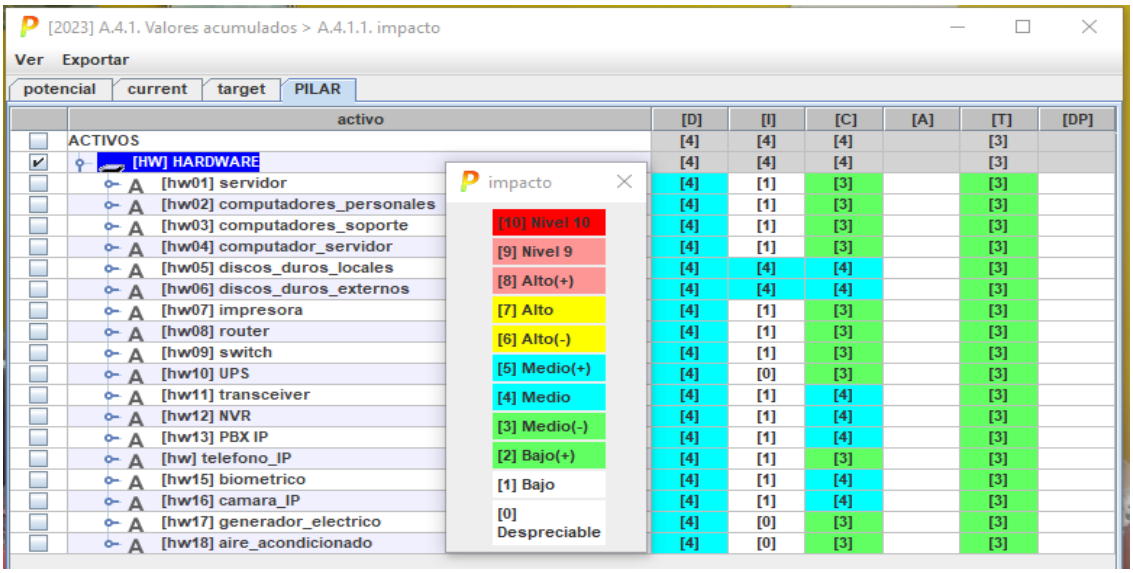
3.8 Evaluación de las Medidas Aplicadas a los Activos de Hardware en el Área de TIC

3.8.1 Estimación del Impacto Acumulado Residual

Una vez aplicadas las salvaguardas que propone la herramienta Pilar se evaluó su nivel de eficacia, calculando el impacto acumulado donde se obtuvo como resultado un nivel de impacto medio con una valoración de 4 a 3 en todos los activos en función de la dimensión disponibilidad, confidencialidad, y trazabilidad; un nivel de impacto bajo y despreciable con una valoración de 1 a 0 en la dimensión de integridad, como se indica en la siguiente figura 37.

Figura 37

Impacto acumulado residual

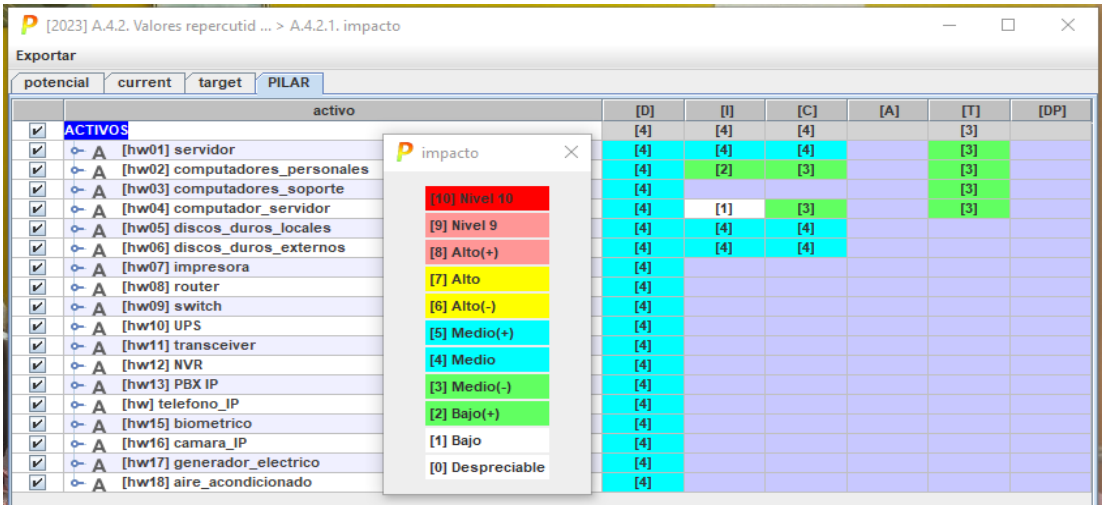


***Nota**: Adaptado de la herramienta pilar, versión 2023.1.1*

También, se calculó el nivel de impacto repercutido una vez desplegadas las salvaguardas que dispone la herramienta Pilar, se obtuvo una valoración de un nivel de impacto medio con valor de 4 en disponibilidad, integridad y confidencialidad; un impacto medio con valores de 3 a 2 en integridad, confidencialidad, y trazabilidad; y un impacto bajo con un valor de 1 en la dimensión de integridad, como se visualiza en la siguiente figura 38.

Figura 38

Impacto repercutido residual



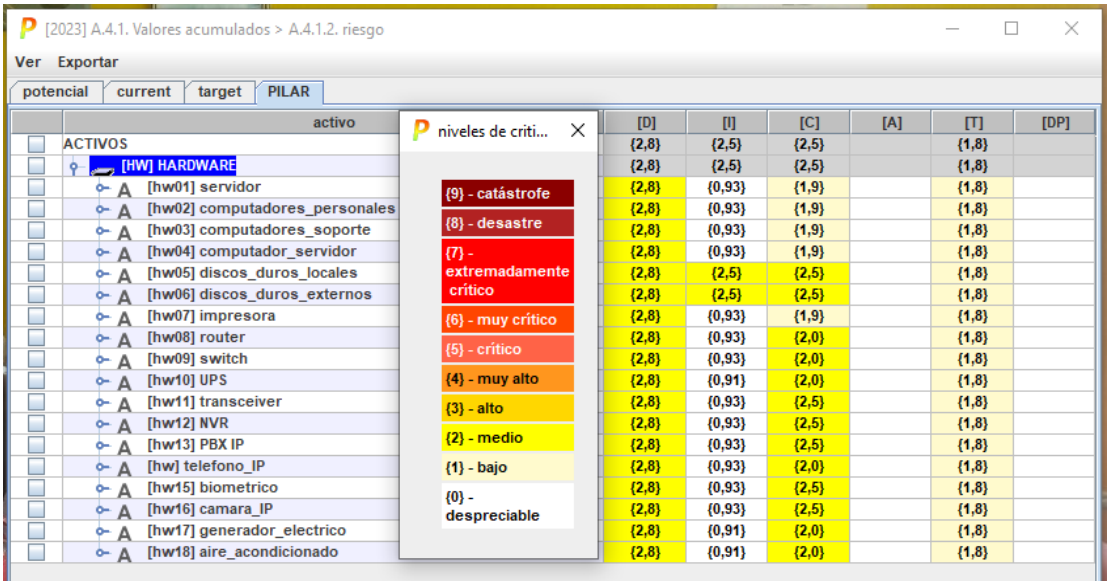
***Nota**: Adaptado de la herramienta pilar, versión 2023.1.1*

3.8.2 Estimación del Riesgo Acumulado Residual

Al gestionar las salvaguardas que propone la herramienta Pilar, se evaluó el nivel de riesgo, donde se logró como consecuencia en el riesgo acumulado un nivel medio en todos los activos en la dimensión de disponibilidad y en confidencialidad trece activos, y en integridad dos activos; un nivel bajo en todos los activos en la dimensión de trazabilidad, mientras que en confidencialidad hay cinco activos; y despreciable en todos los activos en integridad, como resulta en la siguiente figura 39.

Figura 39

Riesgo acumulado residual

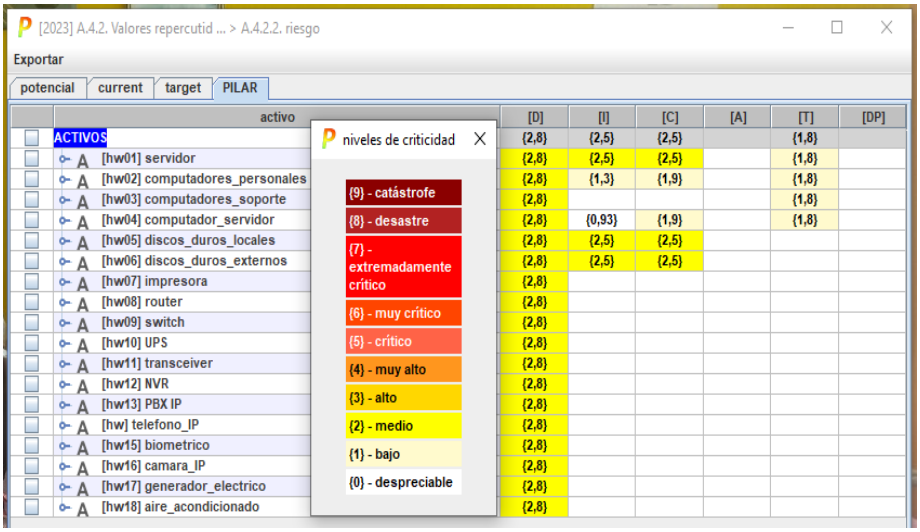


***Nota**: Adaptado de la herramienta pilar, versión 2023.1.1*

Posteriormente, se calculó el riesgo repercutido una vez que se gestionó las salvaguardas que propone la herramienta Pilar, se mitigaron las amenazas y vulnerabilidades donde se obtuvo como resultados un nivel de riesgo medio en todos los activos en la dimensión de disponibilidad, tres activos con nivel medio en la integridad y confidencialidad; un nivel bajo en cuatro activos en trazabilidad, dos en confidencialidad y un activo en integridad; y un nivel despreciable en la dimensión de integridad, como resulta en la siguiente figura 40.

Figura 40

Riesgo repercutido residual



***Nota**: Adaptado de la herramienta pilar, versión 2023.1.1*

Capítulo IV

4. Resultados y Discusión

4.1 Análisis de Resultados

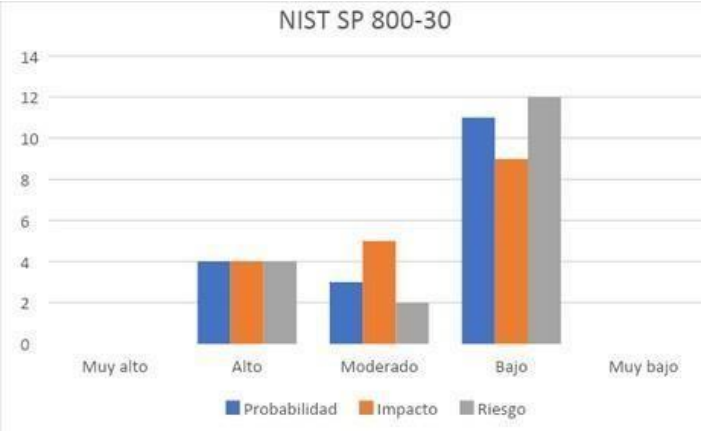
Para mejorar la seguridad de la información en el área de TIC, de la Universidad Técnica Luis Vargas Torres de Esmeraldas se aplicó dos metodologías con la finalidad de identificar y priorizar los riesgos de seguridad de la información, y la selección de la metodología a aplicar dependerá de su nivel de madurez al cumplimiento con los objetivos y misión de la institución. A continuación, se muestran de forma detallada los resultados obtenidos de estas dos metodologías:

Metodología NIST 800 – 30

En la figura 41, se reflejan los resultados en cuanto a probabilidad, impacto y riesgo que existen en cada uno de los activos. Donde, la escala de evaluación utilizada corresponde de 10 a 9 muy alto; de 8 a 6 alto; de 5 a 3 moderado, de 2 a 1 bajo y 0 con valor de muy bajo.

Figura 41

Resultados del proceso de gestión de riesgos de la NIST

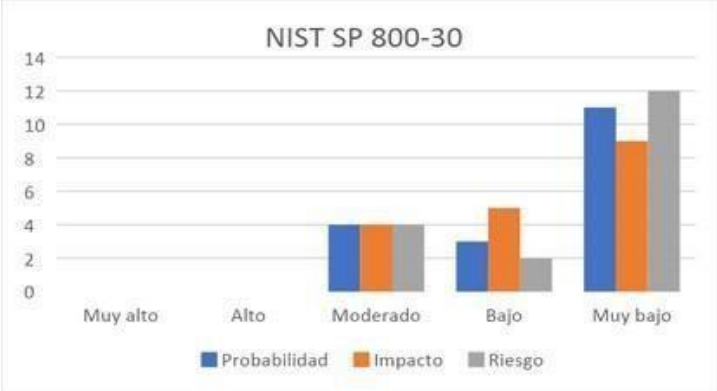


***Nota**: Probabilidad: existen 4 activos en nivel alto, 3 activos en nivel moderado, y 11 activos en nivel bajo. Impacto: 4 activos en nivel alto, 5 activos en nivel moderado, y 9 activos en nivel bajo. Riesgo: 4 activos en nivel alto, 2 en nivel moderado y 12 activos en nivel bajo, elaboración propia.*

Una vez implementadas las medidas de mitigación, se puede determinar que los niveles de probabilidad, impacto y riesgo han disminuido, como se muestra en la siguiente figura 42.

Figura 42

Resultados de NIST al aplicar las medidas de protección



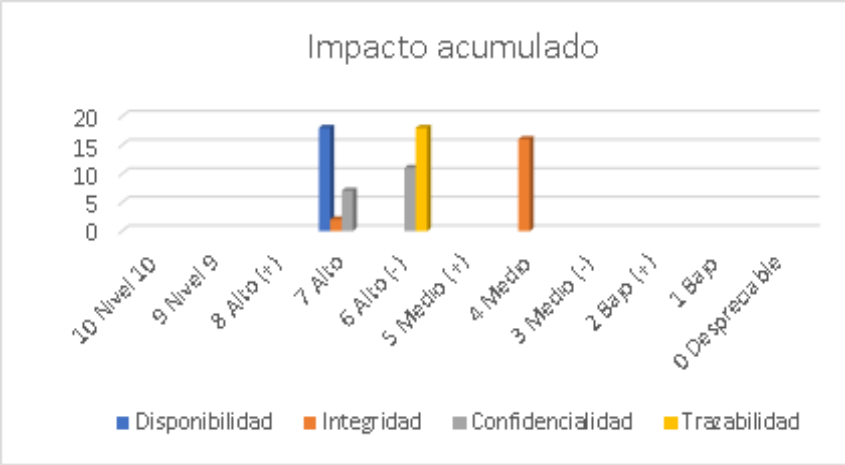
***Nota**: Probabilidad: existen 4 activos en nivel moderado, 3 activos en nivel bajo y 11 activos en nivel muy bajo. Impacto: 4 activos en nivel moderado, 5 activos en nivel bajo y 9 activos en nivel muy bajo. Riesgo: 4 activos en nivel moderado, 2 en nivel bajo y 12 activos en nivel muy bajo, elaboración propia.*

Metodología MAGERIT

En este apartado, se muestran los resultados tomando en cuenta el impacto acumulado, el impacto repercutido y a su vez el riesgo acumulado y repercutido. En la figura 43, en el impacto acumulado se obtuvo lo siguiente:

Figura 43

Resultados del impacto acumulado

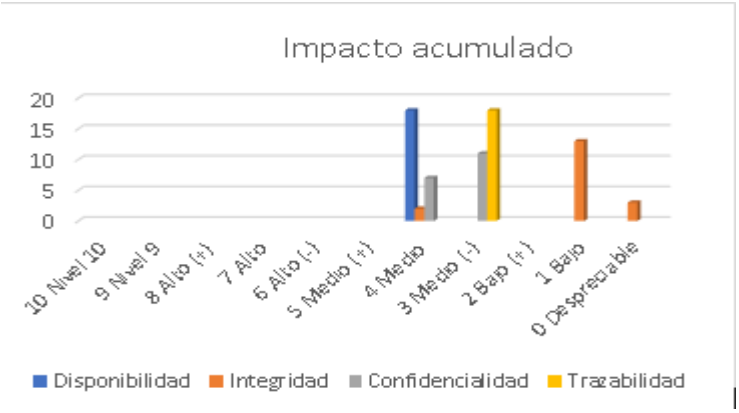


***Nota**: 18 activos en nivel alto en cuanto a disponibilidad, en integridad 2 activos en nivel alto y 16 activos en nivel medio, 7 y 11 activos en nivel alto en confidencialidad, y 18 activos en nivel alto en cuanto a trazabilidad, elaboración propia.*

Al aplicar las medidas sugeridas de mitigación se puede determinar que el nivel de impacto acumulado ha disminuido, como se refleja en la figura 44.

Figura 44

Resultados del impacto acumulado con salvaguardas

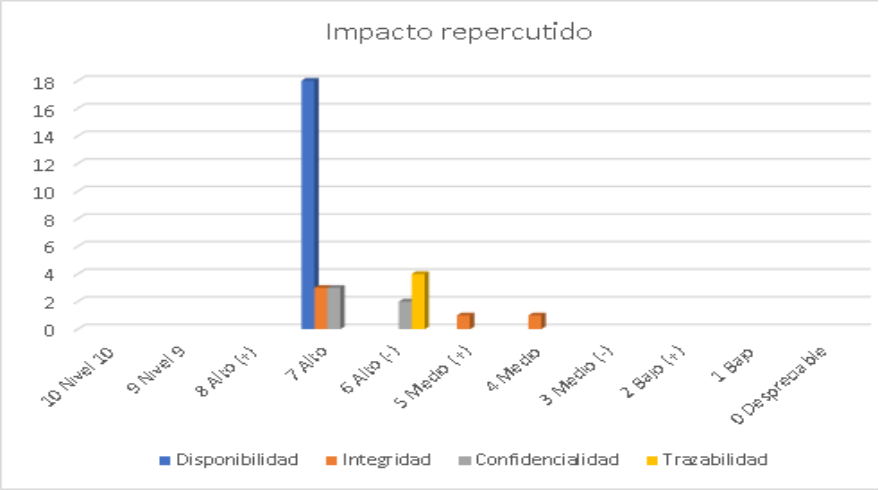


***Nota**: 18 activos en nivel medio en cuanto a disponibilidad, en integridad 2 activos en nivel medio, 13 activos en nivel bajo y 3 activos en nivel despreciable, 7 y 11 activos en nivel medio en confidencialidad, y 18 activos en nivel medio en cuanto a trazabilidad, elaboración propia.*

En la figura 45, en el impacto repercutido se obtuvo lo siguiente:

Figura 45

Resultados del impacto repercutido

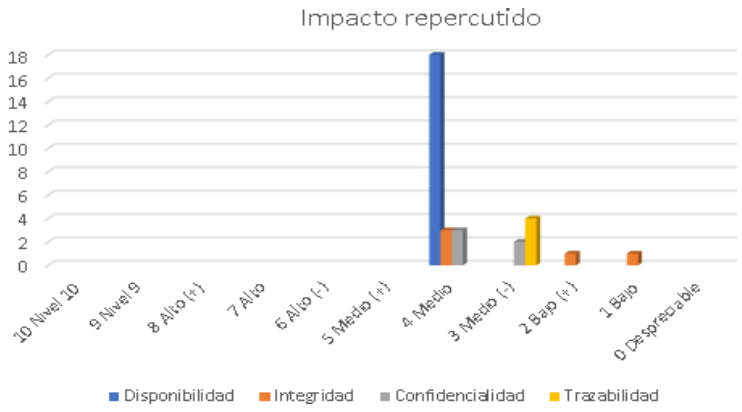


Nota: 18 activos en nivel alto en cuanto a disponibilidad, en integridad 3 activos en nivel alto y 2 activos en nivel medio, 5 activos en nivel alto en confidencialidad, y 4 activos en nivel alto en cuanto a trazabilidad, elaboración propia.

Al aplicar las medidas de mitigación se puede determinar que el nivel de impacto repercutido ha disminuido, como se refleja en la figura 46.

Figura 46

Resultados del impacto repercutido con salvaguardas

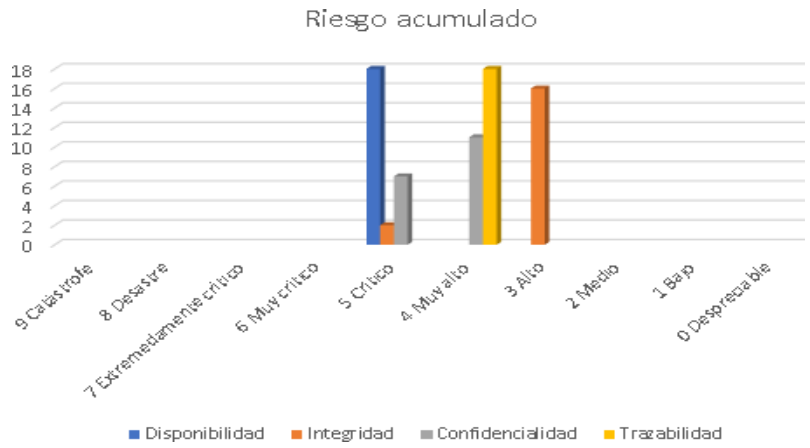


Nota: 18 activos en nivel medio en cuanto a disponibilidad, en integridad 3 activos en nivel medio y 2 activos en nivel bajo, 5 activos en nivel medio en confidencialidad, y 4 activos en nivel medio en cuanto a trazabilidad, elaboración propia.

En la figura 47, en el riesgo acumulado se obtuvo lo siguiente:

Figura 47

Resultados del riesgo acumulado

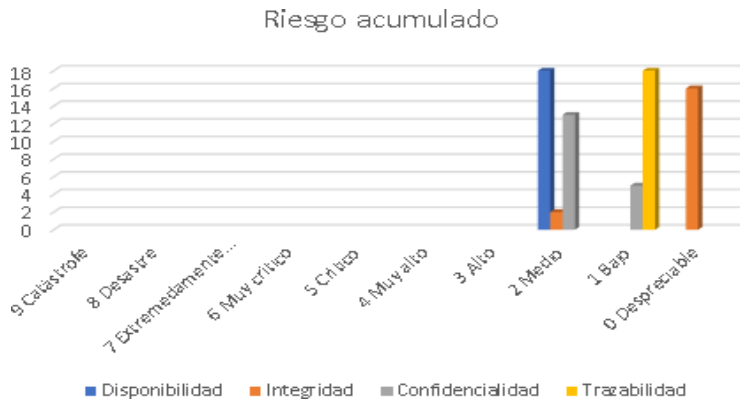


Nota: 18 activos en nivel crítico en cuanto a disponibilidad, en integridad 2 activos en nivel crítico y 16 activos en nivel alto, 7 activos en nivel crítico y 11 activos en nivel muy alto en confidencialidad, y 18 activos en nivel muy alto en cuanto a trazabilidad, elaboración propia.

Al aplicar las medidas sugeridas de mitigación se puede determinar que el nivel de riesgo acumulado ha disminuido, como se refleja en la figura 48.

Figura 48

Resultados del riesgo acumulado con salvaguardas

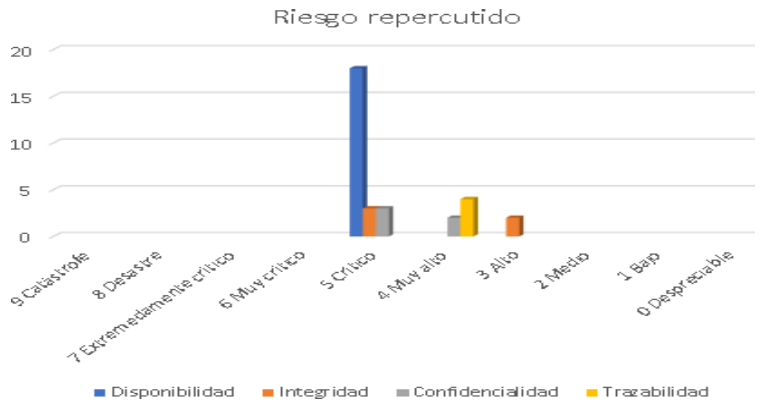


Nota: 18 activos en nivel medio en cuanto a disponibilidad, en integridad 2 activos en nivel medio, y 16 activos en nivel despreciable; 13 activos en nivel medio y 5 activos en nivel bajo en confidencialidad; y 18 activos en nivel bajo en cuanto a trazabilidad, elaboración propia.

En la figura 49, en el riesgo repercutido se obtuvo:

Figura 49

Resultados del riesgo repercutido

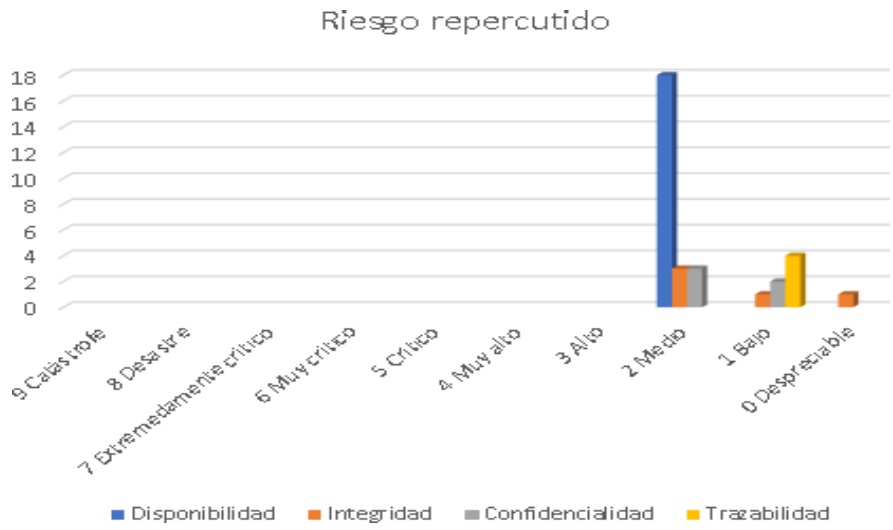


Nota: 18 activos en nivel crítico en cuanto a disponibilidad; en integridad 3 activos en nivel crítico y 2 activos en nivel alto; 3 activos en nivel crítico y 2 activos en nivel muy alto en confidencialidad, y 4 activos en nivel muy alto en cuanto a trazabilidad, elaboración propia.

Al aplicar las medidas de mitigación se puede determinar que el nivel de riesgo repercutido ha disminuido, como se refleja en la figura 50.

Figura 50

Resultados del riesgo repercutido con salvaguardas



Nota: 18 activos en nivel medio en cuanto a disponibilidad; en integridad 3 activos en nivel medio, 1 activo en nivel bajo y 1 activo en nivel despreciable; 3 activos en nivel medio y 2 activos en nivel bajo en confidencialidad; 4 activos en nivel bajo en cuanto a trazabilidad, elaboración propia.

4.2 Discusión

Para conocer la situación actual del área de TIC, se realizó entrevistas al director y al personal del departamento para posteriormente identificar los riesgos de seguridad en los equipos informáticos del sistema de información del área de TIC, al calcular la probabilidad, impacto y nivel de riesgo, los resultados reflejaron que los activos están expuestos desde niveles críticos, hasta nivel medio, esto quiere decir que se debe emplear medidas de protección capaces de mitigar los riesgos.

Estos resultados, son respaldados por Ávila Torres Remigio (2021), quien, en su proceso de investigación, obtuvo como resultado 43 riesgos en nivel alto, 269 en nivel medio y 88 riesgos en nivel bajo, para posteriormente elaborar un plan de tratamiento de los riesgos, haciendo uso de los estándares internacionales como el COBIT 5 o la familia ISO/IEC 27000, ISO/IEC 31000.

Analizando ambos resultados se puede afirmar que es indispensable realizar un análisis de riesgos en los activos de información porque permite gestionar los riesgos de la forma más factible, ya que no existe un sistema seguro al 100%.

Al estimar el nivel de impacto en el proceso de gestión de riesgos del MAGERIT v.3 a través de la herramienta Pilar se puede determinar que la dimensión más recurrente es la disponibilidad y trazabilidad, donde se obtuvo como resultado que todos los activos en nivel alto en impacto acumulado y en impacto repercutido.

De acuerdo con, Víctor Félix Barrezueta Bermeo (2023), donde hubo similitud en la dimensión de disponibilidad, obtuvo en sus resultados niveles con valoración de 10 siendo este el nivel más alto que después de gestionar las salvaguardas los niveles que obtuvo fueron altos con valoración de 6 hasta el nivel despreciable con valor de 0. Con este fundamento se optó por gestionar los riesgos, aplicando salvaguardas que dieron como consecuencia un nivel medio en cuanto a disponibilidad con valoración de 4 y trazabilidad nivel medio con valores de 3.

En consecuencia, al determinar el impacto, el siguiente paso es establecer medidas de protección que permitan reducir los riesgos de seguridad de acuerdo a la normativa ISO/IEC 27001:2022 se puede determinar que, dentro de los 93 controles, las medidas sugeridas fueron las siguientes: controles físicos, controles organizacionales, controles tecnológicos, y control de personas con un nivel de madurez de reproducible a un proceso definido, mientras que el NIST Cybersecurity Framework, en la función de Identificar se seleccionó 26 controles, en la función de Proteger hay 30 controles, en la función de Detectar existen 18 controles, en la función e Responder se toma 16 controles, en la función de Recuperar se eligió 6 controles; los controles tuvieron un nivel de madurez gestionable y medible indicando que los controles están monitorizados.

Esto tiene relación con resultados encontrados en otras investigaciones, en la cual, Chiriboga Mera Teresa (2022), realizó una propuesta de un modelo hibrido basado en la metodología MAGERIT e ISO 27001 donde incluye controles para contrarrestar las amenazas, pero estoy en desacuerdo con la autora ya que en su trabajo realiza una simulación de los riesgos, cuando en un trabajo de investigación debe irse al campo de acción. Los resultados determinan que la implementación de medidas, es necesaria para minimizar o mitigar los riesgos identificados, mejorando la eficacia de toda la institución.

Por último, se evaluó las medidas de protección aplicadas en los activos en el área de TIC, en los resultados encontrados en esta investigación se observó que el nivel de impacto

y riesgo disminuyeron al gestionar las salvaguardas propuestas. Los resultados coinciden con lo obtenido por Luis Adrián Chóez Acosta (2020), quien evaluó los riesgos después de aplicar las salvaguardas. Para finalizar, los resultados obtenidos evidencian que la efectividad de las salvaguardas sugeridas está determinada por un nivel de madurez de reproducible pero intuitivo a gestionable y medible.

Conclusiones y Recomendaciones

Conclusiones

- El proceso de gestión de riesgos, es de vital importancia en una organización, porque permite identificar, comprender, evaluar y mitigar los riesgos; esto debido a que, si no se conoce el riesgo al que puedan estar expuestos los activos informáticos, muy difícil ayudará a evitar la posibilidad de que ocurra un incidente.

  Dentro del análisis se logró identificar que el nivel de impacto es alto en todos los activos, mayormente afectado en la dimensión de la disponibilidad y trazabilidad; mientras que en el riesgo potencial alcanzó niveles críticos, muy alto y alto en disponibilidad, integridad y trazabilidad.

  Es por ello, que la identificación de los riesgos es necesaria para las operaciones, la realización de la misión y la continuidad de las operaciones permitiendo a una organización evaluar lo que está tratando de proteger, y por qué, como elemento de apoyo a la decisión en la identificación de medidas de seguridad.
- La utilización de la herramienta Pilar, permitió la identificación y clasificación de los activos, así como evaluar las posibles amenazas a los que se encuentran expuestos, analizando su nivel de impacto, riesgo, y frecuencia de cada activo en cada una de las dimensiones de la tríada de la seguridad adicionalmente incluyendo a la función de trazabilidad, riesgos que fueron controlados utilizando las medidas de mitigación, los salvaguardas, y los controles de la ISO/IEC 27001:2022 y del NIST Cybersecurity.
- Las medidas de protección orientadas en la ISO/IEC 27001:2022 y NIST Cybersecurity Framework fueron identificadas y valoradas empleando un nivel de madurez de L0 que significa inexiste a L5 que es optimizado, dentro de los resultados las salvaguardas tuvieron una valoración desde L2, donde indica que las salvaguardas son reproducibles hasta L4 donde las medidas son gestionadas y medibles, esto permitió al personal del departamento mitigar su nivel de impacto y riesgo encontrados.
- Evaluar las medidas de protección sugeridas permitió llevar el nivel de riesgo crítico, muy alto y alto en los activos de hardware a valores aceptables, esto indica

que el riesgo fue contrarrestado a un nivel medio, bajo y despreciable, ayudando a la toma de decisiones de manera oportuna para garantizar en todo momento las tres propiedades de la información.

Recomendaciones

- Designar un responsable dentro del área de TIC, que asuma un rol determinante en el control, seguimiento y actualización de políticas de seguridad de la información.
- Capacitar continuamente al personal de TIC sobre temas de seguridad de la información, al menos tres veces al año.
- Mantener actualizado los riesgos y amenazas, ya que al pasar el tiempo pueden sufrir cambios, en especial cuando se integran nuevos activos.
- Realizar una revisión continua de las políticas de seguridad de la información, con el fin de mantener la información actualizada conforme exista cambios en los estándares internacionales.
- Realizar una análisis y evaluación a los activos de redes de comunicaciones, equipos auxiliares, instalaciones, software, servicios y al personal.

Referencias

Código Orgánico Integral Penal. (3 de Febrero de 2014). *CÓDIGO ORGÁNICO INTEGRAL PENAL, COIP*. Obtenido de CÓDIGO ORGÁNICO INTEGRAL PENAL, COIP: https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

Acosta, J. (2018). *Recuperando la ciberseguridad: prepárese para enfrentar ataques cibernéticos.* Obtenido de Recuperando la ciberseguridad: prepárese para enfrentar ataques cibernéticos: https://www.ey.com/es_pe/giss/recuperando-ciberseguridad-enfrentar-ataques-ciberneticos

Acosta, L. A. (2020). *Implementación de un plan de tratamiento de riesgos tecnológicos al centro de cómputo de una organización no gubernamental sin fines de lucro siguiendo la metodología MAGERIT.* Obtenido de Implementación de un plan de tratamiento de riesgos tecnológicos al centro de cómputo de una organización no gubernamental sin fines de lucro siguiendo la metodología MAGERIT: https://www.dspace.espol.edu.ec/xmlui/handle/123456789/50402

Agencia Nacional Digital. (Octubre de 2020). *Procedimiento de gestión de recursos.* Obtenido de Procedimiento de gestión de recursos.: https://and.gov.co/sites/default/files/2022-05/Guia_De_Gestion_y_clasificacion_de_activos_de_informacon.pdf

Alcamí, R. L., Carañana, C. D., & Herrando, J. G. (2011). *Introducción a la gestión de sistemas de información en las empresas.* Obtenido de Introducción a la gestión de sistemas de información en las empresas.: https://libros.metabiblioteca.org/server/api/core/bitstreams/7d943307-adc9-450d- 83a4-6638f1bd24b0/content

Arellano, D. A. (Julio de 2022). *Estrategias de prevención frente a los ciberataques* . Obtenido de Estrategias de prevención frente a los ciberataques : https://dspace.ups.edu.ec/bitstream/123456789/24173/1/UPS-GT004223.pdf

Arias, F. G. (2012). *El proyecto de investigación, introducción a la metodología científica.* Caracas- República Bolivariana de Venezuela: Episteme, C.A.

Asamblea Nacional de Ecuador. (27 de Agosto de 2021). *Biblioteca digital: Ley de Comercio Electrónico, Firmas.* Obtenido de Biblioteca digital: Ley de Comercio Electrónico, Firmas: http://biblioteca.defensoria.gob.ec/handle/37000/3374

Bermeo, V. F. (Junio de 2023). *Repositorio PUCESA.* Obtenido de Repositorio PUCESA: https://repositorio.pucesa.edu.ec/handle/123456789/4208

Chang, J. E. (2020). Análisis de ataques cibernéticos hacia el ecuador. *Aristas*, 10.

Chico, F., & Tatiana, D. (18 de 12 de 2019). *Gestión de cronograma e Ingeniería de costos del proyecto.* Obtenido de Gestión de cronograma e Ingeniería de costos del proyecto: http://repositorio.puce.edu.ec/handle/22000/17470

Contraloria General del Estado. (2023). *Contraloria General del Estado: Normas de control interno.* Obtenido de Contraloria General del Estado: Normas de control interno: https://www.contraloria.gob.ec/Portal/Sistema/NormasControlnterno

Daza, F. (05 de Mayo de 2022). *Guia para la identificación de activos de información.* Obtenido de Guia para la identificación de activos de información: https://www.idiger.gov.co/documents/20182/979738/TC-GU-02+Guia+para+la+identificaci%C3%B3n+de+activos+de+informaci%C3%B3n+V1.pdf/48100f8d-fd2f-4be0-af82-40fb1cda0141

Delgado, C. A. (2017). *Fundamentos de seguridad informática - CORE.* Obtenido de Fundamentos de seguridad informática - CORE: https://core.ac.uk/download/pdf/326424171.pdf

Figueroa, J., Rodriguez, R., Bone, C., & Saltos, J. (2017). La seguridad informática y la seguridad de la información. *Polo del conocimiento*, 11.

Gonzaga, C. A. (05 de Abril de 2021). *Gestión de riesgos informáticos aplicando una metodología.* Obtenido de Gestión de riesgos informáticos aplicando una metodología:

http://repositorio.utn.edu.ec/bitstream/123456789/11042/2/04%20ISC%20580%20TRABAJO%20GRADO.pdf

Guerrero, D. (Abril de 2018). *Planificar el cronograma.* Obtenido de Planificar el cronograma: https://pirhua.udep.edu.pe/bitstream/handle/11042/3608/a4b0ad77f1523df19d7bf18e5abfa32fc05753d10214ab8ca8dfb41781951ee4.pdf?sequence=1&isAllowed=y

IGAC. (Mayo de 2018). *Metodología - inventario de activos de información.* Obtenido de Metodología - inventario de activos de información: http://igacnet2.igac.gov.co/intranet/UserFiles/File/procedimientos/Metodologias%202008/2018/M15000%2001%2018%20V2%20%20Inventario%20Activos%20de%20Informacion.pdf

International Management Systems Marketing. (2022). *ISO/IEC 27001 : 2022 - IMSM.* Obtenido de ISO/IEC 27001 : 2022 - IMSM: https://www.imsm.com/es/wp-content/uploads/sites/12/2022/11/ISO-27001-2022-ES-V1.pdf

Jiménez, A., & Alfonso, E. V. (2015). *Selección de salvaguardas en gestión del riesgo en sistemas.* Obtenido de Selección de salvaguardas en gestión del riesgo en sistemas: https://oa.upm.es/40919/1/INVE_MEM_2015_223957.pdf

Juan, H. (2017). *Investigación Cualitativa.rtf - Juan Herrera .net.* Obtenido de Investigación Cualitativa.rtf - Juan Herrera .net: https://juanherrera.files.wordpress.com/2008/05/investigacion-cualitativa.pdf

Leal, J. A. (2019). *Seguridad de la información, la relación entre clasificación de activos de información y la gestión de riesgos.* Obtenido de Seguridad de la información, la relación entre clasificación de activos de información y la gestión de riesgos. : http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6266/00005217.pdf?sequence=1&isAllowed=y

Lehuedé, H. J. (11 de Septiembre de 2020). *La ciberseguridad y el rol del Directorio en Latinoamérica y el Caribe.* Obtenido de La ciberseguridad y el rol del Directorio en Latinoamérica y el Caribe:

https://www.cepal.org/sites/default/files/events/files/lehuede_presentacion_comtelca_0.pdf

Ley orgánica de protección de datos personales. (21 de Mayo de 2021). *LEY ORGÁNICA DE PROTECCIÓN DE DATOS.* Obtenido de LEY ORGÁNICA DE PROTECCIÓN DE DATOS: https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Lillo, J. S. (Junio de 2019). *Análisis y correlación entre probabilidad e impacto de los riesgos.* Obtenido de Análisis y correlación entre probabilidad e impacto de los riesgos.: https://core.ac.uk/download/pdf/219768322.pdf

Luna, A. A., & Simba, G. C. (2017). *Universidad Politécnica Salesiana sede Quito.* Obtenido de Universidad Politécnica Salesiana sede Quito: https://dspace.ups.edu.ec/bitstream/123456789/14631/1/UPS%20-%20ST003221.pdf

Macía, M. T. (2018). Análisis de riesgos en seguridad de la información. *Polo del Conocimiento,* 18.

Magerit. (2012). *MAGERIT – versión 3.0 Metodologías de análisis y gestión de riesgos de los sistemas de información, libro I.* Obtenido de MAGERIT – versión 3.0 Metodologías de análisis y gestión de riesgos de los sistemas de información, libro I: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Magerit. (Octubre de 2012). *MAGERIT – versión 3.0 Metodologías de análisis y gestión de riesgos de los sistemas de información, libro II.* Obtenido de MAGERIT – versión 3.0 Metodologías de análisis y gestión de riesgos de los sistemas de información, libro II: https://pilar.ccn-cert.cni.es/index.php/docman/documentos/2-magerit-v3- libro-ii-catalogo-de-elementos/file

Maldonado.J., C., Macho.L.K., G., & Casallas.E., C. (2023). La investigación aplicada y el desarrollo experimental en el fortalecimiento de las competencias de la sociedad del siglo XXI. *Tecnura,* 54.

Mera, T. J. (Octubre de 2022). *Escuela Superior Politécnica de Chimborazo.* Obtenido de Escuela Superior Politécnica de Chimborazo: http://dspace.espoch.edu.ec/bitstream/123456789/17706/1/20T01610.pdf

MINTIC. (1 de Abril de 2016). *Guía de gestión de riesgos.* Obtenido de Guía de gestión de riesgos: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

Nacional, E. C. (Mayo de 2004). *Ley Organica de Transparencia y Acceso a la.* Obtenido de Ley Organica de Transparencia y Acceso a la: https://www.educacionsuperior.gob.ec/wp-content/uploads/downloads/2014/09/LOTAIP.pdf

Naciones Unidas. (2018). *La Agenda 2030 y los objetivos de desarrollo sostenible: una oportunidad para América Latina y el Caribe.* Obtenido de La Agenda 2030 y los objetivos de desarrollo sostenible: una oportunidad para América Latina y el Caribe.: https://www.cepal.org/es/temas/agenda-2030-desarrollo-sostenible/objetivos-desarrollo-sostenible-ods

National Institute of Standards and Technology. (Septiembre de 2012). *Guide for Conducting Risk Assessments.* Obtenido de Guide for Conducting Risk Assessments: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf

Neill, D. A., & Suárez, L. C. (2018). Procesos y Fundamentos de la Investigación Científica. *UTMACH*, 33.

Ojeda, N., & Palacios, Y. (2018). Técnicas de investigación documental. *Redalyc*. Obtenido de Técnicas de investigación documental: https://repositorio.unan.edu.ni/12168/1/100795.pdf

Olmedo, J. I., & Gavilanez, F. L. (15 de Septiembre de 2018). *Análisis de los Ciberataques Realizados en América Latina.* Obtenido de Análisis de los Ciberataques Realizados en América Latina: https://repositorio.uide.edu.ec/bitstream/37000/3782/13/An%C3%A1lisis%20de%20los%20Ciberataques%20Realizados%20en%20Am%C3%A9rica%20Latina.pdf

Omar, G. A., & Vinicio, B. G. (Febrero de 2021). *Repositorio Universidad Técnica de Ambato.* Obtenido de Repositorio Universidad Técnica de Ambato: https://repositorio.uta.edu.ec/bitstream/123456789/32301/1/t1775si.pdf

Peña, H. M. (2019). *Aplicacion de la metodología magerit para el análisis de riesgos de los sistemas de control.* Obtenido de Aplicacion de la metodología magerit para el análisis de riesgos de los sistemas de control: https://repository.unad.edu.co/jspui/bitstream/10596/27758/1/1075211684.pdf

Pérez, J. S. (Enero de 2020). *Esquema Director de Seguridad para Empresas pymes del sector Construcción.* Obtenido de Esquema Director de Seguridad para Empresas pymes del sector Construcción: https://rua.ua.es/dspace/bitstream/10045/102087/1/Esquema_Director_de_Seguridad_para_Empresas_pymes_d_Diaz_Perez_Juan_Salvador.pdf

Ramiro, C. T. (2020). *Influencia de la metodología magerit v3 en la seguridad.* Obtenido de Influencia de la metodología magerit v3 en la seguridad: https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/7573/Cabrejos%20Torres%20Ramiro.pdf?sequ.

Sánchez, E. S. (2017). *Inclusión de los sistemas de información de una organización dentro del Esquema Nacional de seguridad (ENS) en virtud del Real Decreto 3/2010.* Obtenido de Inclusión de los sistemas de información de una organización dentro del Esquema Nacional de seguridad (ENS) en virtud del Real Decreto 3/2010: https://openaccess.uoc.edu/bitstream/10609/65269/18/esanchezsanchezTFM0617memm%C3%B2ria.pdf

Sanchez, F. P., & Calispa, N. I. (Marzo de 2021). *Universidad Politécnica Salesiana Sede Quito.* Obtenido de Universidad Politécnica Salesiana Sede Quito: https://dspace.ups.edu.ec/bitstream/123456789/19865/1/UPS%20-%20TTS276.pdf

Toledo, M. O. (2022). *Elaboración de una guía de implementación de un sgsi* . Obtenido de Elaboración de una guía de implementación de un sgsi : https://dspace.ups.edu.ec/bitstream/123456789/22091/1/UPS-CT009625.pdf

Torres, R. A. (2021). Análisis y evaluación de riesgos aplicado a EMAPAL-EP, basado en la metodología de MAGERIT versión 3.0. *Dialnet*, 14.

Universidad Técnica del Norte. (2023). *Universidad Técnica del Norte – Ciencia y Técnica al Servicio*. Obtenido de Universidad Técnica del Norte – Ciencia y Técnica al Servicio: https://www.utn.edu.ec/historia/

Universidad Técnica Luis Vargas Torres. (29 de Junio de 2016). *Estatuto - Universidad Técnica Luis Vargas Torres*. Obtenido de Estatuto - Universidad Técnica Luis Vargas Torres: https://www.utelvt.edu.ec/sitioweb/images/FAER/SECRETARIA1.pdf

Yazmin, C. R. (Noviembre de 2021). *Cybersecurity Framework, para el mejoramiento y estandarización de las evaluaciones tecnológicas del área de auditoría de TI que apoya las auditorías financieras de los clientes de HCR.* Obtenido de Cybersecurity Framework, para el mejoramiento y estandarización de las evaluaciones tecnológicas del área de auditoría de TI que apoya las auditorías financieras de los clientes de HCR: https://repositoriotec.tec.ac.cr/handle/2238/13508

Zambrano, K. Á., Vidal, W. B., & Vera, R. T. (2022). VULNERABILIDADES EN LOS SISTEMAS INFORMÁTICOS . *Journal Business Science*, 8.

Zevallos, M. (2019). Modelo de gestión de riesgos de seguridad de la información. *Peruana de Computación y Sistemas* , 18.

Anexos

Esmeraldas, 16 de junio del 2023

Para: PhD. Girard Vernaza Arroyo
Rector de la Universidad Técnica Luis Vargas Torres De Esmeraldas

De: Ing. Víctor Eduardo Quispe Mera

Asunto: Autorización para realizar un inventario de los equipos de hardware en el área de TIC.

De mi consideración:

Yo, **Quispe Mera Víctor Eduardo**, identificado con C.I **0804383495**, egresado de la carrera de **Ingeniería en Sistemas Informáticos**, de la Facultad de **Ingenierías y Tecnologías**, ante usted respetuosamente me presento y expongo:

Una vez culminado la carrera en dicha institución, solicito a usted el permiso/autorización para realizar el trabajo de caracterizar el equipamiento de hardware en conjunto con el área de TIC, dicha investigación tendrá propósitos académicos, por efecto del estudio de posgrado que estoy realizando actualmente.

Por la atención que brinde a la presente, agradezco y suscribo.

Atentamente,

Ing. Víctor Quispe Mera
Cel: 0989678140
Correo: victor.quispe.mera@utelvt.edu.ec

RECIBIDO
RECTORADO UTE - LVT
16-06-23 HORA: 11:55
FOLIO ING: 1014 ANEXO:
Ionela D
FIRMA RESPONSABLE

SCIENTIA ET THECNICUS IN SERVITIUM

UNIVERSIDAD TÉCNICA DEL NORTE

Resolución No. 001-073 CEAACES-2013-13

FACULTAD DE POSGRADO

Entrevista Al Director De Tic

De La Universidad Técnica Luis Vargas Torres

Fecha: 20 Junio 2023

Nombre: Ing. Leonardo Reyes

Objetivo: La presente tiene por objeto conocer el nivel de conocimiento de los riesgos de seguridad de la información, la finalidad es conocer sus puntos fuertes o áreas de mejora los resultados de esta investigación permitirán ayudarle a alcanzar su máximo potencial dentro del área de trabajo.

1. El departamento cuenta con manuales de:
   Usuario, para el mantenimiento preventivo/correctivo y de las políticas de seguridad del departamento de Tic.
2. El departamento cuenta con planes de:
   Recuperación de desastres naturales, plan de seguridad de los equipos, de recuperación ante ataques cibernéticos.
3. ¿Con que frecuencia realizan capacitaciones a los demás departamentos?
   Cada año se destina a una persona a realizar capacitaciones sobre el uso de alguna herramienta informática.
4. ¿Qué software privado utilizan?
   Software destinados a: la gestión del personal, el almacenamiento de la información y del antivirus.

5. ¿Con que frecuencia se realiza respaldo de la información?
Diariamente, se respalda la información en la nube.

6. ¿Cuántas personas tienen acceso a la información que se respalda?
Tres personas

7. ¿Qué tipo de vigilancia tiene el departamento?
Guardias de seguridad y cámaras de videovigilancia.

8. ¿Con que frecuencia ingresan personas diferentes al departamento?
A diario, ingresan personal administrativo, docentes, estudiantes, alrededor de más de 5 personas y menos de 10.

9. ¿Qué tipo de control se realiza para los visitantes en el departamento?
Anteriormente se realizaba un registro de control del motivo de ingreso pero por disminución del personal actualmente no se realiza ningún control.

10. Cuando un empleado deja de trabajar en el departamento ¿Cuánto tiempo transcurre para que sus cuentas estén inactivas?
Después de 30 días laborales.

11. ¿Existe un equipo de soporte, en caso de un ataque informático?
Por el momento, no. Solo existe una persona responsable de la seguridad de la información

12. ¿Cuáles son los controles fisicos de seguridad que se aplican para el acceso a los racks del servidor?
Se emplea cerraduras con llave, el biométrico y la videovigilancia.

Firma

SCIENTIA ET TECHNICUS IN SERVITIUM

UNIVERSIDAD TÉCNICA DEL NORTE

Resolución No. 001-073 CEAACES-2013-13

FACULTAD DE POSGRADO

SCIENTIA ET THECNICUS IN SERVITIUM

ENCUESTA AL DIRECTOR DE TIC

DE LA UNIVERSIDAD TÉCNICA LUIS VARGAS TORRES

Fecha: 20 Junio 2023

Nombre: Ing. Leonardo Reyes

Objetivo: La presente encuesta tiene por objeto conocer el nivel de conocimiento de los riesgos de seguridad de la información, la finalidad es conocer sus puntos fuertes o áreas de mejora los resultados de esta investigación permitirán ayudarle a alcanzar su máximo potencial dentro del área de trabajo.

Instrucciones: La encuesta cuenta con 21 preguntas y le tomará 10 minutos.

- Lea detenidamente y coloque una (X) en la casilla correspondiente según su apreciación.
- Asegúrese de marcar una sola alternativa, por favor no deje ningún ítem sin responder
- Si surge alguna duda, consulte al encuestador; cabe recordar que sus respuestas son confidenciales.

N°	Pregunta	Si	No
1	¿El centro de datos, dispone de personal de seguridad?		X
2	¿Existe un método de verificación o sistemas de identificación para restringir el acceso fisico al servidor?		X
3	¿Existe un control fisico de las personas que tienen acceso autorizado al servidor?		X
4	¿Cuenta con sistemas de bloqueo para racks de servidores o sistemas biométricos para el acceso a los racks?		X
5	¿Cuenta con firewalls fisicos?	X	
6	¿Cuenta con firewalls virtuales?	X	
7	¿Existe un plan de recuperación de desastres naturales?	X	
8	¿Existe un plan de recuperación ante posibles ciberataques?	X	
9	¿Cuenta sistema de detección y extinción contra incendios?		X

SCIENTIA ET THECNICUS IN SERVITIUM

10	¿Dispone de un certificado que asegure que el cableado del centro de datos está correctamente ubicado?		X
11	¿Tiene actualizado el router con las protecciones fisicas pertinentes?	X	
12	¿Utilizan filtros antispam y sistemas de encriptado de mensajes como medida de seguridad para asegurar la protección y privacidad del correo electrónico?	X	
13	¿Existen programas de prevención de pérdidas de datos (DLP) como medida de seguridad para supervisar que ningún usuario esté copiando o compartiendo información o datos que no debería?		X
14	¿Ha realizado un análisis de riesgo con su personal para conocer las fortalezas y debilidades de los equipos, la red interna, los servidores, las conexiones a Internet?	X	
15	¿Utilizan hardware para detectar, analizar y gestionar los puntos débiles del sistema?		X
16	¿Poseen certificación de normativas de seguridad?		X
17	¿Existe un procedimiento documentado para realizar mantenimiento al equipo biométrico?		X
18	¿Existen equipos de hardware como métodos de detección de intrusos para el computador del servidor?		X

19	¿Cuántas personas tienen acceso fisico al centro de datos? Una ( ) Dos ( ) Tres (X) Más de 5 ( )
20	¿Con que frecuencia comprueba que estén actualizados los equipos de hardware? Cada 15 días ( ) Cada 6 meses (X) Cada año ( ) Nunca ( )
21	¿Cada cuánto se realiza cambio de contraseñas a las cámaras IP? Cada mes ( ) Cada 3 meses ( ) Cada 6 meses (X) Cada año ( )

Firma

UNIVERSIDAD TÉCNICA DEL NORTE

Resolución No. 001-073 CEAACES-2013-13
FACULTAD DE POSGRADO

ENCUESTA AL PERSONAL DEL ÁREA DE TIC

DE LA UNIVERSIDAD TÉCNICA LUIS VARGAS TORRES

Fecha: 21 Junio de 2023
Nombre: Jorman Ordoñez Casierra

Objetivo: La presente encuesta tiene por objeto conocer el nivel de conocimiento de los riesgos de seguridad de la información, la finalidad es conocer sus puntos fuertes o áreas de mejora los resultados de esta investigación permitirán ayudarle a alcanzar su máximo potencial dentro del área de trabajo.

Instrucciones: La encuesta cuenta con 19 preguntas y le tomará 10 minutos.

- Lea detenidamente y coloque una (X) en la casilla correspondiente según su apreciación.
- Asegúrese de marcar una sola alternativa, por favor no deje ningún ítem sin responder
- Si surge alguna duda, consulte al encuestador; cabe recordar que sus respuestas son confidenciales.

Nº	Pregunta	Si	No
1	¿Conoce de que se trata la seguridad de la información?	X	
2	¿Conoce si existe una persona responsable de la seguridad de la información?	X	
3	¿Ha ocurrido algún incidente de pérdida o alteración de la información en su lugar de trabajo?	X	
4	¿Existe un sistema de alarma en caso de robo a un equipo?		X
5	Cuando ingresa una persona al departamento ¿Existe un control de ingreso?		X
6	Cuando no finaliza el trabajo en la institución ¿Almacena la información en los discos duros externos para terminar en casa?		X
7	¿Utiliza USB propios o posee alguno de la empresa para almacenar información?	X	

8	¿Analiza los discos duros internos y externos con el antivirus cada vez que lo conecta a su computador?	X	
9	¿Conoce de la existencia de un plan de seguridad de los sistemas y equipos informáticos?		X
10	¿Utiliza el antivirus en su dispositivo móvil durante su jornada laboral?	X	
11	¿Conoce las políticas de seguridad del departamento?		X
12	¿Ha formado parte de un equipo de trabajo para realizar un análisis de riesgo y vulnerabilidad de los equipos, la red interna, los servidores, las conexiones a Internet?	X	
13	¿Considera que se puede mejorar la infraestructura tecnológica del departamento?	X	
14	¿Existen sensores para controlar los niveles de temperatura y humedad del centro de datos?		X
15	¿Se imprimen documentos de otros departamentos?	X	

16	Si su respuesta a la pregunta anterior fue si ¿Con que frecuencia se imprimen los documentos al día? tres veces ( ) cinco veces (X) más de diez veces ( )
17	¿Cuántas capacitaciones ha recibido en este año acerca de los riesgos de la seguridad de la información? Más de 5 (X) Menos de 5 ( ) Una vez al mes ( ) Nunca ( )
18	¿Cada cuánto se realiza mantenimiento preventivo o correctivo a los equipos del centro de datos? Cada mes ( ) Cada 4 meses ( ) Cada 6 meses (X) Cada año ( )
19	¿Cada cuánto se realiza mantenimiento preventivo o correctivo a los equipos del departamento? Cada mes ( ) Cada 4 meses ( ) Cada 6 meses (X) Cada año ( )

Jairman Cadoñez

Firma

UNIVERSIDAD TÉCNICA DEL NORTE

Resolución No. 001-073 CEAACES-2013-13
FACULTAD DE POSGRADO

ENCUESTA AL PERSONAL DEL ÁREA DE TIC
DE LA UNIVERSIDAD TÉCNICA LUIS VARGAS TORRES

Fecha: 19 de junio del 2023
Nombre: Fabrizio Obregón Plaza

Objetivo: La presente encuesta tiene por objeto conocer el nivel de conocimiento de los riesgos de seguridad de la información, la finalidad es conocer sus puntos fuertes o áreas de mejora los resultados de esta investigación permitirán ayudarle a alcanzar su máximo potencial dentro del área de trabajo.

Instrucciones: La encuesta cuenta con 19 preguntas y le tomará 10 minutos.

- Lea detenidamente y coloque una (X) en la casilla correspondiente según su apreciación.
- Asegúrese de marcar una sola alternativa, por favor no deje ningún ítem sin responder
- Si surge alguna duda, consulte al encuestador; cabe recordar que sus respuestas son confidenciales.

Nº	Pregunta	Si	No
1	¿Conoce de que se trata la seguridad de la información?	X	
2	¿Conoce si existe una persona responsable de la seguridad de la información?	X	
3	¿Ha ocurrido algún incidente de pérdida o alteración de la información en su lugar de trabajo?	X	
4	¿Existe un sistema de alarma en caso de robo a un equipo?		X
5	Cuando ingresa una persona al departamento ¿Existe un control de ingreso?		X
6	Cuando no finaliza el trabajo en la institución ¿Almacena la información en los discos duros externos para terminar en casa?		X
7	¿Utiliza USB propios o posee alguno de la empresa para almacenar información?	X	

8	¿Analiza los discos duros internos y externos con el antivirus cada vez que lo conecta a su computador?		X
9	¿Conoce de la existencia de un plan de seguridad de los sistemas y equipos informáticos?	X	
10	¿Utiliza el antivirus en su dispositivo móvil durante su jornada laboral?	X	
11	¿Conoce las políticas de seguridad del departamento?	X	
12	¿Ha formado parte de un equipo de trabajo para realizar un análisis de riesgo y vulnerabilidad de los equipos, la red interna, los servidores, las conexiones a Internet?	X	
13	¿Considera que se puede mejorar la infraestructura tecnológica del departamento?	X	
14	¿Existen sensores para controlar los niveles de temperatura y humedad del centro de datos?		X
15	¿Se imprimen documentos de otros departamentos?	X	

16	Si su respuesta a la pregunta anterior fue si ¿Con que frecuencia se imprimen los documentos al día? tres veces ( ) cinco veces (X) más de diez veces ( )
17	¿Cuántas capacitaciones ha recibido en este año acerca de los riesgos de la seguridad de la información? Más de 5 ( ) Menos de 5 ( ) Una vez al mes (X) Nunca ( )
18	¿Cada cuánto se realiza mantenimiento preventivo o correctivo a los equipos del centro de datos? Cada mes ( ) Cada 4 meses ( ) Cada 6 meses (X) Cada año ( )
19	¿Cada cuánto se realiza mantenimiento preventivo o correctivo a los equipos del departamento? Cada mes ( ) Cada 4 meses ( ) Cada 6 meses (X) Cada año ( )

Firma

UNIVERSIDAD TÉCNICA DEL NORTE

Resolución No. 001-073 CEAACES-2013-13
FACULTAD DE POSGRADO

ENCUESTA AL PERSONAL DEL ÁREA DE TIC
DE LA UNIVERSIDAD TÉCNICA LUIS VARGAS TORRES

Fecha: 19 de junio 2023
Nombre: Santiago Lucas Gomez

Objetivo: La presente encuesta tiene por objeto conocer el nivel de conocimiento de los riesgos de seguridad de la información, la finalidad es conocer sus puntos fuertes o áreas de mejora los resultados de esta investigación permitirán ayudarle a alcanzar su máximo potencial dentro del área de trabajo.

Instrucciones: La encuesta cuenta con 19 preguntas y le tomará 10 minutos.

- Lea detenidamente y coloque una (X) en la casilla correspondiente según su apreciación.
- Asegúrese de marcar una sola alternativa, por favor no deje ningún ítem sin responder
- Si surge alguna duda, consulte al encuestador; cabe recordar que sus respuestas son confidenciales.

Nº	Pregunta	Si	No
1	¿Conoce de que se trata la seguridad de la información?	X	
2	¿Conoce si existe una persona responsable de la seguridad de la información?	X	
3	¿Ha ocurrido algún incidente de pérdida o alteración de la información en su lugar de trabajo?	X	
4	¿Existe un sistema de alarma en caso de robo a un equipo?		X
5	Cuando ingresa una persona al departamento ¿Existe un control de ingreso?		X
6	Cuando no finaliza el trabajo en la institución ¿Almacena la información en los discos duros externos para terminar en casa?		X
7	¿Utiliza USB propios o posee alguno de la empresa para almacenar información?		X

8	¿Analiza los discos duros internos y externos con el antivirus cada vez que lo conecta a su computador?		X
9	¿Conoce de la existencia de un plan de seguridad de los sistemas y equipos informáticos?		X
10	¿Utiliza el antivirus en su dispositivo móvil durante su jornada laboral?	X	
11	¿Conoce las políticas de seguridad del departamento?	X	
12	¿Ha formado parte de un equipo de trabajo para realizar un análisis de riesgo y vulnerabilidad de los equipos, la red interna, los servidores, las conexiones a Internet?	X	
13	¿Considera que se puede mejorar la infraestructura tecnológica del departamento?	X	
14	¿Existen sensores para controlar los niveles de temperatura y humedad del centro de datos?		X
15	¿Se imprimen documentos de otros departamentos?	X	

16	Si su respuesta a la pregunta anterior fue si ¿Con que frecuencia se imprimen los documentos al día? tres veces ( ) cinco veces (X) más de diez veces ( )
17	¿Cuántas capacitaciones ha recibido en este año acerca de los riesgos de la seguridad de la información? Más de 5 (X) Menos de 5 ( ) Una vez al mes ( ) Nunca ( )
18	¿Cada cuánto se realiza mantenimiento preventivo o correctivo a los equipos del centro de datos? Cada mes ( ) Cada 4 meses ( ) Cada 6 meses (X) Cada año ( )
19	¿Cada cuánto se realiza mantenimiento preventivo o correctivo a los equipos del departamento? Cada mes ( ) Cada 4 meses ( ) Cada 6 meses (X) Cada año ( )

Firma

UNIVERSIDAD TÉCNICA DEL NORTE

Resolución No. 001-073 CEAACES-2013-13
FACULTAD DE POSGRADO

ENCUESTA AL PERSONAL DEL ÁREA DE TIC
DE LA UNIVERSIDAD TÉCNICA LUIS VARGAS TORRES

Fecha: 20 junio 2023

Nombre: Cristina Cotera Bermeo

Objetivo: La presente encuesta tiene por objeto conocer el nivel de conocimiento de los riesgos de seguridad de la información, la finalidad es conocer sus puntos fuertes o áreas de mejora los resultados de esta investigación permitirán ayudarle a alcanzar su máximo potencial dentro del área de trabajo.

Instrucciones: La encuesta cuenta con 19 preguntas y le tomará 10 minutos.

- Lea detenidamente y coloque una (X) en la casilla correspondiente según su apreciación.
- Asegúrese de marcar una sola alternativa, por favor no deje ningún ítem sin responder
- Si surge alguna duda, consulte al encuestador; cabe recordar que sus respuestas son confidenciales.

Nº	Pregunta	Si	No
1	¿Conoce de que se trata la seguridad de la información?	X	
2	¿Conoce si existe una persona responsable de la seguridad de la información?		X
3	¿Ha ocurrido algún incidente de pérdida o alteración de la información en su lugar de trabajo?	X	
4	¿Existe un sistema de alarma en caso de robo a un equipo?		X
5	Cuando ingresa una persona al departamento ¿Existe un control de ingreso?		X
6	Cuando no finaliza el trabajo en la institución ¿Almacena la información en los discos duros externos para terminar en casa?	X	
7	¿Utiliza USB propios o posee alguno de la empresa para almacenar información?	X	

8	¿Analiza los discos duros internos y externos con el antivirus cada vez que lo conecta a su computador?		X
9	¿Conoce de la existencia de un plan de seguridad de los sistemas y equipos informáticos?	X	
10	¿Utiliza el antivirus en su dispositivo móvil durante su jornada laboral?		X
11	¿Conoce las políticas de seguridad del departamento?	X	
12	¿Ha formado parte de un equipo de trabajo para realizar un análisis de riesgo y vulnerabilidad de los equipos, la red interna, los servidores, las conexiones a Internet?		X
13	¿Considera que se puede mejorar la infraestructura tecnológica del departamento?	X	
14	¿Existen sensores para controlar los niveles de temperatura y humedad del centro de datos?		X
15	¿Se imprimen documentos de otros departamentos?	X	

16	Si su respuesta a la pregunta anterior fue si ¿Con que frecuencia se imprimen los documentos al día? tres veces (X) cinco veces ( ) más de diez veces ( )
17	¿Cuántas capacitaciones ha recibido en este año acerca de los riesgos de la seguridad de la información? Más de 5 ( ) Menos de 5 (X) Una vez al mes ( ) Nunca ( )
18	¿Cada cuánto se realiza mantenimiento preventivo o correctivo a los equipos del centro de datos? Cada mes ( ) Cada 4 meses ( ) Cada 6 meses (X) Cada año ( )
19	¿Cada cuánto se realiza mantenimiento preventivo o correctivo a los equipos del departamento? Cada mes ( ) Cada 4 meses ( ) Cada 6 meses (X) Cada año ( )

Firma

UNIVERSIDAD TÉCNICA DEL NORTE

Resolución No. 001-073 CEAACES-2013-13
FACULTAD DE POSGRADO

ENCUESTA AL PERSONAL DEL ÁREA DE TIC

DE LA UNIVERSIDAD TÉCNICA LUIS VARGAS TORRES

Fecha: 20 Junio de 2023
Nombre: Héctor Sacón Klinger

Objetivo: La presente encuesta tiene por objeto conocer el nivel de conocimiento de los riesgos de seguridad de la información, la finalidad es conocer sus puntos fuertes o áreas de mejora los resultados de esta investigación permitirán ayudarle a alcanzar su máximo potencial dentro del área de trabajo.

Instrucciones: La encuesta cuenta con 19 preguntas y le tomará 10 minutos.

- Lea detenidamente y coloque una (X) en la casilla correspondiente según su apreciación.
- Asegúrese de marcar una sola alternativa, por favor no deje ningún ítem sin responder
- Si surge alguna duda, consulte al encuestador; cabe recordar que sus respuestas son confidenciales.

Nº	Pregunta	Si	No
1	¿Conoce de que se trata la seguridad de la información?	X	
2	¿Conoce si existe una persona responsable de la seguridad de la información?	X	
3	¿Ha ocurrido algún incidente de pérdida o alteración de la información en su lugar de trabajo?	X	
4	¿Existe un sistema de alarma en caso de robo a un equipo?		X
5	Cuando ingresa una persona al departamento ¿Existe un control de ingreso?		X
6	Cuando no finaliza el trabajo en la institución ¿Almacena la información en los discos duros externos para terminar en casa?	X	
7	¿Utiliza USB propios o posee alguno de la empresa para almacenar información?	X	

8	¿Analiza los discos duros internos y externos con el antivirus cada vez que lo conecta a su computador?	X	
9	¿Conoce de la existencia de un plan de seguridad de los sistemas y equipos informáticos?		X
10	¿Utiliza el antivirus en su dispositivo móvil durante su jornada laboral?	X	
11	¿Conoce las políticas de seguridad del departamento?	X	
12	¿Ha formado parte de un equipo de trabajo para realizar un análisis de riesgo y vulnerabilidad de los equipos, la red interna, los servidores, las conexiones a Internet?		X
13	¿Considera que se puede mejorar la infraestructura tecnológica del departamento?	X	
14	¿Existen sensores para controlar los niveles de temperatura y humedad del centro de datos?		X
15	¿Se imprimen documentos de otros departamentos?	X	

16	Si su respuesta a la pregunta anterior fue si ¿Con que frecuencia se imprimen los documentos al día? tres veces (X) cinco veces ( ) más de diez veces ( )
17	¿Cuántas capacitaciones ha recibido en este año acerca de los riesgos de la seguridad de la información? Más de 5 ( ) Menos de 5 (X) Una vez al mes ( ) Nunca ( )
18	¿Cada cuánto se realiza mantenimiento preventivo o correctivo a los equipos del centro de datos? Cada mes ( ) Cada 4 meses ( ) Cada 6 meses (X) Cada año ( )
19	¿Cada cuánto se realiza mantenimiento preventivo o correctivo a los equipos del departamento? Cada mes ( ) Cada 4 meses ( ) Cada 6 meses (X) Cada año ( )

Hector Sacon K.

Firma

Anexos NIST 800-30: Tarea 2.1

Identificación de Amenazas Adversarial y no Adversarial

Ficha de Observación

Identificador	Activo	Observaciones	Fuentes de amenaza
A01	Servidor	No hay un control físico establecidos para el ingreso.	Insider de confianza
A02	Computadores personales	Alteración de la información.	Insider privilegiado
A03	Computadores de soporte	Expuestos al polvo.	Estructural
A04	Computador servidor	No disponen de equipo de hardware para detectar hacker.	Insider privilegiado
A05	Discos duros locales	Susceptibilidad a la pérdida del equipo.	Accidental
A06	Discos duros externos	Susceptibilidad a la pérdida del equipo.	Accidental
A07	Impresora monocromática	Ingresan empleados de otros departamentos a imprimir documentos.	Accidental
A08	Router – Mikrotik	Expuestos al polvo.	Estructural
A09	Switch – Cisco	Expuestos al polvo.	Estructural
A10	UPS	Expuestos al polvo.	Estructural

A11	Transceiver	Expuestos al polvo.	Estructural
A12	NVR	Expuestos al polvo.	Estructural
A13	PBX IP	Expuestos al polvo.	Estructural
A14	Teléfonos IP	No hay políticas definidas ya que cualquiera puede usar el teléfono.	Accidental
A15	Biométrico	No hay un mantenimiento eficiente.	Información confidencial
A16	Cámara IP, Hik – Vision	Errores de actualización.	Accidental
A17	Generador eléctrico	Variaciones en el voltaje.	Ambiental
A18	Aire acondicionado	No existen equipos que regulen la temperatura y la humedad.	Estructural

Anexos NIST 800-30: Tarea 2.1

Valoración de Amenazas Adversariales y no Adversariales

Objetivo: Evaluar las fuentes de amenazas adversariales y no adversariales que son relevantes para el departamento de TIC, de acuerdo a las tablas propuestos en la guía, en su apéndice. Donde las amenazas adversariales son las causadas por individuos que tienen acceso a la información privilegiada, insider de confianza o privilegiado, usuarios, grupos, entre otros. Mientras que las amenazas no adversariales son errores causados accidentalmente en el curso de la ejecución de sus responsabilidades, fallas de equipos, desastres naturales.

Producto de entrada: Inventario de equipamiento de hardware.

Producto de salida: Consolidado de las amenazas en los activos de equipamiento de hardware.

Para el desarrollo de esta ficha se debe tener en cuenta las siguientes instrucciones:

- Para evaluar los activos según la capacidad, intención y orientación del adversario, se empleará la escala de valoración que se detalla a continuación:

Muy alto	Alto	Moderado	Bajo	Muy bajo
10 – 9	8-6	5 – 3	2 – 1	0

Valoración de Amenazas Adversariales

Identificador	Activo	Origen de la amenaza	Capacidad	Intención	Orientación
A01	Servidor	Insider de confianza	5	4	7
A02	Computador personal	Insider privilegiado	4	5	6
A04	Computador servidor	Insider privilegiado	4	5	3
A15	Biométrico	Información confidencial	4	4	3

Valoración de Amenazas no Adversariales

Identificador	Activo	Origen de la amenaza	Rango de efectos
A03	Computadores de soporte	Estructural	2
A05	Discos duros locales	Accidental	5
A06	Discos duros externos	Accidental	5
A07	Impresora monocromática	Accidental	2
A08	Router – Mikrotik	Estructural	5
A09	Switch – Cisco	Estructural	4
A10	UPS	Estructural	4
A11	Transceiver	Estructural	4
A12	NVR	Estructural	5
A13	PBX IP	Estructural	2
A14	Teléfonos IP	Accidental	2
A16	Cámara IP, Hik – Vision	Accidental	2
A17	Generador eléctrico	Ambiental	5
A18	Aire acondicionado	Estructural	4

Anexos NIST 800-30: Tarea 2.3

Identificar Vulnerabilidades

Objetivo: La finalidad consiste en identificar las vulnerabilidades que afectan la probabilidad de que los eventos de amenaza de interés resultan en impactos adversos.

Producto de entrada: Inventario de equipamiento de hardware.

Producto de salida: Consolidado de las vulnerabilidades detectadas en los activos de equipamiento de hardware. Para el desarrollo de esta ficha se debe tener en cuenta las siguientes instrucciones:

- Para evaluar los activos se emplea la escala de valoración que se detalla a continuación:

Muy alto	Alto	Moderado	Bajo	Muy bajo
10 – 9	8-6	5 – 3	2 – 1	0

Que corresponde a:

- Muy alto: La vulnerabilidad está expuesta y es explotable.
- Alto: La vulnerabilidad es de alta preocupación.
- Moderado: La vulnerabilidad es de preocupación moderada.
- Bajo: La vulnerabilidad es una preocupación menor.
- Muy bajo: La vulnerabilidad no es motivo de preocupación.

Identificador	Activo	Vulnerabilidad Fuente de información	Gravedad
A01	Servidor	No existe control de los accesos físicos realizados al servidor.	8
A02	Computadores personales	Pérdida y alteración de la información.	8

A03	Computadores de soporte	Falta de mantenimiento preventivo.	2
A04	Computador servidor	Carece de métodos de detección de intrusos (hardware).	7
A05	Discos duros locales	No se evidencian bitácoras para el ingreso al departamento.	5
A06	Discos duros externos	No se evidencian bitácoras para el ingreso al departamento.	5
A07	Impresora monocromática	Se imprimen documentos de otros departamentos.	2
A08	Router - Mikrotik	Falta de mantenimiento preventivo.	2
A09	Switch – Cisco	Falta de mantenimiento preventivo.	2
A10	UPS	Falta de mantenimiento preventivo.	4
A11	Transceiver	Falta de mantenimiento preventivo.	2
A12	NVR	Falta de mantenimiento preventivo.	2
A13	PBX IP	Falta de mantenimiento preventivo.	2
A14	Teléfonos IP	Falta de políticas de uso definidas.	2
A15	Biométrico	Ausencia de un eficiente control en el mantenimiento.	8
A16	Cámara IP, Hik – Vision	Las contraseñas se cambian cada 3 meses.	2
A17	Generador eléctrico	Energía eléctrica insuficiente.	5

A18	Aire acondicionado	Falta de sensores de monitoreo de temperatura y humedad.	5

Anexos NIST 800-30: Tarea 2.4

Determinar la Probabilidad

Objetivo: Determinar la probabilidad de que los eventos de amenaza de interés resulten en impactos adversos, considerando: las características de las fuentes de amenaza que podrían iniciar los eventos, las vulnerabilidades identificadas y la susceptibilidad que refleja las salvaguardas.

Producto de entrada: Tarea 2.3 Identificar vulnerabilidades.

Producto de salida: Consolidado de probabilidad de iniciación del evento de amenaza y que resulten en impactos en los activos equipamiento de hardware. Para el desarrollo de esta ficha se debe tener en cuenta las siguientes instrucciones:

- Para evaluar los activos se emplea la escala de valoración que se detalla a continuación:

Muy alto	Alto	Moderado	Bajo	Muy bajo
10 - 9	8-6	5 – 3	2 – 1	0

Que corresponde a:

- Muy alto: Es casi seguro que se inicie, ocurra un error o un acto de la naturaleza.
- Alto: Es muy probable que se inicie, ocurra un error o un acto de la naturaleza.
- Moderado: Es probable que se inicie, ocurra un error o un acto de la naturaleza.
- Bajo: Es poco probable que se inicie, ocurra un error o un acto de la naturaleza.
- Muy bajo: Es muy poco probable que se inicie, ocurra un error o un acto de la naturaleza.

Identificador	Activo	Probabilidad de iniciación del evento de amenaza	Probabilidad que resulten en impactos adversos
A01	Servidor	7	7
A02	Computadores personales	7	7
A03	Computadores de soporte	4	5
A04	Computador servidor	7	7
A05	Discos duros locales	2	2
A06	Discos duros externos	2	2
A07	Impresora monocromática	2	2
A08	Router - Mikrotik	4	2
A09	Switch – Cisco	4	2
A10	UPS	4	2
A11	Transceiver	4	2
A12	NVR	4	2
A13	PBX IP	4	2
A14	Teléfonos IP	2	2
A15	Biométrico	7	7
A16	Cámara IP, Hik – Vision	2	2
A17	Generador eléctrico	4	4
A18	Aire acondicionado	4	4

Anexos NIST 800-30: Tarea 2.4.1

Determinar la Probabilidad General

Objetivo: Determinar la probabilidad general que resulta de la probabilidad de iniciación de evento de amenaza y la probabilidad de resultar en impactos adversos.

Producto de entrada: Tarea 2.4 Determinar probabilidad.

Producto de salida: Consolidado de probabilidad general.

Para el desarrollo de esta ficha se debe tener en cuenta las siguientes instrucciones:

- Para evaluar los activos se emplea la escala de valoración que se detalla a continuación:

Probabilidad de iniciación	**Probabilidad que resulten en impactos adversos**				
	Muy bajo	**Bajo**	**Moderado**	**Alto**	**Muy alto**
Muy alto	Bajo	Moderado	Alto	Muy alto	Muy alto
Alto	Bajo	Moderado	Moderado	Alto	Muy alto
Moderado	Bajo	Bajo	Moderado	Moderado	Alto
Bajo	Muy bajo	Bajo	Bajo	Moderado	Moderado
Muy bajo	Muy bajo	Muy bajo	Bajo	Bajo	Bajo

Identificador	**Activo**	**Probabilidad de iniciación**	**Probabilidad Impactos adversos**	**Probabilidad general**
A01	Servidor	Alto	Alto	Alto
A02	Computadores personales	Alto	Alto	Alto
A03	Computadores de soporte	Moderado	Moderado	Moderado

A04	Computador servidor	Alto	Alto	Alto
A05	Discos duros locales	Bajo	Bajo	Bajo
A06	Discos duros externos	Bajo	Bajo	Bajo
A07	Impresora monocromática	Bajo	Bajo	Bajo
A08	Router – Mikrotik	Moderado	Bajo	Bajo
A09	Switch – Cisco	Moderado	Bajo	Bajo
A10	UPS	Moderado	Bajo	Bajo
A11	Transceiver	Moderado	Bajo	Bajo
A12	NVR	Moderado	Bajo	Bajo
A13	PBX IP	Moderado	Bajo	Bajo
A14	Teléfonos IP	Bajo	Bajo	Bajo
A15	Biométrico	Alto	Alto	Alto
A16	Cámara IP, marca Hik – Vision	Bajo	Bajo	Bajo
A17	Generador eléctrico	Moderado	Moderado	Moderado
A18	Aire acondicionado	Moderado	Moderado	Moderado

Anexos NIST 800-30: Tarea 2.5

Determinar el Impacto

Objetivo: Determinar los impactos adversos de los eventos de amenaza de interés considerando: las características de las fuentes de amenaza que podrían iniciar los eventos, las vulnerabilidades identificadas y la susceptibilidad que refleja las salvaguardas planeadas o implementadas para impedir tales eventos.

Producto de entrada: Inventario de equipamiento de hardware.

Producto de salida: Consolidado del impacto en los activos de equipamiento de hardware.

Para el desarrollo de esta ficha se debe tener en cuenta las siguientes instrucciones:

- Para evaluar los activos se emplea la escala de valoración que se detalla a continuación:

Muy alto	Alto	Moderado	Bajo	Muy bajo
10 - 9	8-6	5 – 3	2 - 1	0

Identificador	**Activo**	**Impacto**
A01	Servidor	7
A02	Computadores personales	7
A03	Computadores de soporte	2
A04	Computador servidor	7
A05	Discos duros locales	3
A06	Discos duros externos	3
A07	Impresora monocromática	3
A08	Router – Mikrotik	2
A09	Switch – Cisco	2

A10	UPS	2
A11	Transceiver	2
A12	NVR	2
A13	PBX IP	2
A14	Teléfonos IP	2
A15	Biométrico	6
A16	Cámara IP, Hik – Vision	2
A17	Generador eléctrico	4
A18	Aire acondicionado	4

Anexos NIST 800-30: Tarea 2.6

Determinar el Riesgo

Objetivo: Determinar el riesgo que resulta de los cálculos entre la probabilidad de eventos de amenaza que resultan en impactos adversos más el resultado del impacto.

Producto de entrada: Tarea 2.4 y Tarea 2.5

Producto de salida: Consolidado del riesgo en los activos de equipamiento de hardware. Para el desarrollo de esta ficha se debe tener en cuenta las siguientes instrucciones:

- Para evaluar los activos se emplea la escala de valoración que se detalla a continuación:

Probabilidad que resulte en impacto	**Nivel de impacto**				
	Muy bajo	**Bajo**	**Moderado**	**Alto**	**Muy alto**
Muy alto	Muy bajo	Bajo	Moderado	Alto	Muy alto
Alto	Muy bajo	Bajo	Moderado	Alto	Muy alto
Moderado	Muy bajo	Bajo	Moderado	Moderado	Alto
Bajo	Muy bajo	Bajo	Bajo	Bajo	Moderado
Muy bajo	Muy bajo	Muy bajo	Muy bajo	Bajo	Bajo

Identificador	Activo	Probabilidad de resultar en impacto	Impacto	Riesgo
A01	Servidor	Alto	Alto	Alto
A02	Computadores personales	Alto	Alto	Alto
A03	Computadores de soporte	Moderado	Bajo	Bajo

A04	Computador servidor	Alto	Alto	Alto
A05	Discos duros locales	Bajo	Moderado	Bajo
A06	Discos duros externos	Bajo	Moderado	Bajo
A07	Impresora monocromática	Bajo	Moderado	Bajo
A08	Router – Mikrotik	Bajo	Bajo	Bajo
A09	Switch – Cisco	Bajo	Bajo	Bajo
A10	UPS	Bajo	Bajo	Bajo
A11	Transceiver	Bajo	Bajo	Bajo
A12	NVR	Bajo	Bajo	Bajo
A13	PBX IP	Bajo	Bajo	Bajo
A14	Teléfonos IP	Bajo	Bajo	Bajo
A15	Biométrico	Alto	Alto	Alto
A16	Cámara IP, marca Hik – Vision	Bajo	Bajo	Bajo
A17	Generador eléctrico	Moderado	Moderado	Moderado
A18	Aire acondicionado	Moderado	Moderado	Moderado

Anexos MAR.1.1
Caracterización de los Activos
MAR.1.1 Identificación de Activos

Objetivo: Identificar los activos que componen el sistema, determinando sus características, atributos y clasificación en los tipos determinados.

Producto de entrada: Inventario de equipamiento de hardware.

Producto de salida: Caracterización de los activos.

Técnicas, prácticas y pautas: Reuniones y entrevistas.

N°	Cantidad	Nombre	Descripción	Unidad Responsable	Personal responsable	Ubicación
1	1	Servidor	Servidor de base de datos	Área de TIC	Director de TIC	Centro de datos
			Servidor de aplicaciones			
			Servidor de antivirus – virtual			
			Servidor de archivos – Virtual			
2	5	Computadores	Computadores personales			Área de TIC
3	1		Computadores de soporte			Área de TIC
4	1		Computador servidor			Centro de datos

5	2	Almacenamiento de datos	Discos duros locales			Área de TIC
6	1		Discos duros externos			Área de TIC
7	1	Perifèricos de impresión	Impresora monocromática			Área de TIC
8	1		Router – Mikrotik			Centro de datos
9	3		Switch - Cisco			Centro de datos
10	3		UPS			Centro de datos
11	8	Soporte de red	Transceiver			Centro de datos
12	1		NVR	Área de TIC	Director de TIC	Centro de datos
13	1		PBX IP			Centro de datos
14	5	Central telefónica	Teléfonos IP			Área de TIC
15	1	Sistema de control de acceso	Biométrico			Área de TIC
16	1	Equipo de videovigilancia	Cámara IP, marca Hik – Vision			Área de TIC

17	1	Equipo eléctrico	Generador eléctrico	Área de TIC
18	1	Equipo de climatización	Aire acondicionado	Área de TIC

ANEXOS MAR. 1.3

Valoración de los Activos del Área de TIC de la Universidad Técnica Luis Vargas Torres de Esmeraldas

Objetivo: Identificar en qué dimensión es valioso cada activo.

Productos de entrada: Resultados de la tarea MAR.1.1, identificación de los activos.

Productos de salida: Informe de valor de los activos.

Técnicas, prácticas y pautas: Libro II –" Catálogo" y entrevistas.

Nombre: Leonardo Reyes

Título: Ingeniero en sistemas

Cargo: Director de TIC

Para la realización de esta actividad se debe valorar respecto a las siguientes dimensiones: Integridad (I), Confidencialidad (C), Autenticidad (A), Trazabilidad (T) y Disponibilidad (D). En la valoración de los activos se toma como referencia la escala de criterios definidos por la metodología MAGERIT, como se observa a continuación:

Escala	Valor	Criterio
10	Extremo	Daño extremadamente grave
8-9	Muy alto	Daño muy grave
6-7	Alto	Daño grave
3-5	Medio	Daño importante
1-2	Bajo	Daño menor

0	Despreciable	Irrelevante a efectos prácticos.

En la siguiente tabla, realizar la valoración de los activos de acuerdo a los criterios descritos anteriormente.

nº	Cantidad	Descripcion	Dimensiones				
			D	**I**	**C**	**A**	**T**
1	1	Servidor	7	7	7	7	7
2	5	Computadores personales	5	5	5	5	5
3	1	Computadores de soporte	3			1	3
4	1	Computador servidor	3	3	3	3	3
5	2	Discos duros locales	1	1	1		
6	1	Discos duros externos	1	1	1		
7	1	Impresora monocromática	1				
8	1	Router – Mikrotik	1				
9	3	Switch – Cisco	1				
10	3	UPS	1				
11	8	Transceiver	1				
12	1	NVR	1				
13	1	PBX IP	1				
14	5	Teléfonos IP	1				
15	1	Biométrico	3				
16	1	Cámara IP, marca Hik – Vision	1				

17	1	Generador eléctrico	3
18	1	Aire acondicionado	3

ANEXOS MAR. 2.0

Catálogo de Amenazas

Objetivo: Presentar un catálogo de amenazas posibles sobre los activos de un sistema de información.

Productos de entrada: Catálogo de amenazas.

Productos de salida: Informe de amenazas asociadas a los activos.

Técnicas, prácticas y pautas: Libro II, de MAGERIT v.3.

Amenazas	Tipo de amenazas
Desastres naturales	Fuego.
	Daños por el agua.
	Desastres naturales (fenómeno climático, de origen sísmico, volcánico, meteorológico, e inundación)
De origen industrial	Fuego.
	Daños por el agua.
	Desastres industriales.
	Contaminación medioambiental, mecánica y electromagnética.
	Avería de origen físico o lógico.
	Corte del suministro eléctrico.
	Condiciones inadecuadas de temperatura o humedad.
	Fallo de servicios de comunicaciones.
	Interrupción de otros servicios o suministros esenciales.
	Degradación de los soportes de almacenamiento de la información.
	Emanaciones electromagnéticas.
	Errores de los usuarios.

Errores y fallos no intencionados	Errores del administrador del sistema/ de la seguridad.
	Errores de monitorización, configuración y de secuencia.
	Deficiencias en la organización.
	Difusión de software dañino.
	Errores de re-encaminamiento.
	Fugas, alteración, y destrucción de la información.
	Vulnerabilidades de los programas.
	Errores de mantenimiento/ actualización de programas. (software).
	Errores de mantenimiento/ actualización de equipos. (hardware).
	Caída del sistema por agotamiento de recursos.
	Pérdida de equipos.
	Indisponibilidad del personal.
Ataques intencionados o deliberados	Manipulación de los registros de actividad y de los ficheros de configuración.
	Suplantación de la identidad.
	Abuso de privilegios de acceso.
	Uso no previsto.
	Difusión de software dañino.
	Re-encaminamiento de mensajes.
	Alteración de la secuencia.
	Análisis de tráfico.

	Repudio (negación de actuaciones).
	Intercepción de información (escucha).
	Modificación, destrucción y revelación de la información.
	Manipulación de programas.
	Manipulación del hardware.
	Denegación de servicio.
	Robo de equipos.
	Ataque destructivo.
	Ocupación enemiga.
	Indisponibilidad del personal.
	Extorsión.
	Ingeniería social.
	Distracción.
	Incumplimiento (leyes, normas, reglamentos, …)
	Inyección de código malicioso (a través de una frontera lógica).
	Extracción de información (a través de una frontera lógica).
	Acceso no autorizado (a través de una frontera lógica o del perímetro físico).
	Introducción y retirada de objetos (a través del perímetro físico).
	Destrucción del perímetro físico. Fuga de emanaciones.
Riesgos sobre la privacidad	No facilitar la información en materia de protección de datos o no redactarla de forma accesible y fácil de entender.

Tratar datos inadecuados y excesivos para la finalidad del tratamiento.

Carecer de una base jurídica sobre la que se sustenten los tratamientos realizados sobre los datos.

Tratar datos personales con una finalidad distinta para lo cual fueron recabados.

No disponer de una estructura organizativa, procesos y recursos para una adecuada gestión de la privacidad en la organización.

Almacenar los datos por periodos superiores a los necesarios para la finalidad del tratamiento y a la legislación vigente.

Realizar transferencias internacionales a países que no ofrezcan un nivel de protección adecuado.

No tramitar o dificultar el ejercicio de los derechos de los interesados.

Resolución indebida del ejercicio de derecho de los interesados en tiempo, formato y forma.

Seleccionar o mantener una relación con un encargado de tratamiento sin disponer de las garantías adecuadas.

Carecer de mecanismos de supervisión y control sobre las medidas que regulan la relación con un encargado.

No registrar la creación, modificación o cancelación de las actividades de tratamiento efectuadas bajo su responsabilidad.

No llevar a cabo por parte del responsable del tratamiento una evaluación de impacto adecuada en los supuestos detallados por la normativa aplicable.

Disociación deficiente o reversible que permita la re-identificación de datos.

Información no actualizada o incorrecta.

Deficiencias en los protocolos de almacenamiento de los datos personales en formato físico.

Obtener un consentimiento dudoso, viciado o inválido para el tratamiento o cesión de datos personales.

Accesos no autorizados a datos personales (modificación).

Accesos no autorizados a datos personales (lectura).

ANEXOS MAR. 2.1

Caracterización de las Amenazas

MAR.2.1 Identificación de las Amenazas

Objetivos: Identificar las amenazas relevantes sobre cada activo.

Productos de entrada: Resultados de la tarea MAR.2.0: catálogo de amenazas.

Productos de salida: Relación de amenazas posibles.

Técnicas, prácticas y pautas: Reuniones, catálogo de amenazas.

Las amenazas típicas que se pueden encontrar son: desastres naturales, de origen industrial, errores y fallos no intencionados, ataques deliberados y riesgos sobre la privacidad que se detalla el catálogo de amenazas de la actividad MAR.2.0.

De acuerdo al catálogo se procede a identificar por activo cada una de las posibles amenazas que pueden materializarse.

AMENAZA	TIPO DE AMENAZA	ACTIVO
Desastres naturales	Fuego.	Servidor
	Daños por el agua.	Computadores personales
	Desastres naturales	Computadores de soporte
De origen industrial	Fuego.	Computador servidor
	Daños por el agua.	Discos duros locales
	Desastres industriales.	Discos duros externos
	Contaminación medioambiental, y electromagnética.	Impresora monocromática
	Avería de origen físico o lógico.	Router - Mikrotik
	Corte del suministro eléctrico.	

	Condiciones inadecuadas de temperatura o humedad.	Switch - Cisco
	Emanaciones electromagnéticas.	UPS
Errores y fallos no intencionados	Errores de mantenimiento/ actualización de equipos. (hardware).	Transceiver
	Caída del sistema por agotamiento de recursos.	NVR
	Pérdida de equipos.	PBX IP
Ataques deliberados	Uso no previsto.	Teléfonos IP
	Acceso no autorizado.	Biométrico
	Repudio (negación de actuaciones).	Cámara IP, marca Hik – Vision
	Manipulación del hardware.	Generador eléctrico
	Denegación de servicio.	Aire acondicionado
	Robo de equipos.	
	Ataque destructivo.	

ANEXOS MAR. 2.2

MAR.2.2 – Valoración de las Amenazas

Objetivos: Estimar la frecuencia de ocurrencia de cada amenaza sobre cada activo.
Estimar la degradación que causaría la amenaza en cada dimensión del activo si llegara a materializarse.

Productos de entrada: Resultados de la tarea MAR.2.1 Identificación de amenazas.
Productos de salida: Informe de amenazas posibles, caracterizadas por su frecuencia de ocurrencia y la degradación que causarían en los activos.
Técnicas, prácticas y pautas: Reuniones.

ACTIVO	AMENAZAS	FRECUENCIA	DEGRADACIÓN EN DIMENSIONES				
			D	I	C	A	T
			100%	10%	50%		50%
	Fuego.	0,1	100%				
	Daños por el agua.	0,1	50%				
Servidor	Desastres naturales.	0,1	100%				
	Fuego.	0,5	100%				
	Daños por el agua.	0,5	50%				
	Desastres industriales.	0,5	100%				
Computadores personales	Contaminación medioambiental.	0,1	50%				
	Contaminación electromagnética.	1	10%				

	Avería de origen físico o lógico.	1	50%			
Computadores de soporte	Corte del suministro eléctrico.	1	100%			
	Condiciones inadecuadas de temperatura o humedad.	1	100%			
	Emanaciones electromagnéticas.	1		1%		
Computador servidor	Errores de mantenimiento/ actualización de equipos. (hardware).	1	10%			
	Caída del sistema por agotamiento de recursos.	10	50%			
Teléfonos IP	Pérdida de equipos.	5	5%		10%	
	Uso no previsto.	1	10%	1%	10%	
	Acceso no autorizado.	1	10%	10%	50%	
	Repudio (negación de actuaciones).	1				50%
	Manipulación del hardware.	0,5	50%		50%	
	Denegación de servicio.	2	100%			
	Robo de equipos.	5	5%		10%	
	Ataque destructivo.	1	100%			

ACTIVO	AMENAZAS	FRECUENCIA	DEGRADACIÓN EN DIMENSIONES				
			D	I	C	A	T
			100%	100%	100%		50%
Discos duros locales	Fuego.	0,1	100%				
	Daños por el agua.	0,1	50%				
	Desastres naturales.	0,1	100%				
	Fuego.	0,5	100%				
	Daños por el agua.	0,5	50%				
	Desastres industriales.	0,5	100%				
Discos duros externos	Contaminación medioambiental.	0,1	50%				
	Contaminación electromagnética.	1	10%				
	Avería de origen físico o lógico.	1	50%				
	Corte del suministro eléctrico.	1	100%				
	Condiciones inadecuadas de temperatura o humedad.	1	100%				
	Emanaciones electromagnéticas.	1			1%		
	Errores de mantenimiento/ actualización de equipos. (hardware).	1	10%	10%	50%		
	Caída del sistema por agotamiento de recursos.	10	50%				

	Pérdida de equipos.	1	100%		100%	
	Uso no previsto.	1	10%	100%	100%	
	Acceso no autorizado.	1	10%	10%	100%	
	Repudio (negación de actuaciones).	1	10%	100%	100%	
	Manipulación del hardware.	1				50%
	Denegación de servicio.	2	100%			
	Robo de equipos.	0,5	100%		100%	
	Ataque destructivo.	1	100%			

ACTIVO	AMENAZAS	FRECUENCIA	DEGRADACIÓN EN DIMENSIONES				
			D	I	C	A	T
			100%	10%	50%		50%
	Fuego.	0,1	100%				
	Daños por el agua.	0,1	50%				
Impresora	Desastres naturales.	0,1	100%				
	Fuego.	0,5	100%				
	Daños por el agua.	0,5	50%				
Router	Desastres industriales.	0,5	100%				

	Contaminación medioambiental.	0,1	50%			
Switch	Contaminación electromagnética.	1	10%			
	Avería de origen físico o lógico.	1	50%			
UPS	Corte del suministro eléctrico.	1	100%			
	Condiciones inadecuadas de temperatura o humedad.	1	100%			
Generador eléctrico	Emanaciones electromagnéticas.	1			1%	
	Errores de mantenimiento/ actualización de equipos. (hardware).	1	10%			
Aire acondicionado	Caída del sistema por agotamiento de recursos.	10	50%			
	Pérdida de equipos.	1	100%		50%	
	Uso no previsto	1	1%			
	Acceso no autorizado.	1	10%	10%	50%	
	Repudio (negación de actuaciones).	1				50%
	Manipulación del hardware.	0,5	50%		50%	
	Denegación de servicio.	2	100%			
	Robo de equipos.	0,5	100%		50%	

	Ataque destructivo.	1	100%					

ACTIVO	AMENAZAS	FRECUENCIA	DEGRADACIÓN EN DIMENSIONES				
			D	I	C	A	T
			100%	10%	100%		50%
	Fuego.	0,1	100%				
	Daños por el agua.	0,1	50%				
Transceiver	Desastres naturales.	0,1	100%				
	Fuego.	0,5	100%				
	Daños por el agua.	0,5	50%				
	Desastres industriales.	0,5	100%				
NVR	Contaminación medioambiental.	0,1	50%				
	Contaminación electromagnética.	1	10%				
	Avería de origen físico o lógico.	1	50%				
PBX IP	Corte del suministro eléctrico.	1	100%				
	Condiciones inadecuadas de temperatura o humedad.	1	100%				

Biométrico	Emanaciones electromagnéticas.	1			1%	
	Errores de mantenimiento/ actualización de equipos.	1	10%			
	Caída del sistema por agotamiento de recursos.	10	50%			
Cámara IP	Pérdida de equipos.	1	100%		100%	
	Uso no previsto.	1	1%	1%	10%	
	Acceso no autorizado.	1	10%	10%	50%	
	Repudio (negación de actuaciones).	1				50%
	Manipulación del hardware.	0,5	50%		50%	
	Denegación de servicio.	2	100%			
	Robo de equipos.	0,5	100%		100%	
	Ataque destructivo.	1	100%			

ANEXOS MAR. 3. 2

Mar.3 Caracterización de las Salvaguardas

Mar.3.2 – Identificación y Valoración de las Salvaguardas

Objetivos: Determinar la eficacia de las salvaguardas pertinentes.

Productos de entrada: Catálogo de salvaguardas

Productos de salida: Informe de salvaguardas desplegadas, caracterizadas por su grado de efectividad.

Técnicas, prácticas y pautas: Reuniones y entrevistas.

Nº	SALVAGUARDAS	Valoración
1	Protección de los equipos informáticos (HW).	L2
2	Protección a elementos auxiliares (HW).	L2
3	Protección física de los equipos.	L3
4	Gestión de incidentes.	L2
5	Herramientas de seguridad (HW).	L2
6	Registro y auditoria.	L2
7	Continuidad del negocio.	L2
8	Organización.	L2
9	Relaciones externas.	L2
10	Adquisición / desarrollo.	L2
11	Protección de emanaciones.	L2

Nº	Control de la Seguridad de la Información (ISO/IEC 27002: 2022)	Valoración
5	**Organización**	
5.1	Políticas para la seguridad de la información.	L2
5.2	Roles y responsabilidades en seguridad de la información.	L2
5.4	Responsabilidad de la dirección.	L2
5.5	Contacto con las autoridades.	L2
5.6	Contacto con grupos de interés especial.	L2
5.7	Inteligencia de amenazas.	L2 – L3
5.8	Seguridad de la información en la gestión de proyectos.	L2
5.9	Inventario de información y otros activos asociados.	L2
5.10	Uso aceptable de la información y activos asociados.	L2
5.11	Devolución de activos.	L2
5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información.	L2 – L3
5.25	Evaluación y decisión sobre los eventos de seguridad de la información.	L2
5.26	Respuesta a incidentes de seguridad de la información.	L2 – L3
5.27	Aprender de los incidentes de seguridad de la información.	L2 – L3
5.28	Recopilación de evidencias.	L2 – L3
5.29	Seguridad de la información durante la interrupción de incidentes.	L2 – L3
5.30	Preparación para las TIC para la continuidad del negocio.	L2 – L3

5.32	Derechos de propiedad intelectual.	L2
5.35	Revisión independiente de la seguridad de la información.	L2 – L3
5.36	Cumplimiento de las políticas y normas de seguridad de la información.	L2 – L3
5.37	Documentación de procedimientos operacionales.	L2
6	**Controles de Personas**	
6.8	Notificación de los eventos de seguridad de la información.	L2 – L3
7	**Controles Físicos**	
7.6	Trabajo en áreas seguras.	L2
7.7	Puesto de trabajo despejado y pantalla limpia.	L2 – L3
7.8	Emplazamiento y protección de equipos.	L2 – L3
7.9	Seguridad de los equipos fuera de las instalaciones.	L2 – L3
7.11	Instalaciones de suministro.	L2 – L3
7.13	Mantenimiento de los equipos.	L2 – L3
8	**Soportes de Almacenamiento**	
8.1	Dispositivos finales de usuario.	L2
8.6	Gestión de capacidades.	L2
8.14	Redundancia de los recursos de tratamiento de la información.	L2 – L3
8.24	Uso de la criptografía.	L2
8.27	Arquitectura segura de sistemas y principios de ingeniería.	L2
8.32	Gestión de cambios.	L2 – L3

8.34	Protección de los sistemas de información durante las pruebas de auditoría.	L2 – L3

Controles del NIST Cybersecurity Framework

Función	Categoría	Subcategoría	Valoración
Identificar	Gestión de activos	Los dispositivos y sistemas físicos dentro de la organización están inventariados.	L2
		Los sistemas de información externos están catalogados.	L3
		Los recursos (hardware, dispositivos, datos, tiempo, personal y software) se priorizan en función de su clasificación, criticidad y valor comercial.	L4
	Entorno empresarial	Se identifica y comunica la función de la organización en la cadena de suministro.	L4
		Se identifica y comunica el lugar de la organización en la infraestructura crítica y su sector industrial.	L4
		Se establecen y comunican las prioridades para la misión, los objetivos y las actividades de la organización.	L4
		Se establecen dependencias y funciones fundamentales para la prestación de servicios críticos.	L4
		Los requisitos de resiliencia para respaldar la entrega de servicios críticos se establecen para todos los estados operativos (bajo coacción/ataque, durante la recuperación, y operaciones normales).	L4
	Gobernanza	Se establece y se comunica la política de seguridad de la información organizacional.	L4

		Las funciones y responsabilidades de seguridad de la información están coordinadas y alineadas con roles internos y los socios externos.	L4
		Se comprenden y se gestionan los requisitos legales y regulatorios relacionados con la ciberseguridad, incluidas las obligaciones de privacidad y libertades civiles.	L4
	Evaluación de riesgos	Las vulnerabilidades de los activos se identifican y se documentan.	L4
		La inteligencia sobre amenazas cibernéticas se recibe de foros y fuentes de intercambio de información.	L4
		Se identifican y documentan las amenazas, tanto internas como externas.	L4
		Se identifican los posibles impactos y las probabilidades del negocio.	L4
		Se utilizan amenazas, vulnerabilidades, probabilidades e impactos para determinar el riesgo.	L4
		Se identifican y priorizan las respuestas a los riesgos.	L4
	Estrategia de gestión de riesgos	Los procesos de gestión de riesgos son establecidos, gestionados y acordados por las partes interesadas de la organización.	L4
		La tolerancia al riesgo organizacional se determinada y se expresa claramente.	L4
		La determinación de la tolerancia al riesgo por parte de la organización se basa en su papel en la infraestructura crítica y el análisis de riesgos específicos del sector.	L4
Riesgo	estrategia	Los procesos de gestión de riesgos de la cadena de suministro cibernético son identificados, establecidos, evaluados, gestionados y acordados por las partes interesadas de la organización.	L4
		Los procesos de gestión de riesgos de la cadena de suministro cibernético son identificados, establecidos,	L4

		evaluados, gestionados y acordados por las partes interesadas de la organización.	
		Los contratos con proveedores y socios externos se utilizan para implementar medidas apropiadas diseñadas para cumplir con los objetivos del programa de ciberseguridad de una organización y el plan de gestión de riesgos de la cadena de suministro cibernético.	L4
		La planificación y las pruebas de respuesta y recuperación se llevan a cabo con proveedores.	L4
		Los proveedores y socios externos son evaluados de forma rutinaria mediante auditorías, resultados de pruebas u otras formas de evaluaciones para confirmar que están cumpliendo con sus obligaciones contractuales.	L4
		La planificación y las pruebas de respuesta y recuperación se llevan a cabo con proveedores.	L4
PROTEGER	Control de acceso	Se gestiona y se protege el acceso físico a los activos.	L4
		Se gestiona el acceso remoto.	L4
		Se gestionan los permisos de acceso incorporando los principios de privilegio mínimo y separación de funciones.	L4
	Concienciación y formación	La integridad de la red se protegida (por ejemplo, segregación de la red, segmentación de la red).	L4
		Todos los usuarios están informados y capacitados.	L4
		Los usuarios privilegiados comprenden sus funciones y responsabilidades.	L4
		Los terceros interesados (por ejemplo, proveedores, clientes, socios) comprenden sus funciones y responsabilidades.	L4

	Los altos ejecutivos comprenden sus funciones y responsabilidades.	L4
	El personal de seguridad física y de ciberseguridad comprende sus funciones y responsabilidades.	L4
Seguridad de los datos	Los datos en reposo están protegidos.	L4
	Los datos en tránsito están protegidos.	L4
	Los activos se gestionan formalmente durante su eliminación, transferencias y disposición.	L4
	Se mantiene una capacidad adecuada para asegurar la disponibilidad.	L4
	Se implementan protecciones contra fugas de datos.	L4
	Los mecanismos de verificación de integridad se utilizan para verificar la integridad del software, el firmware y la información.	L4
	Los entornos de desarrollo y prueba están separados del entorno de producción.	L4
	Los mecanismos de verificación de integridad se utilizan para verificar la integridad del hardware.	L4
Procesos y procedimientos de protección de la información	Se crea y se mantiene una configuración básica de los sistemas de tecnología de la información/control industrial incorporando principios de seguridad (por ejemplo, concepto de funcionalidad mínima).	L4
	Se implementa el ciclo de vida del desarrollo del sistema para gestionar los sistemas.	L4
	Se encuentran establecidos procesos de cambio de configuración.	L4
	Se realizan, mantienen y prueban copias de seguridad de la información.	L4

		Se cumplen las políticas y regulaciones relativas al entorno físico operativo de los activos de la organización.	L4
		Los datos se eliminan según la política.	L4
	Mantenimiento	El mantenimiento y la reparación de los activos de la organización se realizan y se registran con herramientas aprobadas y controladas.	L4
		El mantenimiento remoto de los activos de la organización se aprueba, registra y realiza de manera que evite el acceso no autorizado.	L4
	Tecnología de protección	Los registros de auditoría/registro se determinan, documentan, implementan y revisan de acuerdo con la política.	L4
		Los medios extraíbles están protegidos y su uso restringido de acuerdo con la política.	L4
		Se incorpora el principio menor funcionalidad mediante la configuración de los sistemas para proporcionar solo las capacidades esenciales.	L4
		Las redes de comunicaciones y de control están protegidas.	L4
		Se implementan mecanismos (por ejemplo, a prueba de fallos, equilibrio de carga, cambio en caliente) para lograr los requisitos de resiliencia en situaciones normales y adversas.	L4
DETECTAR	Anomalías y eventos	Se establece y gestiona una línea base de referencia para operaciones de red y flujos de datos esperados para usuarios y sistemas.	L4
		Los eventos detectados se analizan para comprender los objetivos y métodos de los ataques.	L4

	Los datos de eventos se recopilan y correlacionan a partir de múltiples fuentes y sensores.	L4
	Se determina el impacto de los eventos.	L4
	Se establecen umbrales de alerta de incidentes.	L4
Monitoreo continuo de seguridad.	La red es monitoreada para detectar posibles eventos de ciberseguridad.	L4
	Se monitorea el entorno físico para detectar posibles eventos de ciberseguridad.	L4
	Se monitorea la actividad del personal para detectar posibles eventos de ciberseguridad.	L4
	Se detecta código malicioso.	L4
	Se detecta el código móvil no autorizado.	L4
	La actividad del proveedor de servicios externos se monitorea para detectar posibles eventos de ciberseguridad.	L4
	Se realiza el monitoreo de personal, conexiones, dispositivos y software no autorizados.	L4
	Se realizan análisis de vulnerabilidad.	L4
Proceso de detección	Las funciones y responsabilidades de la detección están bien definidas para asegurar la responsabilidad.	L4
	Las actividades de detección cumplen con todos los requisitos aplicables.	L4
	Se prueban los procesos de detección.	L4
	Se comunica la información de detección de eventos.	L4
	Los procesos de detección se mejoran continuamente.	L4

RESPONDER	Planificación de la respuesta	El plan de respuesta se ejecuta durante o después de un incidente.	L4
	Comunicaciones	El personal conoce sus funciones y el orden de las operaciones cuando se necesita una respuesta.	L4
		Los incidentes se reportan de acuerdo con los criterios establecidos.	L4
		La información se comparte de acuerdo con los planes de respuesta.	L4
		La coordinación con las partes interesadas ocurre de manera consistente con los planes de respuesta.	L4
		El intercambio voluntario de información se produce con partes interesadas externas para lograr una conciencia situacional de ciberseguridad más amplia.	L4
	Análisis	Se investigan las notificaciones de los sistemas de detección.	L4
		Se comprende el impacto del incidente.	L4
		Se realizan análisis forenses.	L4
		Los incidentes se clasifican de acuerdo con los planes de respuesta.	L4
		Se establecen procesos para recibir, analizar y responder a las vulnerabilidades reveladas a la organización desde fuentes internas y externas (pruebas internas, boletines de seguridad o investigadores de seguridad).	L4
	Mitigación	Los incidentes están contenidos.	L4
		Se mitigan las incidencias.	L4
		Las vulnerabilidades recientemente identificadas se mitigan o documentan como riesgos aceptados.	L4
	Mejoras	Los planes de respuesta incorporan lecciones aprendidas.	L4
		Se actualizan las estrategias de respuesta.	L4

RECUPERAR	Planificación de recuperación		El plan de recuperación se ejecuta durante o después de un incidente de ciberseguridad.	L4
	Mejoras		Los planes de recuperación incorporan las lecciones aprendidas.	L4
			Se actualizan las estrategias de recuperación.	L4
	Comunicaciones		Se gestionan las relaciones públicas.	L4
			La reputación se repara después de un incidente.	L4
			Las actividades de recuperación se comunican a las partes interesadas internas y externas, así como a los equipos ejecutivos y de gestión.	L4

REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

ACTA PARA ESTABLECER SALVAGUARDAS N° 01

Siendo las 19:00 pm del día lunes, 11 de septiembre del 2023, se reunieron vía plataforma virtual en Microsoft Teams, para la selección y evaluación de salvaguardas del proyecto de investigación titulado: Mitigación de riesgos de la seguridad en la infraestructura de hardware del área de TIC de la Universidad Técnica Luis Vargas Torres basado en la metodología MAGERIT v. 3 y NIST Cybersecurity Framework, con la finalidad de evaluar las salvaguardas más pertinentes y determinar su eficacia, conformada por las siguientes personas:

- Msc. Reyes Vélez Leonardo, Personal del DDTI.
- Ing. Quispe Mera Víctor, tesista.
- Msc. Cuzme Rodríguez Fabián, tutor de tesis.

Conforme al libro I, metodología de análisis y gestión de riesgos de los sistemas de información, en la versión 3.0, se hace referencia al paso tres de la metodología en los puntos de: selección de salvaguardas, efecto de las salvaguardas, tipo de protección y eficacia de la protección, para elegir aquellas que son más relevantes para los activos a proteger, que se detalla a continuación:

Convenciones utilizadas en los controles:

Efecto	Tipo
Preventivas: reducen la probabilidad	Preventivas (PR) Disuasoria (DR) Eliminatorias (EL) Minimizadoras (IM)
Acotan la degradación	Correctivas (CR) Recuperativas (RC) Monitorización (MN)
Consolidan el efecto de las demás	Detección (DC) Concienciación (AW) Administrativas (AD)

Factor	Nivel	Significado
0%	L0	Inexistente
	L1	Inicial
	L2	Reproducible
	L3	Proceso definido
	L4	Gestionado
100%	L5	Optimizado

Tabla de resumen:

Controles del NIST Cybersecurity Framework							
Activo	**Función**	**Categoría**	**Subcategoría**	**Control**	**Efecto de la salvaguarda**	**Tipo de protección a aplicarse**	**Posible eficacia de la protección**
Servidor	Proteger	Control de acceso	Se gestionan los permisos de acceso incorporando los principios de privilegio mínimo y separación de funciones.	Limitar y restringir el acceso mediante sistemas de identificación y métodos de verificación como tarjetas personales, y sistemas biométricos.	Reducen la probabilidad.	PR	L4
Computadores personales	Proteger	Seguridad de los datos	Se implementan protecciones contra fugas de datos.	Implementar hardware DLP (prevención de pérdida de datos) para supervisar la red y evitar que usuarios no autorizados copien o compartan información privada.	Acotan la degradación	IM	L4

Discos duros locales y externos	Proteger	Tecnología de protección	Los medios extraíbles estarán protegidos y su uso restringido de acuerdo con la política.	Control de registro de actividades mediante bitácoras que registre la fecha y el motivo de las personas que ingresan.	Consolidan el efecto de las demás	MN	L4
Biométrico	Proteger	Mantenimiento	El mantenimiento y la reparación de los activos de la organización se realizan y se registran con herramientas aprobadas y controladas.	Elaborar y ejecutar un plan actividades de mantenimiento preventivo y correctivo, además llevar un registro de incidentes.	Consolidan el efecto de las demás	AD	L4

Controles de la Seguridad de la Información (ISO/IEC 27001: 2022)

Activo	Dominio	Sección	Objetivo del control	Control	Efecto de la salvaguarda	Tipo de protección a aplicarse	Posible eficacia de la protección
Computadores de soporte, Router – Mikrotik , Switch – Cisco, UPS, Transceiver, NVR, PBX IP	Controles Físicos	7.13	Mantenimiento de los equipos.	Elaborar y ejecutar un plan actividades de mantenimiento preventivo y correctivo, además llevar un registro de incidentes.	Consolidan el efecto de las demás	AD	L2 – L3
Computador servidor	Controles Físicos	7.8	Emplazamiento y protección de equipos.	Implementar sistemas de prevención de intrusos (IPS).	Reducen la probabilidad.	PR	L2 – L3
Impresora monocromática	Organización	5.36	Cumplimiento de las políticas y normas de seguridad de la información.	Implementar políticas de seguridad de los dispositivos que pueden conectarse.	Reducen la probabilidad.	PR	L2 – L3
Teléfonos IP	Organización	5.37	Documentación de procedimientos operacionales.	Diseñar políticas del uso y acceso del hardware.	Reducen la probabilidad.	PR	L2

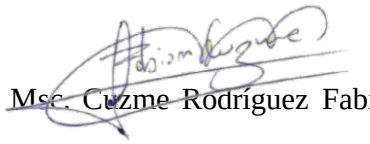
Cámara IP	Controles tecnológicos	8.9	Control de gestión de configuración.	Cambiar las contraseñas cada 90 días como mínimo e implementación del cifrado hash para el almacenamiento de contraseñas.	Reducen la probabilidad.	PR	L2 – L3
Generador eléctrico	Controles físicos	7.12	Seguridad del cableado.	Revisar las conexiones eléctricas, cables, contactos.	Acotan la degradación	IM	L2 – L3
Aire acondicionado	Controles tecnológicos	8.27	Arquitectura de sistemas seguros y principios de ingeniería.	Implementar sensores de monitoreo de temperatura y humedad.	Reducen la probabilidad.	PR	L2 – L3

Una vez finalizado con el análisis del riesgo en los activos de hardware e identificado las salvaguardas se procede a aplicar las medidas sugeridas iniciando el jueves 14 de septiembre del 2023 hasta el viernes 10 de noviembre del 2023, estos controles se deben aplicar para determinar el riesgo e impacto residual, obteniendo como resultados disminuir los riesgos presentes.

Para constancia de lo actuado, suscriben esta acta el Personal del DDTI, el tutor de tesis y el tesista, quienes certifican las salvaguardas seleccionadas.

Msc. Reyes Vélez Leonardo

Personal del DDTI



Msc. Cuzme Rodríguez Fabián

Tutor de Tesis

Ing. Quispe Mera Víctor

Tesista