LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades, Asunción, Paraguay
ISSN en línea: 2789-3855, 2026

Modelo de evaluación del riesgo informático aplicando las metodologías MAGERIT y NIST SP 800-30

Information risk assessment model base don MAGERIT and NIST SP 800-30

Víctor Eduardo Quispe Mera
victor.quispe.mera@utelvt.edu.ec
https://orcid.org/0000-0001-9010-4791
Universidad Técnica Luis Vargas Torres de Esmeraldas
Esmeraldas – Ecuador

Lenin Vicente Quispe Mera
lvquispem@utn.edu.ec
https://orcid.org/0009-0002-1251-3201
Universidad Técnica del Norte Ibarra
Esmeraldas – Ecuador

Galo Eduardo Maldonado Ibarra
galo.maldonado@utelvt.edu.ec
https://orcid.org/0000-0002-5309-5053
Universidad Técnica Luis Vargas Torres de Esmeraldas
Esmeraldas – Ecuador

Ingrid Magdalena Rodriguez Cevallos
ingridmagdalenarc@gmail.com
https://orcid.org/0009-0007-0302-3303
Universidad Técnica Luis Vargas Torres de Esmeraldas
Esmeraldas – Ecuador

DOI: https://doi.org/10.56712/latam.v7i2.5781

Artículo recibido: 27 de diciembre de 2025.
Aceptado para publicación: 30 de abril de 2026.
Conflictos de Interés: Ninguno que declarar.

Redilat
Red de Investigadores Latinoamericanos

LATAM
Revista Latinoamericana de Ciencias Sociales y Humanidades

VOLUMEN VII

DOI: https://doi.org/10.56712/latam.v7i2.5781

Modelo de evaluación del riesgo informático aplicando las metodologías MAGERIT y NIST SP 800-30

Information risk assessment model base don MAGERIT and NIST SP 800-30

Víctor Eduardo Quispe Mera[1]
victor.quispe.mera@utelvt.edu.ec
https://orcid.org/0000-0001-9010-4791
Universidad Técnica Luis Vargas Torres de Esmeraldas
Esmeraldas – Ecuador

Lenin Vicente Quispe Mera
lvquispem@utn.edu.ec
https://orcid.org/0009-0002-1251-3201
Universidad Técnica del Norte Ibarra
Esmeraldas – Ecuador

Galo Eduardo Maldonado Ibarra
galo.maldonado@utelvt.edu.ec
https://orcid.org/0000-0002-5309-5053
Universidad Técnica Luis Vargas Torres de Esmeraldas
Esmeraldas – Ecuador

Ingrid Magdalena Rodriguez Cevallos
ingridmagdalenarc@gmail.com
https://orcid.org/0009-0007-0302-3303
Universidad Técnica Luis Vargas Torres de Esmeraldas
Esmeraldas – Ecuador

Artículo recibido: 27 de diciembre de 2025. Aceptado para publicación: 30 de abril de 2026.
Conflictos de Interés: Ninguno que declarar.

Resumen

Los avances tecnológicos han mejorado los procesos institucionales; sin embargo, también han incrementado la exposición a riesgos de seguridad de la información. Cuando no existen medidas de seguridad adecuadas, las instituciones se vuelven más vulnerables a diversas amenazas. En este contexto, se realizó una evaluación de riesgos de seguridad de la información en la infraestructura de hardware del área de Tecnologías de la Información y la Comunicación de la Universidad Técnica Luis Vargas Torres de Esmeraldas, mediante la aplicación de las metodologías MAGERIT versión 3 y NIST SP 800-30. Para la evaluación se utilizó la herramienta Pilar, la cual soporta las cuatro fases del método MAGERIT: caracterización de los activos, identificación de amenazas, análisis de salvaguardas y estimación del estado del riesgo. De forma complementaria, la metodología NIST SP 800-30 orientó las etapas de preparación de la evaluación, realizar la evaluación que incluyó cinco actividades y comunicación de resultados. La evaluación identificó riesgos asociados a la infraestructura y permitió determinar los niveles de riesgo presentes en los activos tecnológicos. Con base en estos resultados, se estableció la necesidad de implementar un plan de tratamiento que reduzca los riesgos a niveles aceptables mediante la aplicación de salvaguardas y controles alineados con la norma ISO/IEC 27001:2022.

Palabras clave: amenazas, riesgos, salvaguardas, vulnerabilidades

[1] Autor de correspondencia.

Abstract

Technological advances have improved institutional processes; however, they have also increased exposure to information security risks. When adequate security measures are not implemented, institutions become more vulnerable to various threats. In this context, an information security risk assessment was conducted on the hardware infrastructure of the Information and Communication Technologies (ICT) department at the Universidad Técnica Luis Vargas Torres de Esmeraldas by applying the MAGERIT version 3 and NIST SP 800-30 methodologies. The assessment used the Pilar tool, which supports the four phases of the MAGERIT method: asset characterization, threat identification, safeguard analysis, and risk state estimation. In addition, the NIST SP 800-30 methodology guided the stages of assessment preparation, risk assessment execution —which included five activities— and communication of results. The evaluation identified risks associated with the infrastructure and determined the risk levels present in technological assets. Based on these results, the need to implement a risk treatment plan was established in order to reduce risks to acceptable levels through the application of safeguards and controls aligned with the ISO/IEC 27001:2022 standard.

Keywords: threats, risks, safeguards, vulnerabilities

Cómo citar: Quispe Mera, V. E., Quispe Mera, L. V., Maldonado Ibarra, G. E., & Rodriguez Cevallos, I. M. (2026). Modelo de evaluación del riesgo informático aplicando las metodologías MAGERIT y NIST SP 800-30. *LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades 7 (2), 1991 – 2004. https://doi.org/10.56712/latam.v7i2.5781*

INTRODUCCIÓN

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).

Los riesgos informáticos son amenazas y vulnerabilidades que afectan en todos los aspectos a la empresa, y las consecuencias pueden ser muy graves en relación a la información que se está manejando (Helmer & Laura, 2019).

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. Algunos ejemplos de estas amenazas pueden ser: virus informáticos, robo o alteración de información, uso no autorizado de los sistemas, espionajes y ciberataques (Suárez, Andrade, Obando, & Gómez, 2017).

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 (Arellano, 2022).

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).

En consecuencia, por todos estos posibles eventos de amenazas, es esencial que las empresas y los individuos tomen medidas para proteger sus datos y minimizar su impacto en caso de materializarse (Cruz, Delgado, & Ponce, 2022).

Cabe destacar que, 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 (Ministerio de Hacienda y Administraciones Públicas, 2012).

Ante esta problemática surge la necesidad de evaluar el nivel de riesgo informático en la Universidad Técnica Luis Vargas Torres de Esmeraldas mediante metodologías especializadas de análisis de riesgos. Por ello, es vital para su supervivencia y desarrollo sostenible, contar con una adecuada gestión de riesgos con un enfoque integral, holístico y global, que le permita administrar de manera adecuada la exposición a los riesgos, minimizar las posibles pérdidas que se puedan efectuar en caso de que se lleguen a presentar amenazas, ya sean aceptarlas, mitigarlas, transferirlas y en ocasiones poder evitarlas (Reina, 2022).

Es por ello que, el análisis de riesgo para las universidades, les permitirá tener una visión más clara sobre su estado de seguridad actual y brindar mecanismos para reducir las vulnerabilidades de los sistemas de información ya que estos son accesibles mediante diferentes mecanismos incluyendo la utilización de las redes WLAN que consultan información de procesos académicos. Para esto es necesario realizar un proceso de análisis de las amenazas y el impacto para todos los activos (Aristizabal, 2021).

Por consiguiente, en esta investigación se emplea la metodología MAGERIT v.3 y NIST SP 800-30. Conforme con MAGERIT (2012), esta metodología persigue lo siguiente; 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 (Sanchez & Calispa, 2021).

Mientras que la metodología 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 de TI (Tecnología de la Información), proporciona una guía para la seguridad de las infraestructuras de la misma desde una perspectiva técnica (Macías, 2018).

Por otro lado, la seguridad de la información es un alto factor de riesgo de ataques, por eso al aplicar metodologías de análisis de riesgos, es indispensable implementar medidas eficaces como; por ejemplo, el cumplimiento de las normativas, entre ellas se encuentran la familia ISO. Los estándares ISO/IEC son desarrollados por organizaciones internacionales, gubernamentales y no gubernamentales, así como por miembros de ISO (la Organización Internacional de Estandarización) e IEC (la Comisión Electrotécnica Internacional). Este proyecto está enfocado en el estándar ISO/IEC 27001:2022, como herramienta de apoyo para la definición de normas de gestión de la seguridad de la información (Hernández, 2022).

METODOLOGÍA

Enfoque de investigación: La investigación se desarrolló bajo un enfoque cualitativo, ya que permitió analizar la información obtenida mediante la interacción directa con el personal del área de Tecnologías de la Información y la Comunicación (TIC) y comprender las condiciones relacionadas con la gestión de riesgos en la infraestructura tecnológica de la institución.

Diseño del estudio: El estudio se desarrolló con un diseño descriptivo de carácter aplicado. Para su desarrollo se emplearon tres modalidades de investigación: documental, de campo y aplicada. La investigación documental permitió estudiar trabajos de investigación de otros autores, libros digitales, artículos web, sitios web, 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.

La investigación de campo permitió la recolección de datos directamente desde personal del área de Tecnologías de la Información y la Comunicación. Donde, el objetivo primario en la investigación aplicada se centró en apoyar la resolución de problemas prácticos o de acción, que colabora en la toma de decisiones (Baudean, 2015).

Los participantes estuvieron conformados por personal del área de Tecnologías de la Información y la Comunicación (TIC) de la institución, seleccionados mediante un muestreo intencional debido a su participación directa en la administración, mantenimiento y gestión de los activos tecnológicos. Para la recolección de información se utilizaron entrevistas estructuradas y no estructuradas, así como una encuesta compuesta por 19 preguntas orientadas a identificar los activos tecnológicos, las amenazas potenciales y las medidas de seguridad implementadas.

Además, se aplicó la observación directa con el fin de identificar las características de la infraestructura tecnológica y complementar la información obtenida.

El proceso de recolección de datos se realizó mediante la aplicación de entrevistas y encuestas a seis personas del área de TIC, lo que permitió recopilar información relacionada con los activos tecnológicos, los posibles escenarios de amenaza y las salvaguardas existentes. La observación directa permitió verificar y ampliar la información proporcionada por los participantes.

Posteriormente, la información recopilada fue organizada y categorizada a partir de los datos obtenidos mediante las entrevistas, encuestas y observación. Con base en estos datos se aplicaron los procedimientos establecidos en las metodologías MAGERIT versión 3 y NIST SP 800-30 para identificar activos, amenazas, vulnerabilidades y salvaguardas, así como estimar los niveles de riesgo presentes en la infraestructura tecnológica analizada. Durante el desarrollo de la investigación se garantiza la confidencialidad de la información proporcionada por los participantes, y los datos recopilados fueron utilizados exclusivamente con fines académicos y de investigación.

Análisis de datos

En las siguientes secciones se describe el procedimiento aplicado en cada metodología, detallando sus fases, actividades y criterios utilizados para la identificación de activos, amenazas, vulnerabilidades y salvaguardas, así como para la estimación de los niveles de riesgo.

Metodología MAGERIT

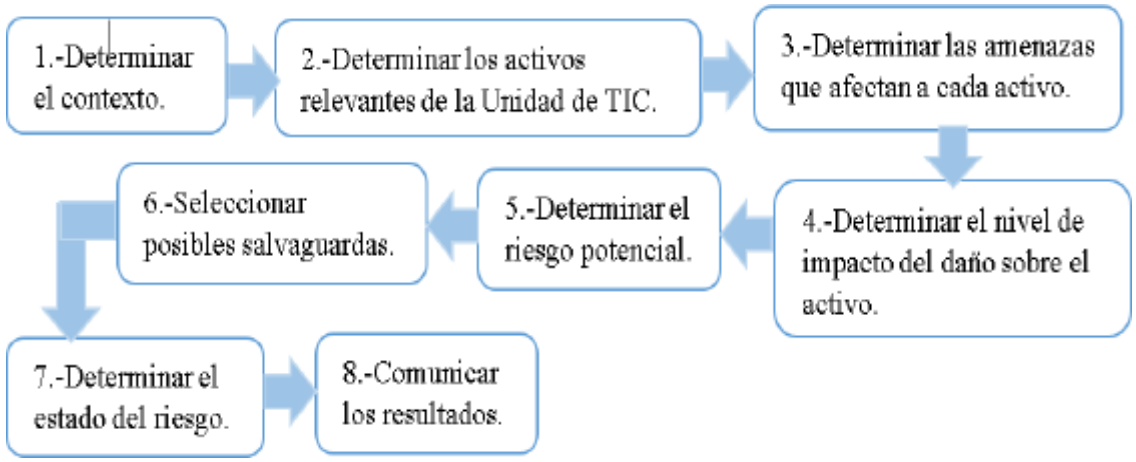
MAGERIT, son las siglas de Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, su fin es informar de los riesgos y de la necesidad de gestionarlos a los responsables de la actividad, así como ayudar a encontrar y planificar un plan adecuado para tratarlos (Iván, 2019).

Es una de las metodologías más utilizadas en el ámbito empresarial ya que les permite prepararse para procesos de auditorías, certificaciones y acreditaciones (Tejena, 2018). La herramienta PILAR (Procedimiento Informático-Lógico para el Análisis de Riesgos) está destinada al análisis y gestión de riesgos de una organización. Al estar basada en MAGERIT, hereda particularidades de la metodología (Ángel, 2019).

Para la realización de esta metodología de análisis y gestión de riesgos se utilizó la herramienta Pilar versión 2023.1.1. En esta sección se explica el procedimiento de la metodología MAGERIT v.3 que se utilizó para el análisis y gestión de riesgos, a continuación, en la siguiente figura 1 se detallan los pasos llevados a cabo.

Figura 1

Proceso de la metodología MAGERIT v.3



Nota: *El* proceso de análisis de riesgos consta de ocho fases, adaptado de MAGERIT versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (https://pilar.ccn-cert.cni.es/docman/documentos/1-magerit-v3-libro-i-metodo/file).

Paso 1 – Determinar el contexto: Esta actividad consistió en el levantamiento de la información inicial, es decir, se definió el alcance y límites para la investigación.

Paso 2 – Determinar los activos relevantes de la Unidad de TIC: Para la realización de esta actividad se contó con la información de los activos de hardware con los que dispone el departamento y se realizó una valoración que determina el valor en cuanto a disponibilidad, integridad, confidencialidad, y trazabilidad sobre cada activo.

Paso 3 – Determinar las amenazas que afectan a cada activo: Se considera una amenaza los ataques informáticos que puedan darse y ocasionar daños a los equipos tecnológicos, sistemas de información y todo el medio que comprometen la seguridad de la información (Quizhpi Cazho, 2022). Se realizó una valoración de las amenazas y la frecuencia de ocurrencia de cada amenaza por activo en las siguientes dimensiones: disponibilidad, integridad, confidencialidad, y trazabilidad.

Paso 4 – Determinar el nivel de impacto del daño sobre el activo: Una vez analizado los resultados de la valoración de los activos, su frecuencia y degradación que causan las amenazas, se obtuvo el impacto potencial, la degradación, en este proceso se analizó el impacto potencial acumulado y el impacto potencial repercutido.

Paso 5 – Determinar el riesgo potencial: El riesgo es la combinación de probabilidad de ocurrencia y el impacto potencial que podría causar una amenaza (Hacknoid, 2020). Cuando se ha identificado el impacto sobre las amenazas de los activos se calculó el riesgo potencial acumulado y riesgo potencial repercutido.

Paso 6 – Seleccionar posibles salvaguardas: Las 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 (Martín & Mateo, 2015).

Para seleccionar salvaguardas, de acuerdo al MAGERIT v.3, se tomó en cuenta los siguientes aspectos: tipos de activos a proteger, dimensiones de seguridad, amenazas, si hay salvaguardas alternativas.

Paso 7 – Determinar el estado del riesgo: Se realizó una estimación del impacto residual y riesgo residual. Una vez aplicadas las salvaguardas que propone la herramienta Pilar se evaluó su nivel de eficacia, calculando el impacto residual donde se obtuvo un nivel de impacto medio.

El riesgo residual es el resultado obtenido después de la implementación de los controles. Sin embargo, algunos riesgos se pueden mitigar y otros solo minimizar por su complejidad, los cuales requieren tener un monitoreo permanente (Marín & CampoverdeMolina, 2021).

Paso 8 – Comunicar los resultados: Se explicó en forma clara sobre los procedimientos llevados a cabo y sobre los resultados obtenidos al personal del área de TIC.

Metodología NIST SP 800-30

Es una guía que la protección de la información de las organizaciones lleva un proceso lógico y analítico para cumplir con el análisis y evaluación de amenazas, la selección de salvaguardas para la mitigación de riesgos y el desarrollo y puesta a prueba de planes de contingencia (Intriago, 2022). Además, ofrece un modelo de riesgo que ayuda a definir los factores de riesgo que deben ser evaluados y qué relaciones existen entre esos factores (Guerrero, 2021).

En el proceso de evaluación se destacan las siguientes tareas específicas que se llevó a cabo, que son: prepararse para la evaluación, realizar la evaluación y comunicar los resultados, por último, mantener la evaluación de riesgos.

Paso 1 – Prepárese para la evaluación: Se identificó el propósito y el alcance de los activos y las fuentes de información.

Paso 2 – Realice la evaluación: Esta actividad incluyó las siguientes tareas específicas: donde se identificó las fuentes de amenazas relevantes, los eventos de amenazas que producen esas fuentes y las vulnerabilidades que están expuestas por fuentes de amenazas, la probabilidad, el impacto adverso y el riesgo.

Paso 3 – Comunicar los resultados: Se explicó en forma clara sobre los procedimientos llevados a cabo y sobre los resultados obtenidos al personal del área de TIC.

Paso 4 – Mantener la evaluación: Esta actividad consistió en realizar un seguimiento continuo de los factores de riesgo que contribuyen a los cambios en el riesgo para la unidad de TIC. Para la realización de este procedimiento del análisisy gestión de riesgos se utilizó las tablas de los apéndices, desde la página 65 hasta la página 89 propuestas en la metodología NIST SP 800-30, donde se presentaron resultados.

Objetivos

Objetivo General

- Evaluar 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.

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.

Preguntas de la Investigación

- ¿Cuál es el nivel de riesgo en la infraestructura de hardware del área de TIC de la Universidad Técnica Luis Vargas Torres de Esmeraldas utilizando las metodologías MAGERIT v.3 y NIST Cybersecurity Framework?
- ¿Qué medidas de protección pueden implementarse para reducir los riesgos de seguridad de la información en el área de TIC de la universidad?

RESULTADOS

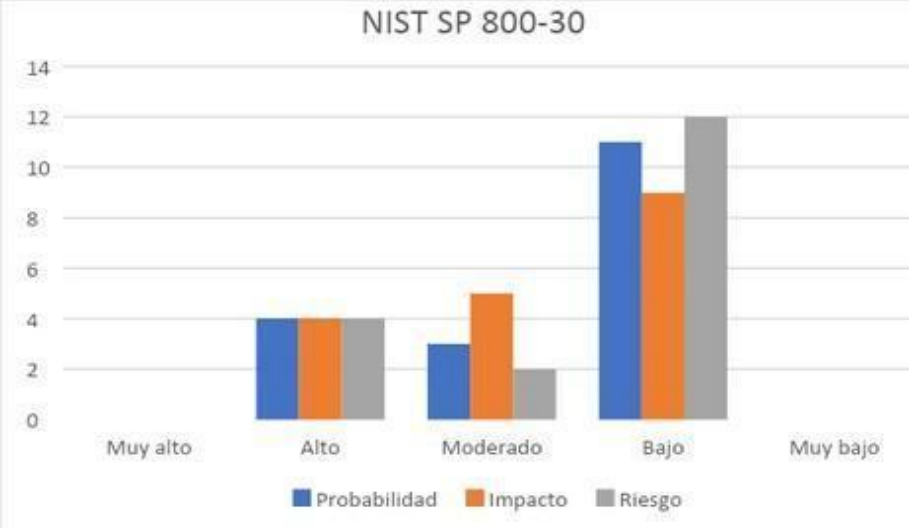
A continuación, se visualizan los resultados obtenidos de ambas metodologías:

Metodología NIST 800 – 30

En la figura 2, 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.

Gráfico 1

Resultados del proceso de gestión de riesgos de la NIST

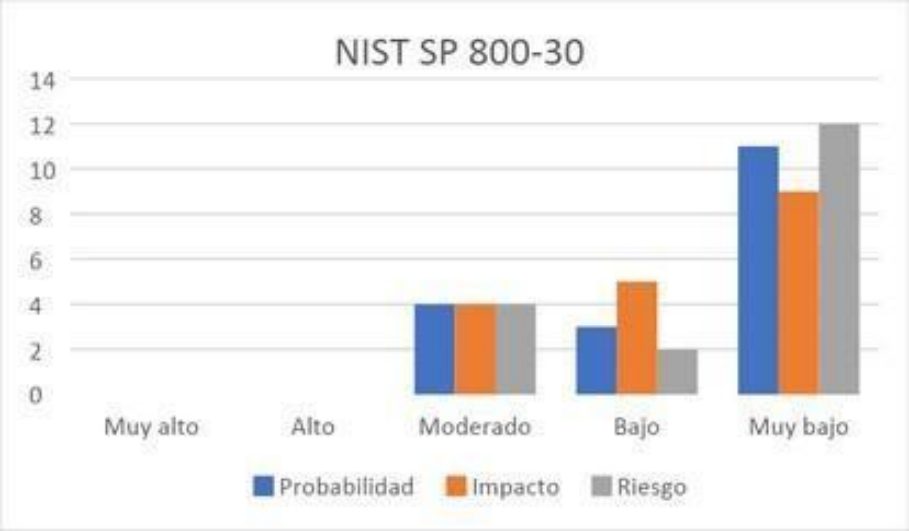


Fuente: elaboración propia.

Una vez implementadas las medidas de mitigación, se puede determinar que los niveles de probabilidad, impacto y riesgo han disminuido, como se muestra en el siguiente gráfico:

Gráfico 2

Resultados de NIST al aplicar las medidas de protección



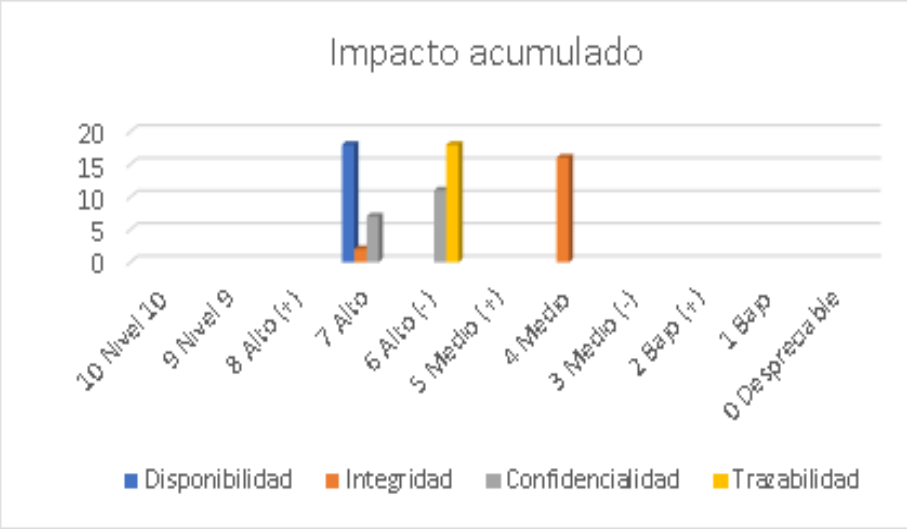
Fuente: elaboración propia.

Metodología MAGERIT

En este apartado, se muestran los resultados de: impacto acumulado, y el riesgo acumulado. En el gráfico 3, en el impacto acumulado y la figura 5 se refleja el impacto una vez aplicadas las salvaguardas.

Gráfico 3

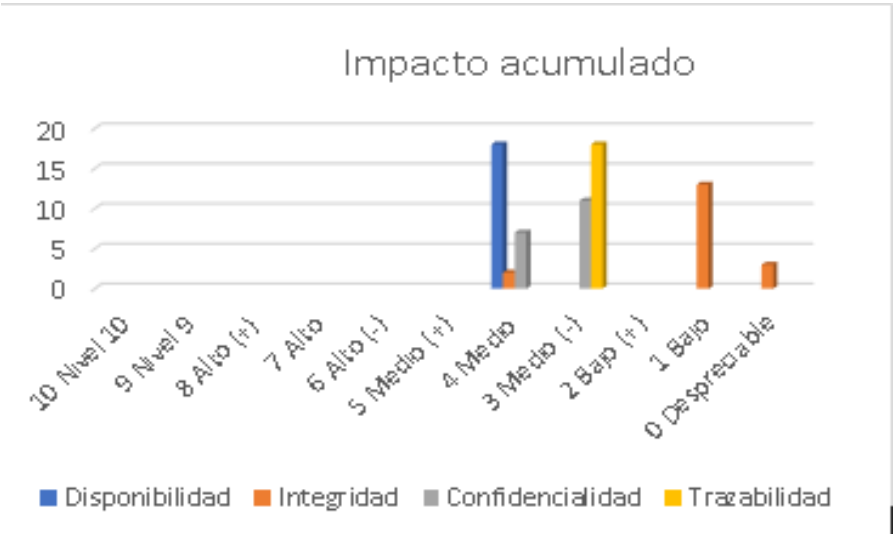
Resultados del impacto acumulado



Fuente: elaboración propia.

Gráfico 4

Impacto acumulado con salvaguardas

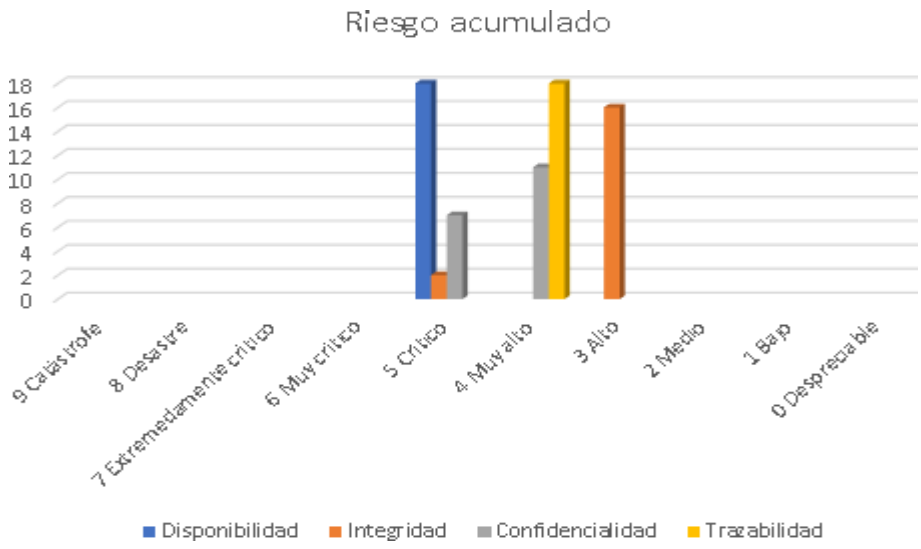


Fuente: elaboración propia.

En el gráfico 5, en el riesgo acumulado se obtuvo lo siguientes valores:

Gráfico 5

Resultados del riesgo acumulado

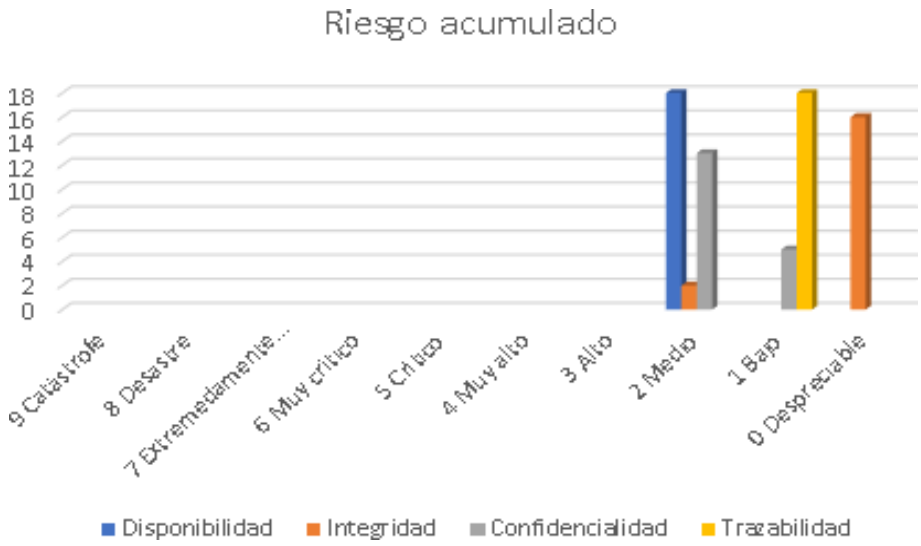


Fuente: elaboración propia.

Al aplicar las medidas sugeridas de mitigación se puede determinar que el nivel de riesgo acumulado ha disminuido, como se refleja en el gráfico 6.

Gráfico 6

Resultados del riesgo acumulado con salvaguardas



Fuente: elaboración propia.

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 (Avila Torres & Tapia, 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 (Felix, 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 de 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 Teresa, realizó una propuesta de un modelo híbrido basado en la metodología MAGERIT e ISO 27001 donde incluye controles para contrarrestar las amenazas (Jacqueline, 2022). 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 (Adrián, 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

La investigación permitió identificar los principales riesgos de seguridad presentes en los equipos informáticos del área de TIC de la Universidad Técnica Luis Vargas Torres de Esmeraldas, evidenciando

diversas amenazas y vulnerabilidades que pueden afectar el funcionamiento de la infraestructura tecnológica. Estos resultados resaltan la importancia de implementar procesos sistemáticos de identificación y gestión de riesgos para fortalecer la seguridad de la información institucional.

Mediante la aplicación de la metodología MAGERIT v.3, apoyada en la herramienta PILAR, se determinó el nivel de impacto, riesgo y frecuencia de las amenazas que afectan a los activos tecnológicos, lo que permitió obtener una visión clara del estado de seguridad de la infraestructura informática y la necesidad de mantener procesos permanentes de seguimiento y evaluación por parte del personal del área de TIC.

A partir de este análisis, se establecieron medidas de protección orientadas a reducir los niveles de riesgo a valores aceptables, mediante la selección de salvaguardas basadas en los lineamientos de ISO/IEC 27001:2022 y el NIST Cybersecurity Framework, contribuyendo a fortalecer la gestión de la seguridad de la información y la protección de los activos tecnológicos.

Finalmente, la evaluación de las medidas implementadas evidenció que la vulnerabilidad del hardware puede comprometer la disponibilidad, integridad y continuidad de los servicios tecnológicos institucionales, por lo que la aplicación sistemática de metodologías de análisis de riesgos y estándares de seguridad resulta fundamental para mejorar la gestión de la ciberseguridad en el entorno universitario.

REFERENCIAS

3.0 Metodología y Análisis y Gestión de Riesgos de los Sistemas de Información. Obtenido de Magerit - versión 3.0 Metodología y Análisis y Gestión de Riesgos de los Sistemas de Información: https://pilar.ccn-cert.cni.es/docman/documentos/1- magerit-v3-libro-i-metodo/file

Adrián, C. 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/handle/123456789/50402

Ángel, M. O. (8 de Octubre de 2019). Estudio de herramientas de análisis y gestión de riesgos y propuesta de mejora de la herramienta Pilar. Obtenido de Estudio de herramientas de análisis y gestión de riesgos y propuesta de mejora de la herramienta Pilar: https://uvadoc.uva.es/handle/10324/41310

Arellano, D. A. (29 de Julio de 2022). Estrategias de prevención frente a los ciberataques en la Unidad Educativa Fiscal Luis Alfredo Noboa Icaza. Obtenido de Estrategias de prevención frente a los ciberataques en la Unidad Educativa Fiscal Luis Alfredo Noboa Icaza: https://dspace.ups.edu.ec/bitstream/123456789/24173/1/UPS- GT004223.pdf

Aristizabal, A. O. (2021). Análisis de riesgos basados en la norma Magerit v3 de la red WLAN de las intituciones de educación superior del Tolima. Obtenido de Análisis de riesgos basados en la norma Magerit v3 de la red WLAN de las intituciones de educación superior del Tolima: https://repository.unad.edu.co/jspui/bitstream/10596/41960/3/aortizari.pdf

Avila Torres, A., & Tapia, J. C. (2021). Análisis y evaluación de riesgos: aplicado a EMAPAL-EP, basado en la metodología de MAGERIT versión 3.0. Dominio de las Ciencias, 14.

Baudean, M. (18 de Julio de 2015). Introducción a la investigación aplicada. Obtenido de https://marcosbaudean.net/wp-content/uploads/2015/11/MBS_Introduccion-a-la- investigacion-aplicada.pdf

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

Cruz, G., Delgado, L., & Ponce, B. (2022). Riesgos de seguridad de los datos en la web. Journal TechInnovation, 7.

Felix, B. B. (Junio de 2023). Guía de gestión de seguridad de la información para el Gobierno Provincial de Tungurahua. Obtenido de Guía de gestión de seguridad de la información para el Gobierno Provincial de Tungurahua: https://repositorio.puce.edu.ec/items/c9d11f7b-3d52-48da-8720-f36d7c029124

Guerrero, J. V. (Febrero de 2021). Análisis de seguridad de la información aplicando la metodología IST SP 800-30 Y NIST SP 800-115 para la empresa textiles JHONATEX. Obtenido de https://repositorio.uta.edu.ec/server/api/core/bitstreams/3aca72d1-299a- 4add-a856-eef2272f4f6d/content Hacknoid. (Abril de 2020). Cómo gestionar los riesgos informáticos de forma eficiente. Obtenido de https://hacknoid.com/wp-content/uploads/2020/04/GestionRiesgosTI-Hacknoid-Ebook.pdf

Helmer, M., & Laura, Z. (2019). Riesgos informáticos y alternativas para la seguridad informática en sistemas contables en Colombia. Venezolana de Gerencia, 13.

Hernández, E. S. (25 de Mayo de 2022). Plan de Implementación de la norma ISO/IEC 27001. Obtenido de https://openaccess.uoc.edu/bitstream/10609/145849/11/esanchezhernTFM0622mem oria.pdf

Intriago, J. Y. (Junio de 2022). Aplicación del NIST CYBERSECURITY FRAMEWORK en el Instituto Superior Tecnológico Sucre. Obtenido de Aplicación del NIST CYBERSECURITY FRAMEWORK en el Instituto Superior Tecnológico Sucre.

Iván, S. B. (Julio de 2019). Análisis de MAGERIT y PILAR. Obtenido de https://uvadoc.uva.es/bitstream/handle/10324/37736/TFG-I-1213.pdf?sequence=1

Jacqueline, C. M. (12 de Octubre de 2022). Propuesta de un modelo híbrido basado en las metodologías Magerit E ISO 27001 para controlar amenazas internas identificadas en la intranet de la Facultad de Informática y Electrónica. Obtenido de Propuesta de un modelo híbrido basado en las metodologías Magerit E ISO 27001 para controlar amenazas internas identificadas en la intranet de la Facultad de Informática y Electrónica.: http://dspace.espoch.edu.ec/handle/123456789/17706

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://rua.ua.es/dspace/bitstream/10045/93271/1/Analisis_y_correlacion_entre_probabilidad_e_impacto_de_l_Santonja_Lillo_Juan.pdf

Macías, M. A. (2018). Análisis de riesgos en seguridad de la información. Polo del conocimiento, 15.

Marín, C. P., & CampoverdeMolina, M. (2021). Análisis de riesgos del departamento de Tecnologías de la Información y Comunicación del Registro de la Propiedad de la ciudad de Cuenca, Ecuador. Polo del conocimiento, 18.

Martín, A. J., & Mateo, E. V. (2015). Selección de salvaguardas en gestión del riesgo en sistemas de la información: un enfoque borroso. Obtenido de https://oa.upm.es/40919/1/INVE_MEM_2015_223957.pdf

Ministerio de Hacienda y Administraciones Públicas. (Octubre de 2012). Magerit - versión

Quizhpi Cazho, L. M. (2022). Riesgos que afectan la disponibilidad de servicio en los proveedores de internet en los cantones Cañar, El Tambo y Suscal. Pro Sciences: Revista De Producción, Ciencias E Investigación, 14.

Reina, J. O. (2022). El impacto de la gestión integral de riesgo en el contexto actual. South Florida Journal of Developmen, 18.

Sanchez, F. P., & Calispa, N. I. (Marzo de 2021). Propuesta de un plan de contingencia para salvaguardar los activos de información en el departamento de Tecnología de la Información y Comunicación. Obtenido de Propuesta de un plan de contingencia para salvaguardar los activos de información en el departamento de Tecnología de la Información y Comunicación: https://dspace.ups.edu.ec/bitstream/123456789/19865/1/UPS%20-%20TTS276.pdf

Suárez, J. A., Andrade, R. F., Obando, C. C., & Gómez, a. A. (2017). La seguridad informática y la seguridad de la información. Polo del conocimiento, 11.

Tejena, M. M. (2018). Análisis de riesgos en seguridad de la información. Polo del conocimiento, 15.