UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR

POSGRADOS

MAESTRÍA EN
SEGURIDAD DE LA INFORMACIÓN
RPC-SO-28-NO.669-2021

OPCIÓN DE TITULACIÓN:
PROYECTO DE TITULACIÓN CON COMPONENTES DE INVESTIGACIÓN APLICADA Y/O DE DESARROLLO

TEMA:
ANÁLISIS COMPARATIVO DE METODOLOGÍAS DE ANÁLISIS DE RIESGOS (MAGERIT VS. NIST SP 800-30)

AUTORES:
STEVEN XAVIER ROMO SAÑICELA
MIRIAM ILIANA VÁSQUEZ CASTRO

DIRECTOR:
RODOLFO XAVIER BOJORQUE CHASI

CUENCA – ECUADOR
2023

Autores:

Steven Xavier Romo Sañicela
Ingeniero de Sistemas.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
sromo@est.ups.edu.ec

Miriam Iliana Vásquez Castro
Ingeniero de Sistemas.
Candidata a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
mvasquezcas@est.ups.edu.ec

Dirigido por:

Rodolfo Xavier Bojorque Chasi
Ingeniero de Sistemas.
PhD. Ciencias de la Computación.
rbojorque@ups.edu.ec

DEDICATORIA

"Le dedicamos los resultados de este trabajo a Dios, a nuestras familias y verdaderos amigos que de algún u otro modo colaboraron en la realización de este trabajo y supieron apoyarnos en este camino de aprendizaje y conocimiento profesional, tenido gran confianza en nosotros y en este proyecto.

Pero principalmente lo dedicamos a nuestros padres que con sus consejos de perseverancia nos aconsejan para culminar la maestría y la presentación de este trabajo, esperando ver a sus hijos seguir creciendo en lo personal y profesional.

Estoy muy seguro de que lo que se ha llevado a cabo será de gran beneficio para todos.

Dios, Patria y Libertad".

Steven Xavier Romo Sañicela

"Dedico los resultados de este trabajo principalmente a Dios por haberme dado la vida y permitir haber llegado hasta este momento tan importante de mi formación profesional.

A mis padres, abuelita, hermana, mi novio Edgar y mi Margarita por demostrarme siempre apoyo y acompañarme en este proceso.

¡Muchas gracias por todo!"

Mirian Iliana Vásquez Castro

AGRADECIMIENTO

"Agradezco en primer lugar a Dios por darnos salud y habernos ayudado maravillosamente en cada paso de esta investigación, a mis padres por apoyarme siempre, a mi abuelita por ser quien siempre me inspirar a seguir avanzando ante situaciones difíciles inclusive, a nuestro tutor por su dedicación, paciencia y guía para supervisar este trabajo de investigación, a la Universidad Politécnica Salesiana del Ecuador por permitirnos ser los primeros maestrantes en cursar la maestría, a mi colega y amigo Steven y todos mis compañeros, director y docentes de la maestría Seguridad de la Información los cuales trasmitieron su experiencias y conocimiento necesario para poder estar aquí."

Miriam Iliana Vásquez Castro

"Quiero agradecer en primer lugar a Dios por guiarme y fortalecerme espiritualmente para empezar un camino lleno de éxito y llegar hasta este momento, a mi familia y amigos incondicionales, a mis padres las personas más importantes en mi vida quienes me han apoyado en todo momento con paciencia y comprensión en este proyecto.

A nuestro tutor que con paciencia y dedicación supo guiarnos en la realización de este trabajo y a la Universidad Politécnica Salesiana y a su grupo de docentes de la maestría por compartir su conocimiento, experiencias y darnos la oportunidad de seguir creciendo profesionalmente"

Steven Xavier Romo Sañicela

Tabla de Contenido

Análisis Comparativo de metodologías de análisis de riesgos (Magerit vs. NIST SP 800-30)

Autor(es):

Steven Xavier Romo Sañicela
Mirian Iliana Vásquez Castro

Resumen

En la actualidad la adopción de Tecnologías de Información y Comunicación (TIC), representan una necesidad con un factor de riesgo inherente, las organizaciones cada vez requieren conocer más sobre la mitigación de estos y como contar con planes de contingencias y control para evitarlos. El objetivo principal de este documento es analizar y comparar las metodologías de análisis de riesgos, Magerit y NIST SP 800-30 estableciendo criterios entre las metodologías la cual guíen a una elección empresarial. En este análisis se aplicó un enfoque cuantitativo donde se analizaron las metodologías de análisis de riesgos, descriptivo porque el objetivo de la investigación consiste en analizar las metodologías y estándares, dando como resultado un análisis con criterio para un marco de tomas de decisiones. Los métodos proporcionan una guía detallada para el análisis de riesgo, sin embargo, Magerit determina estos análisis de manera distinta que NIST y viceversa. Concluyendo que tanto Magerit como NIST SP 800-30 son metodologías aplicables en cualquier organización que requiera minimizar riesgos dentro de un sistema de información y siguen los tres pasos generales que incluyen la identificación de amenazas, vulnerabilidades y determinación de riesgo.

Palabras clave: Magerit, NIST, Sistemas de información, riesgos, amenazas, activos, metodología.

ABSTRACT

Currently, the adoption of Information and Communication Technologies (TIC) represents a necessity with an inherent risk factor, organizations increasingly need to know more about mitigating these and how to have contingency and control plans to avoid them. The main objective of this document is to analyze and compare the risk analysis methodologies, Magerit and NIST SP 800-30, establishing criteria between the methodologies which guide a business choice. In this analysis, there is a qualitative approach where the risk analysis methodologies analyzed, descriptive because the objective of the research is to analyze the methodologies and standards, resulting in an analysis with criteria for a decision-making framework. The methods provide detailed guidance for risk analysis, however, Magerit determines these analyzes differently than NIST and vice versa.

Concluding that both Magerit and NIST SP 800-30 are methodologies applicable in any organization that requires minimizing risks within an information system and follow the three general steps that include the identification of threats, vulnerabilities, and risk determination.

Keywords: Magerit, NIST, information system, risks, threats, assets, methodolgy.

1. Introducción

Hoy en día las compañías a nivel global se enfocan en cuidar y manejar sus más valiosos activos, el principal que incluye la información y posterior o de apoyo que incluyen Software, Hardware, redes, usuarios e infraestructura, Con el uso de internet a nivel mundial a aumentado los ataques a los sistemas informáticos lo que ha llevado a las empresas a buscar planes o estrategias que permitan mitigar los riesgos de ataque que son asociados a la vulnerabilidad de la información.

(Muñoz Mata & Institute of Electrical and Electronics Engineers, s. d.)(Muñoz Mata & Institute of Electrical and Electronics Engineers, s. d.)(Muñoz Mata & Institute of Electrical and Electronics Engineers, s. d.)En la actualidad la adopción de Tecnologías de Información y Comunicación (TIC), así como la implantación de Sistemas de Información (SI), representan una necesidad con un factor de riesgo crítico inherente para la aplicación de sistemas de las organizaciones (Muñoz Mata & Institute of Electrical and Electronics Engineers, s. d.).

La sociedad de la información depende cada vez más de un Sistema de Gestión de la Seguridad de la Información (SGSI) y del conocimiento de los riesgos de seguridad asociados al valor de sus activos (Santos Olmo Parra et al., 2016).

Si la organización quiere estimar el riesgo de un incidente de seguridad de TI, el daño financiero se debe considerar como una métrica en el análisis de riesgo (Aditya Putra Fatri et al., 2017).

Para hablar de análisis de riesgo debemos definir principalmente que es el riesgo, el cual se define como una probabilidad que ocurra un evento y el que pueda ser evitado y previsto, las vulnerabilidades y amenazas no llegan a presentar daños en grandes magnitudes si se presentan por separadas, pero si se mezcla con la probabilidad de daño el riesgo es mayor. El análisis de riesgos se convierte en el inicio y pieza clave dentro de la implementación de un SGSI. Su resultado final es la elaboración de la declaración de aplicabilidad (SOA - Statement of Applicability), sin

embargo, las decisiones más difíciles a nivel empresarial es seleccionar la metodología que mejor se adapte a la organización, ya que los recursos (económicos, humanos, tiempo) son limitados y por ello no podemos asegurar todo el ciclo de vida de los sistemas de información, por lo que solo podemos manejar los más amenazados y cuyo impacto sea alto para la organización.

Pero ¿Por qué se debe realizar un análisis comparativo de metodologías de análisis de riesgos? Hay muchos métodos que han sido desarrollados por muchas organizaciones para análisis de riesgos. En este análisis comparativo elegimos dos de ellas y las compararemos, lo que no implica que los dos métodos sean mejores que otras metodologías existentes. Los métodos de evaluación de riesgos que analizaremos son Magerit y NIST SP 800-30 y han sido seleccionadas por su alta difusión a nivel internacional. El objetivo principal del análisis es comparar estas metodologías de riesgos y establecer criterios que guíen una selección empresarial entre las metodologías de análisis de riesgos Magerit y NIST SP 800-30.

La intención de nuestro proyecto de investigación es proporcionar un marco de toma de decisiones entre las metodologías más reconocidas (Magerit vs. NIST SP 800-30) que permita que el Sistema de Gestión de Seguridad de la Información de la organización tenga un mecanismo definido de gestión del riesgo, para ello es necesario que las organizaciones comprendan que deben saber evaluar cualitativa y cuantitativamente su nivel de madurez de seguridad, para ello se parte de una evaluación inicial que se conoce como el Gap Analysis o "Análisis de Brecha" y en función de este análisis se mide el riesgo para determinar la declaración de aplicabilidad.

2. Determinación del Problema

Los análisis de riesgos son técnicas que permiten administrar y evaluar de mejor forma las exposiciones al riesgo en un sistema de información, mitigando la pérdida

de información ante imprevistos que pueden ser predecibles con respecto a su probabilidad de ocurrencia.

Estándares como ISO/IEC 27001 y 27002 no definen pasos detallados de evaluación de riesgos, por lo que, si queremos usar dichos estándares, debemos definir nuestro propio método de evaluación de seguridad o usar métodos desarrollados por otras organizaciones (Syalim et al., 2009).

Aplicar una metodología de análisis de riesgos exitoso proporciona información de valor referente a los riesgos y amenazas que puedan afectar los planes estratégicos y de crecimiento organizacional, esto a través de procesos de análisis, evaluación e información sobre las posibles vulnerabilidades que surgen de los mismos, así como la reacción y enfoque de la empresa ante dichos riesgos.

Hay muchos métodos que han sido desarrollados por muchas organizaciones para el análisis de riesgos, en esté análisis comparativo elegimos dos de ellas, Magerit y NIST SP 800-30. Las cuales son herramientas de uso a gran escala y en el que emitiremos un análisis crítico basado en sus métodos para realizar los análisis de riesgos y el contenido de dichos métodos con documentación complementaria que ellos proporcionan para el uso de estas metodologías.

3. Marco Teórico Referencial

3.1 Gestión de Riesgo

Al hablar de gestión de riesgos debemos primero definir que es el riesgo, que es la probabilidad que una amenaza se convierta en un desastre. Las vulnerabilidades y las amenazas por separado no representan un daño proporcional, pero si se mezclan representan un daño sustancial. El desarrollo del riesgo informático se encuentra a la par de la tecnología y cada día las amenazas y vulnerabilidades acechan más la información(Hurtado, s. d.). La inversión de tiempo, esfuerzo y dedicación en la seguridad de la información dentro de una organización son piezas claves para contar con una buena gestión de riesgos, la organización que entienda

el valor sustancial de sus activos y desee realizar una inversión para gestionar sus vulnerabilidades debe inclinarse hacia sistemas de gestión basados en políticas, procesos, recursos, estructura de organización y documentación, todo esto permiten planificar, desarrollar, controlar y tomar acciones pertinentes que suelen acogerse a la normas ISO 27005. Si bien se requiere implementar una gestión para el riesgo en una organización se debe tener claro que no solo es para asegurar los activos de información, si no más bien procura que la misma cumpla con su misión, por lo que hablar de gestión se puede definir como un ciclo reiterativo donde se identifica, evalúa y ejecuta.

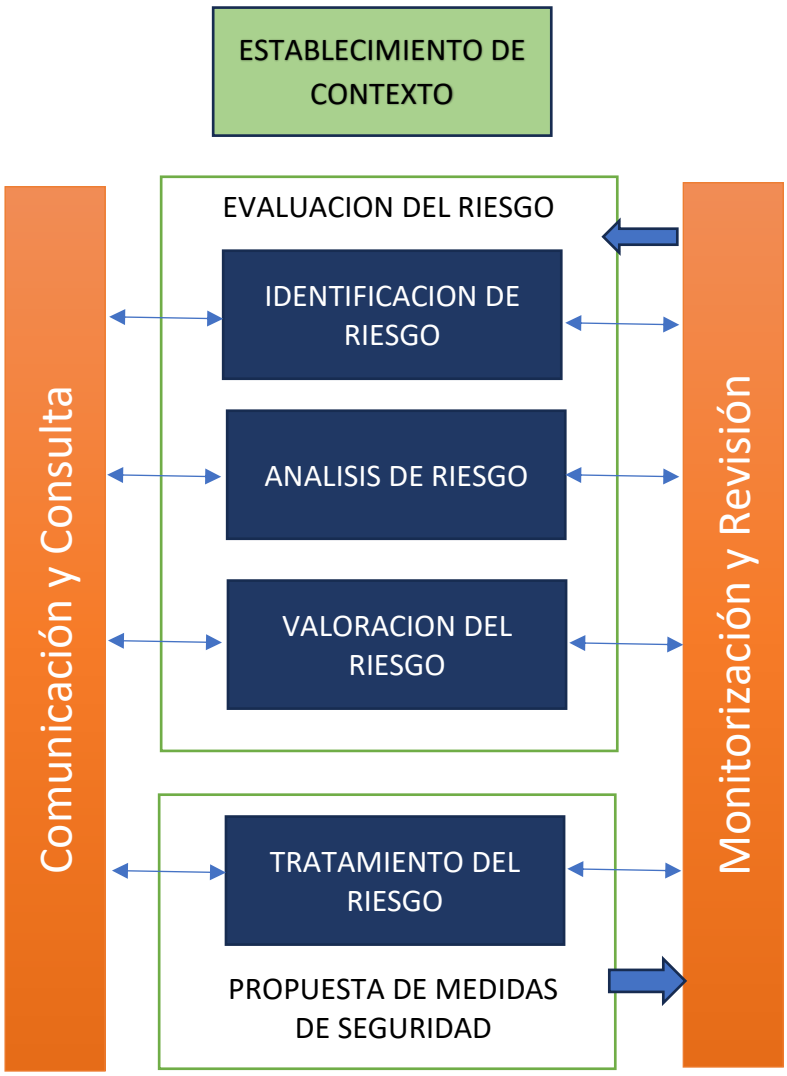
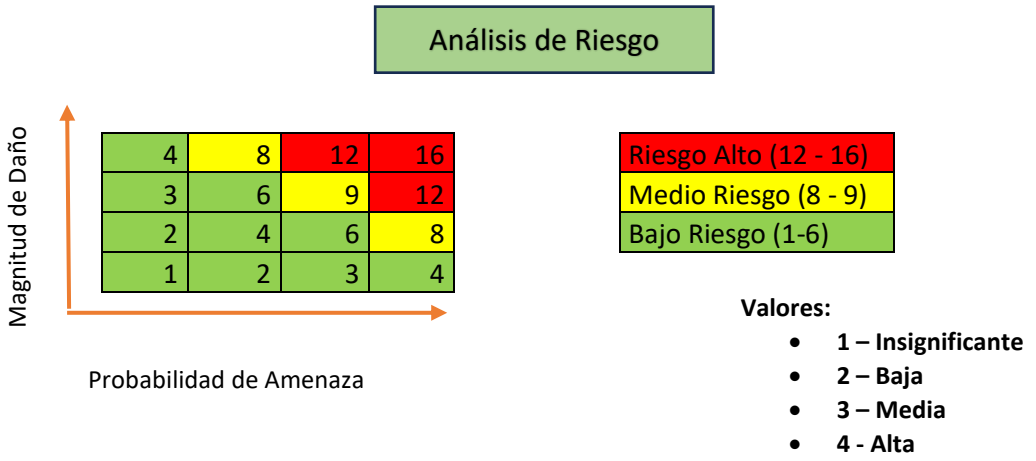


Fig 1 *Proceso de Gestión de Riesgos. Fuente: El autor*



Riesgo = Probabilidad de Amenaza * Magnitud de daño.

Fig 2 *Análisis de Riesgo. Fuente: El autor.*

El proceso de gestión de riesgo se ve en la Fig 1, y se encuentra conformado de 5 fases:

1. **Establecimiento de Contexto:**

   En este proceso se contextualiza el entorno recibiendo la información más importante del mismo.

2. **Evaluación del Riesgo:**

   Este proceso contiene tres subprocesos, la identificación, control y revisión y control de riesgos.

   En este método se identifica de forma cuantitativa y cualitativa los riesgos dándole una cierta prioridad a los criterios de evaluación que están alineados a los objetivos de la organización. De esta manera controla y determina lo que seria una pérdida de gran magnitud y en donde puedan ocurrir. Y por ultimo el proceso de evaluación compara los niveles de criterio del riesgo y los de aceptación, su resultado genera un listado de vulnerabilidades y amenazas priorizadas, todo esto finalizando con una interpretación llamada matriz de análisis. En esta se determina la probabilidad de amenaza contra la magnitud de

daño tomando valores desde el 1 hasta el 4, o en casos de calificación serian bajo, moderado, importante y critico contra las consecuencias Fig 2.

3. **Tratamiento de Riesgos:**

   En este proceso se plantea las medidas de seguridad reduciendo o evitando riesgos generando contingencias.

4. **Consulta de Riesgos:**

   Este proceso detalla los riesgos existentes a las partes interesadas de la organización.

5. **Monitoreo del Riesgo:**

   En este procede se supervisa todas las medidas de seguridad determinadas para mitigar los riesgos, con el objetivo de determinar si esta funcionando correctamente o está ejecutando la acción para la cual fue contemplada.

La evaluación de riesgos es un paso en el proceso de gestión de riesgos. El principal problema en la evaluación de riesgos es cómo evaluar todos los riesgos en un sistema u organización para que, al usar el resultado de la evaluación de riesgos, estos sistemas u organizaciones puedan definir controles apropiados para mitigar esos riesgos (Aditya Putra Fatri et al., 2017). Determinando su probabilidad de ocurrencia, impacto y mitigar el riesgo.

La evaluación de riesgos es una evaluación o descripción cuantitativa que permite al administrador priorizar la coincidencia de riesgos con la gravedad u otros criterios especificados. El método para evaluar los riesgos generalmente se compone de los siguientes cuatro identificadores:

1. **Identificadores de Amenazas**

   La identificación de amenazas nos permite identificar las amenazas potenciales dentro de un sistema de información y así desarrollar una lista de posibles amenazas.

2. **Identificadores de Vulnerabilidades**

   Este paso nos permite desarrollar un listado de posibles fuentes de amenazas que pueden ser comprometidas en el sistema de información.

3. **Determinación de riesgos**

En este paso evaluamos el nivel de riesgo potencial de un sistema de información determinando las amenazas y vulnerabilidades.

4. **Recomendación de control**

El propósito de este paso es proporcionar los controles que pueden minimizar o eliminar los riesgos ya identificados en los identificadores anteriores, reduciendo los niveles de riesgos que el sistema de información pueda sufrir.

Estos cuatro pasos de la evaluación de riesgos se basan en experiencias prácticas en la evaluación de la seguridad. Estos pasos provienen de las mejores prácticas que han aplicado muchas organizaciones para la evaluación de la seguridad.

Existen metodologías que permiten el uso adecuado de un análisis de riesgo el cual nos permita asegurar los sistemas de información en las organizaciones, entre los principales podemos indicar: OCTAVE, MEHARI, MAGERIT, CRAMM, NIST SP 800:30.

Estas no son las únicas metodologías que existen, pero se las hemos considerado como las principales para este estudio.

Magerit, es una metodología de análisis de riesgos para los sistemas de información la cual fue creada por el Consejo Superior de Administración Electrónica de España con el propósito de minimizar los riesgos en la implementación de tecnologías de la información.

NIST SP 800-30, es una guía de gestión de riesgos para los sistemas de información y tecnología la cual proporciona normas y estándares publicada por el Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos de América.

Según el reporte de la Agencia Europea de Ciberseguridad(Lambrinoudakis et al., s. d.) señala la popularidad de estas metodologías, pero destaca el uso de otras como OCTAVE ALLEGRO que sigue el enfoque OCTAVE y también es una metodología de evaluación de riesgos autodirigida. OCTAVE Allegro está diseñado para permitir una evaluación amplia del entorno de riesgo operativo de una organización, con el objetivo de producir resultados sólidos sin la necesidad de un

conocimiento extenso de la evaluación de riesgos. Se diferencia de los enfoques OCTAVE anteriores (OCTAVE y OCTAVE-S) al centrarse en los activos de información

en el contexto de cómo se utilizan, dónde se almacenan, transportan y procesan, y cómo se exponen a amenazas, vulnerabilidades e interrupciones. MEHARI que fue desarrollado MEHARI fue desarrollado y actualizado desde 1996 por CLUSIF y CLUSIQ y se distribuye gratuitamente bajo una licencia Creative Commons. MEHARI cumple con las directrices establecidas por la norma ISO 27005:2011 e ISO 31000, y permite la perfecta integración del riesgo en un proceso de desarrollo de SGSI ISO 27001. MEHARI está disponible de forma gratuita. Incluye un proceso de identificación de riesgos, basado en la identificación y evaluación de activos, un proceso de evaluación de riesgos guiado por un directorio de amenazas y respalda la gestión de riesgos al proporcionar un catálogo de medidas de seguridad. Mehari 2010 se ha actualizado y actualmente está disponible como Mehari Expert, habiendo sido revisado para cumplir con las actualizaciones de ISO/IEC 27005:2011, ISO 2700,1 e ISO 27002 2013. Actualmente hay tres variantes de las bases de conocimientos de Mehari disponibles en francés: Mehari Expert para organizaciones medianas y muy grandes, Mehari Standard para organizaciones pequeñas, medianas y grandes y Mehari Pro para entidades muy pequeñas. La base de conocimientos de Mehari Expert también se ha traducido al inglés.

3.2 MAGERIT

Magerit es una metodología de análisis y gestión de riesgos promovido por el Consejo Superior de Administración Electrónica (CSAE). Es de carácter público diseñada para satisfacer la gestión de la seguridad considerando las dependencias de las tecnologías de la información para lograr sus objetivos en el servicio. (coordinación de contenidos et al., s. d.)

Fue creada en el año 1997 y actualmente se encuentra en su segunda versión, los parámetros con los que trabaja esta metodología basan en términos como:

A. Activos
B. Amenazas
C. Vulnerabilidades

D. Impacto

E. Riesgos

F. Contingencia

El análisis de riesgo de Magerit determina el riesgo siguiendo los siguientes pasos:

1. **Determina los activos relevantes para la organización, su interrelación con su valor, es decir, que costo supondría su degradación.**

   Los activos son el recurso principal de un sistema de información y son los necesarios para que el sistema u organización funcionen correctamente y cumplan los objetivos propuestos.

   Los sistemas de información tienen dos activos importantes que son:

   - La información que maneja
   - Los servicios que presta

   Se pueden identificar otros activos relevantes que pueden ser:

   - Las aplicaciones o software informático que manejan los datos.
   - Los equipos informáticos o hardware que es donde se almacenan datos, aplicaciones y servicios.
   - Las redes de comunicación que intercambia los datos
   - Las instalaciones donde se interconectas los equipos de informática.
   - Personas que manejan los equipos informáticos y de red.
   - Soportes de información y auxiliares que complementan los equipos informáticos y de almacenamiento.

2. **Determina que amenazas están expuestos dichos activos**

   Las amenazas a nuestros sistemas de información son cosas que pueden suceder y causar daños a los activos. Las amenazas pueden ser por, desastres naturales (terremotos, inundaciones, etc.), de origen industrial (contaminación, fallos eléctricos, etc.) y por causas humanas las cuales se dividen en forma errores accidental o ataques deliberados.

3. **Determina la salvaguardia están disponibles y que tan eficiente son contra el riesgo**

Las salvaguardias son mecanismos tecnológicos que nos permiten reducir o mermar el riesgo contra una amenaza. Algunas amenazas pueden eliminarse mediante algún mecanismo adecuado y otros requieren de dispositivos técnicos como software, equipos, seguridad física y políticas de usuarios.

4. **Estima el impacto, definido como el daño al activo derivado de la ocurrencia de la amenaza**

   La estimación del impacto es la medida del daño sobre el activo que presente la aparición de la amenaza, conociendo el valor de los activos y el daño que es causado por la amenaza se deriva el impacto que tendrá sobre el sistema de información.

5. **Estima el riesgo definido como el impacto ponderado sobre la tasa de ocurrencia o expectativa de aparición de la amenaza**

   La estimación del riesgo es la medida del daño probable sobre el sistema de información, una vez conociendo el impacto de la amenaza se deriva el riesgo teniendo en cuenta la probabilidad de la ocurrencia.

   El riesgo aumenta con el impacto y la frecuencia.

3.3 NIST SP 800-30

NIST es un estándar desarrollado por el Instituto Nacional de Estándares y tecnología (NIST) que fue desarrollado para la evaluación de riesgos de un sistema de información, proporcionado una guía de fundamentos para la administración y mitigación de riesgos

La metodología NIST SP 800-30 está compuesta por nueve pasos los cuales permiten establecer los alcances y limites operacionales de la evaluación de riesgos de un sistema de información. (Tejena-Macías, 2018). Y los cuales son:

1. **Caracterización del sistema**

   Esta fase nos permite identificar el alcance de nuestro sistema de información en base a la evaluación de riesgos, así mismo determina los

límites de operación en la evaluación de riesgos proporcionado información de hardware, software, comunicación del sistema, responsables y personal de soporte para definir el riesgo.

2. **Identificación de Amenazas**

   Se identifica las probabilidades de las amenazas que atenten contra nuestro sistema de información, para esto es recomendable revisar historial de ataques, fuentes de vulnerabilidades y controles existentes.

3. **Identificación de Vulnerabilidades**

   En esta fase se detalla una lista de debilidades que podrían ser explotadas por posibles amenazas que existan en el sistema de información.

4. **Análisis de Control (Actuales y Planificados)**

   El objetivo de esta fase es analizar los controles ya establecidos o por implementar en el sistema de información minimizando o eliminando la probabilidad que una amenaza vulnere el sistema de información.

5. **Determinación de Probabilidad**

   Se determina la probabilidad que una amenaza potencial que ejerza una vulnerabilidad dentro del sistema, los factores considerados son:

   - Motivación y capacidad de la amenaza
   - Naturaleza de la vulnerabilidad
   - Existencia y eficacia de controles actuales

6. **Análisis de Impacto**

   Esta fase determina el impacto resultante de un ejercicio de amenaza exitoso sobre una vulnerabilidad.

7. **Determinación del riesgo**

   Determina los riesgos dentro del sistema de información.

8. **Recomendación de Control**

   En esta fase proporciona controles que podrían minimizar o eliminar riesgos encontrados, estos controles deben reducir el nivel de riesgo del sistema de información a niveles aceptables, estas también van acompañadas de revisiones periódicas en nuestro sistema de información.

9. **Documentación de resultado**

En esta fase se genera un informe detallando la descripción de las amenazas, vulnerabilidades, riesgos evaluados y controles de recomendación.

3.3 Antecedentes referenciales

Dentro de las investigaciones realizadas con las metodologías de estudio, se puede evidenciar que, a nivel regional, existen diversos estudios que proponen una estrategia metodológica basada en Magerit, tal como se describe a continuación:

Rivera y Valdivia (2022), realizaron la Implementación de la metodología Magerit V3 para mejorar la gestión de riesgos de Seguridad de la Información y propuesta de políticas de seguridad basadas en norma técnica peruana ISO/IEC 27001:2014 en la Dirección Regional de Trabajo y Promoción del Empleo de Huánuco – 2021.

> "Las técnicas empleadas para la recolección de data fueron observacionales a través de formatos controlados, entrevistas, el alcance del estudio fue descriptivo, correlacional, el tipo utilizado y el diseño del estudio fueron cuasi – experimental. La muestra estuvo compuesta por 54 activos, se emplearon tablas de frecuencias para las dimensiones de las variables independiente y dependiente. Los resultados relacionados a los equipos tecnológicos arrojan que existe una reducción del estado de riesgos de la categoría "Intolerable" del 28% a 2%, así como la categoría "tolerable" disminuyo de 61% a 57%, de igual manera se vio una reducción de la probabilidad de amenaza en el 59 % al 35 % de los activos informáticos en la categoría Probabilidad de la categoría Amenaza probable, y se han observado reducciones generales. El estado de riesgo de los activos informáticos disminuye con el tiempo, aspectos de la seguridad de la información, como la confidencialidad, la integridad y la disponibilidad, para comprender mejor el contexto en el que se protege la información para que estas amenazas puedan abordarse adecuadamente a través de recomendaciones de política de privacidad."

López (2021), en su investigación denominada Gestión de riesgos con metodología NIST SP 800-30 a la seguridad en redes inalámbricas en la empresa Servintecomp

Ucayali-Pucallpa:2018, desarrolla un sistema de Gestión de Riesgo utilizando la metodología NIST SP 800-30 a la seguridad en redes inalámbricas, propuesta por el Instituto Nacional de Estándares y Tecnología. En su trabajo menciona: "*Con la metodología NIST SP 800-30 permite hacer 9 faces de la cual ayuda a evaluar los riesgos de la información especialmente a los sistemas de TI (Tecnología de la Información), por la cual es aplicable con el sistema de seguridad de la red inalámbrica. En la metodología permite hacer caracterización del sistema a su vez también hace un inventario de los activos. Se plantea la recolección de un listado de amenazas que podría explotar las vulnerabilidades del sistema, un listado de vulnerabilidades relacionados con los activos, y un listado de controles. Con una evaluación del riesgo hace posible comprender la probabilidad de vulnerabilidades, análisis de impacto y ocurrencia de amenazas, cálculo de riesgo y por último hace posible la toma de decisiones y controles recomendados*".

Cabrejos (2020), en su investigación sobre la influencia de la metodología Magerit v3 en la seguridad de información de la empresa Deco Interiors Sac. para lo cual se estableció el siguiente planteamiento metodológico: "*investigación de tipo aplicada con un diseño correlacional descriptivo, en una población de 115 colaboradores de donde se obtuvo una muestra correspondiente a los responsables del departamento de informática a los cuales se les aplicó un instrumento realizado y validado por juicio de expertos. Al procesarse e interpretarse los resultados conseguidos pudo evidenciarse una correlación positiva importante de 0.781 de la Metodología Magerit V3 y la seguridad de la información con un nivel de significancia por debajo de 0.05 propuesta en la investigación, así mismo, se determinó que la seguridad de la información se encuentra explicada en un 70.6% por la Metodología Magerit V3 realizada en la empresa. De esta manera, se confirma que hay influencia significativamente de una variable sobre la otra, lo que le asegura a la empresa la necesidad de aplicar la Metodología Magerit para poner en práctica una apropiada gestión de los riesgos a los que se encuentran expuestos sus activos de información*".

Florestino et al. (2015), en su investigación denominada Aplicación de la metodología MAGERIT en el análisis de riesgo del flujo de información en el área de gestión de una empresa dedicada a la aplicación de exámenes de control de confianza, llevada a cabo en la ciudad de México, concluyendo que la correcta

implementación de la metodología permite establecer prioridades, a su vez que se establecen los mecanismos de seguridad de la información, considerándolo como principal activo de la organización. Su delimitación se sustenta en factores como: tiempo de aplicación de la metodología, aceptación de la alta dirección, disponibilidad del personal del equipo asignado.

Pazmiño y Aldaz (2021), generaron la Propuesta de un plan de contingencia para salvaguardar los activos de información en el departamento de tecnología de la información y comunicación de la empresa pública municipal de residuos sólidos Rumiñahui-aseo EPM empleando la metodología Magerit, identificó los activos más importantes del departamento de tecnología, así como los riesgos y amenazas a los que pueden estar expuestos, para recomendar la implementación de salvaguardas. Con la ayuda de la herramienta PILAR, que fue utilizada principalmente por MAGERIT, se identificaron los activos para realizar el análisis de riesgo, se listaron los activos críticos, así como sus amenazas y salvaguardas, se realizó una evaluación de estos para identificar los riesgo e impacto que pueden causar si se materializan las amenazas. Se evidenció que, de veinte activos críticos, el 90% redujo al mínimo el impacto y los restantes bajaron su nivel de riesgo.

Guevara y Bonilla (2021), en su Análisis de seguridad de la información aplicando la metodología NIST SP 800-30 y NIST 800-115 para la Empresa Textiles JHONATHEX muestra que las organizaciones se encuentran inmersas en un contexto de fuerte desarrollo de negocios digitales, implementando nuevas tecnologías en sus sistemas de información, por tal motivo se exponen a mayores riesgos inherentes a este nuevo contexto de negocio y para proteger proactivamente a la empresa Textiles Jhonatex, se propone un proceso de gestión de vulnerabilidades adoptando la metodología NIST800-115 con un enfoque defensivo en las vulnerabilidades en tecnologías de la información, puesto que cada día se descubren miles de estas, mediante software de auditoría que permitirá identificar, analizar y remediar las vulnerabilidades de mayor preocupación. En su trabajo indican: "*La definición de un esquema para administrar vulnerabilidades técnicas, mejoraría la seguridad informática de la empresa, sin embargo, es necesario conocer los riesgos a los que está expuesto la empresa, con el propósito de mejorar los niveles de protección, haciendo uso de la metodología NIST800-30 se logrará definir estrategias que*

permitirán disminuir el impacto adverso que puede causar una o varias fuentes de amenazas. Al utilizar ambas metodologías, se logrará niveles óptimos en la seguridad de la información".

En el estudio de Gutiérrez (2019), quien hace la Aplicación de la metodología Magerit para el análisis del riesgo informático al departamento informático del Gobierno Autónomo Descentralizado Municipal del Cantón La Libertad utilizando la herramienta Pilar. En el trabajo se realizó el análisis de riesgo informático y se pudo identificar el nivel de riesgo en el que se encuentran los activos del departamento informático del GADMCLL mediante el nivel de madurez; mostrándonos que los activos cuentan con un alto índice de amenazas y riesgos que deben ser tratados de manera urgente; por lo que se presenta las salvaguardas con el fin de mitigar el riesgo.

Finalmente se presenta propuesta de lineamiento y un Plan de seguridad de la información con el fin de incentivar al personal a seguir con las normas y procedimientos referentes a la seguridad de la información y estar atentos a cualquier evento que se pueda presentar.

4. MATERIALES Y METODOLOGÍA

El presente apartado recorre sobre la forma en que se ejecutará la investigación, determinando el tipo de la investigación que se llevará a cabo, así como el diseño, alcance y variables de estudios. Además de mantener una definición sobre la población y la muestra sobre la que se aplicarán los diversos instrumentos que se diseñaron para la recopilación de datos de los sujetos de estudio.

La investigación es de tipo transversal, no experimental, aplicada ya que se pretende contribuir, desde los resultados obtenidos con una lista de recomendaciones que permita dar una solución a la problemática planteada.

El estudio es no experimental porque no se manipula deliberadamente las variables (Martínez C. , 2020). De la misma manera, el diseño es de campo, transversal, ya que para el estudio diagnostico se requiere una medición del fenómeno objeto de estudio en un solo momento.

4.1 Diseño de investigación

El enfoque cuantitativo utiliza la recolección y análisis de datos, para contestar preguntas de investigación y probar hipótesis establecidas y confía en la medición es decir examinar los datos de manera numérica, especialmente en el campo de la Estadística (Hernández et al., 2019)

Mientras que la investigación es descriptiva (Guevara et al., 2020) porque determina las características que identifica a las metodologías que se están comparando, como base fundamental para estructurar recomendaciones y buenas prácticas que apoye a la organización que las elija. Por ello este tipo de estudio está basado en técnicas específicas de recolección de la información, como lo es la ficha de revisión documental.

Es importante resaltar que además del tipo de investigación definido en este apartado, se debe hacer énfasis en que la investigación es de tipo proyectivo (proyecto factible) (Martínez y Vivas, 2022) porque el objetivo general apunta a recomendar mejores prácticas para el uso de las metodologías revisadas.

4.2 Instrumentos de medición y técnicas

La técnica para emplear en la presente investigación es la revisión documental, es una técnica de observación complementaria, en el caso de un registro de acciones y programas. La revisión documental permite hacer una idea del desarrollo y las características de los procesos y también la información que se confirma o se pone en duda (Hernández et al., 2019).

4.3 Metodología

Para este proyecto de investigación se aplicó un método cuantitativo donde se utilizará la teoría en los métodos de análisis de riesgos como fundamento en la elaboración de criterios y comparativas que permitan la selección de una, y con un mecanismo comparativo descriptivo porque el objetivo de la investigación consiste en analizar las metodologías y estándares dando resultado un análisis con criterio para un marco de tomas de decisiones.

Por otra parte, el desarrollo de esta investigación se llevará acabado en tres fases:

- Revisión de teoría y conceptos de investigaciones relacionados a la gestión y análisis de riesgos.
- Analizar metodologías de riesgos Magerit y NIST SP 800-30 con trabajos relacionados y de igual manera con metodologías existentes en la actualidad.
- Construcción de un marco comparativo para un modelo de toma de decisión.

4.4 Procedimientos

La metodología para emplear el desarrollo de la presente investigación fue:

- Levantamiento de información, que es el primer momento donde se realiza la revisión documental que justifica la investigación y el acercamiento hacia las fuentes primarias de información desde donde se consideraron los aspectos contextuales de cada una de las metodologías objeto de estudio.
- Procesamiento de datos, que es la siguiente fase luego de tener los datos correspondientes al estudio, se realizó la comparación de cada una de las características de las metodologías, identificando las concordancias y diferencias entre ambas.
- Análisis de los datos, con los insumos anteriores, se pretende justificar una lista de recomendaciones que orienten al lector sobre las ventajas de las metodologías estudiadas.

4.5 Materiales

Para realizar este análisis se consideraron artículos de referencia los que nos permite presentar los dos métodos de análisis de riesgos que comparamos en esta investigación.

Como se puede observar en la tabla 1, los objetivos que pretende Magerit sobre los de NIST SP 800-30, evolucionan hacia la conciencia de quienes usan los sistemas de información, para manejarlos y gestionarlos de la mejor forma, mientras que la NIST SP 800-30 se limitan hacia la necesidad de solo administrarlos.

Tabla 1. Comparación Objetivos

MAGERIT Metodología de análisis y Gestión de Riesgos de los Sistemas de información	NIST SP 800-30 Instituto Nacional de Estándares y Tecnología
Objetivos de la metodología: • Concienciar a los responsables de TI de una organización de la existencia de riesgos y de gestionarlos. • Ofrece una metodología sistemática que permite analizar, identificar y planificar los riesgos y tenerlo gestionados.	**Objetivo de la metodología:** 1. Asegurar de mejor manera la administración de los sistemas de información con guías de como mitigar y gestionar los riesgos asociados.

En la tabla 2, se especifica las fases o pasos que cada metodología emplea para cumplir sus propósitos, por una parte, Magerit mantiene cinco fases, mientras NIST SP 800-30 sigue varios pasos que incorporan identificación de amenazas, vulnerabilidades, control, probabilidad e impacto del riesgo.

Tabla 2. Comparación Metodología

MAGERIT Metodología de análisis y Gestión de Riesgos de los Sistemas de información	NIST SP 800-30 Instituto Nacional de Estándares y Tecnología
Fases de la metodología: • Identificación de los activos • Determina Amenazas • Determina Salvaguardias • Estimar el impacto residual • Estima Riesgos residual	**Pasos de la metodología:** • Caracterización del sistema • Identificación de Amenazas • Identificación de Vulnerabilidades • Análisis de Control • Determinación de Probabilidad • Análisis de Impacto • Determinación del riesgo • Recomendación de control

	• Documentación de resultado

En cuanto al análisis de riesgos, la metodología MAGERIT determina, identifica y valora los impactos sobre cada activo que pudiera estar expuesto, mientras que la NIST SP 800-30 hace una caracterización ampliada del sistema incorporando, sistemas de conectividad, datos e información, personal y riesgo crítico de datos.

Tabla 3. Comparación Análisis de riesgos

MAGERIT Metodología de análisis y Gestión de Riesgos de los Sistemas de información	NIST SP 800-30 Instituto Nacional de Estándares y Tecnología
Análisis de Riesgo e identificación de los activos: • Determina e identifica los activos que tiene la organización. • Determina las amenazas e impacto sobre cada activo que pudiera estar expuesto.	**Caracterización del Sistemas:** • Determina el entorno operativo de un sistema de TI tales como: o Hardware o Software o Sistemas de conectividad o Datos e información o Personal o Criticidad de los datos

En cuanto a las amenazas, tal como se muestran en la tabla 4, la metodología Magerit, determina y valora las amenazas a través de criterios como impacto y riesgo potencial, mientras que la NIST SP 800-30 aplica métodos de detención para las amenazas sin contemplar algún criterio específico.

Tabla 4. Comparación Parámetro Amenazas

MAGERIT Metodología de análisis y Gestión de Riesgos de los Sistemas de información	NIST SP 800-30 Instituto Nacional de Estándares y Tecnología
Determinación de Amenazas:	**Identificación de Amenazas:** • Identifica amenazas potenciales aplicando métodos de detención

• Determina e identifica las amenazas que pudieran afectar a cada activo y cause daño. • Añadimos valoración a las amenazas identificadas e impacto y riesgo potencial.	para explotar una vulnerabilidad o que pueda materializar una amenaza.

En cuanto al manejo de riesgos, la tabla 5 muestra la metodología Magerit cuenta con procedimientos o mecanismos que nos ayuden a mitigar o reducir los riesgos e impactos de una amenaza, mientras que la NIST SP 800-30 identifica una lista de vulnerabilidades que pueden ser consideradas amenazas, incluyendo en su perímetro de seguridad exterior o infraestructura.

Tabla 5. Comparación Parámetro Salvaguardias/vulnerabilidades

MAGERIT Metodología de análisis y Gestión de Riesgos de los Sistemas de información	NIST SP 800-30 Instituto Nacional de Estándares y Tecnología
Determinación de Salvaguardias: • Procedimientos o mecanismos que nos ayuden a mitigar o reducir los riesgos e impactos de una amenaza.	**Identificación de vulnerabilidades:** • Identifica un listado de vulnerabilidades que podrían ser explotados por una amenaza o Hardware o Software o Personal o Instalaciones

En la tabla 6 se puede evidenciar una de las mas importantes fases que tienen estas metodologías y es la evaluación del impacto, en este caso para Magerit, se estima el impacto y el riesgo residual, mientras que para la metodología NIST SP 800-30, se recrea un análisis de control, hasta llegar a las recomendaciones apropiadas para cada vulnerabilidad.

Tabla 6. Comparación Impactos

MAGERIT Metodología de análisis y Gestión de Riesgos de los Sistemas de información	NIST SP 800-30 Instituto Nacional de Estándares y Tecnología
Estimar impacto residual: • definido como el daño al activo derivado de la ocurrencia de la amenaza **Estimar riesgo residual:** • definido como el impacto ponderado sobre la tasa de ocurrencia o expectativa de aparición de la amenaza	**Análisis de Control:** • Analiza los controles implementados por TI para la reducción de amenazas. **Determinación de Probabilidad:** • Se determina una clasificación global del riesgo la cual indica la probabilidad de materialización de la amenaza. **Análisis de Impacto:** • Mide el riesgo determinando efectos adversos materializados de una amenaza. **Determinación del riesgo:** • Evalúa el nivel de riesgo, determinando las amenazas y de donde provienen. **Recomendación de control:** • Detalla los controles de reducción de los riesgos en los sistemas de TI teniendo en cuenta: o Eficiencia de las soluciones o Legislación y Regulación o Impacto Operativo o Seguridad y fiabilidad **Documentación de resultado:**

	• Documentación de evaluación de riesgos, vulnerabilidades y amenazas con resultados obtenidos para posteriores análisis

5. Resultados y discusión

Cada metodología analizada (Magerit y NIST SP 300-80) aborda los procesos de la gestión de riesgos con enfoques diferentes, métodos, características y otros aspectos analizados.

Las organizaciones que hacen uso de metodologías o requieren aplicarlas, pueden construir todo el proceso de análisis, identificación, evaluación y gestión de riesgos ya que las metodologías analizadas proporcionan un enfoque sistemático sobre como identificar, analizar, evaluar y gestionar el riesgo.(Seguridad de la Información, 2021)

En el apartado de metodología, compararemos Magerit con NIST SP 800-30. Para desarrollar una comparación adecuada, se ha seleccionado diferentes criterios de comparación de estas metodologías, con valoraciones entre 3 y 0 puntos, con la finalidad que un mayor puntaje refleja un mejor acercamiento del aspecto más importante al momento de seleccionar una.

Recordemos que la valoración es solo para el criterio, para comparar las metodologías y no quiere decir que una es mejor que otra.

Tabla 7. Valoración según criterios de evaluación

CRITERIO DE EVALUACION	DESCRIPCION
ENFOQUE	Aborda los riesgos en la Seguridad de la Información o de manera general Valoración: • 2: En Seguridad de la Información • 1: De manera General
	Idiomas disponibles Valoración:

IDIOMA	• 2: En español • 1: En ingles • 0: Otro idioma
TIPO DE EMPRESA QUE ES DIRIGIDA	Pequeña, mediana, grande Valoración: • 2: Aplica para la mayoría • 1: Aplica para grandes y pequeñas • 0: Aplica solo grandes
GESTION DE RIESGOS	Procesos principales de la metodología abordada Valoración: • 2: Cuenta con la mayoría de los procesos principales • 1: No cuenta con la mayoría de los procesos principales
SOPORTE O APOYO	Se cuenta con guías de apoyo o soporte Valoración: • 2: Se cuenta con guías de apoyo para la implementación • 1: Documentación general de la norma
HERRAMIENTA DE SOPORTE	La metodología utiliza alguna herramienta gratuita o de pago Valoración: • 3: Existen herramientas gratuitas, pero no las requiere • 2: Existen herramientas de pago, pero no las requiere • 1: No requiere • 0: Requiere
IMPLEMENTACION	Cuenta con planeación de proyectos, roles, técnica, etc. Valoración: • 2: Cuenta con la mayoría • 1: No cuenta con la mayoría • 0: No cuenta
COSTOS	Libre o mediante pago Valoración: • 2: Libre • 1: De Pago
	Activos, procesos, recursos, amenazas, vulnerabilidades y controles

ELEMENTOS	Valoración: • 3: Cuenta con todos • 2: Cuenta con la mayoría (4 o 5 de ellos) • 1: tiene alguno (1 o 3 de ellos)
TIPOS DE ANALISIS	Cualitativo o Cuantitativo Valoración: • 3: Cuenta con ambos • 2: Cualitativo • 1: Cuantitativo
COMPLEJIDAD DE IMPLEMENTACION	Alta, media y baja Valoración: • 3: Alta • 2: Media • 1: Baja

Ahora que tenemos una valoración en los criterios de evaluación por cada metodología investigada, presentamos los resultados en la tabla 8 con los criterios que creemos y analizamos desde dicha comparación.

Se puede observar que, en cuanto al enfoque, ambas metodologías se orientan específicamente hacia la Seguridad de los sistemas de información, aunque la NIST SP 800-30 puede limitarse solo a la administración de los sistemas, ya que no especifica claramente el alcance hacia los demás elementos como el personal, en cuanto a su enfoque.

En cuanto a la disponibilidad de idiomas, en la región Latinoamericana, puede esto ser un impedimento, considerando que el lenguaje nativo para las instrucciones de implementación debe ser en español, por lo que la ventaja es para Magerit que tiene esa disponibilidad.

Existe una distinción importante en cuanto a las herramientas de soporte, que son necesarias y de pago, en este contexto, se considera que Magerit tiene una importante ventaja debido a que no requiere soporte, mientras que la NIST SP 800-30 puede complicar su uso y soporte, limitando el acceso a esta metodología.

Adicionalmente, los elementos que son incorporados en cada metodología se orientan hacia el enfoque que inicialmente se ha medido y que es parte de la orientación de la herramienta, por lo que en este caso la NIST SP 800-30 cuenta con una consideración mayor de la cantidad de elementos que esta incorpora.

En relación con el criterio del tipo de análisis que estas metodologías llevan adelante, se puede considerar como una ventaja que la Metodología Magerit pueda evaluarse en una metodología mixta (incluyendo análisis cualitativo y cuantitativo), puesto que, desde este punto de vista, se recrea la situación del contexto considerando una mirada integral del objeto y los sujetos de estudio involucrados en la organización sobre la que se desea realizar la implementación.

Tabla 8. Evaluación realizada – Resultados comparativos

	METODOLOGIA	
CRITERIO DE EVALUACION	**MAGERIT**	**NIST SP 800-30**
Enfoque	**2**	**2**
Idioma	**2**	**1**
Tipo de empresa que es dirigida	**1**	**1**
Gestión de Riesgos	**2**	**2**
Soporte o apoyo	**2**	**2**
Herramientas de Soporte	**1**	**3**
Implementación	**2**	**2**
Costos	**2**	**2**
Elementos	**1**	**2**
Tipo de análisis	**3**	**2**
Complejidad de implementación	**2**	**2**
TOTAL	**20**	**21**

A partir del puntaje obtenido por las metodologías analizadas en esta investigación podemos definir en cada metodología una estructura por la cual las organizaciones pueden elaborar sus procesos de identificación, evaluación y análisis de riesgos en sus sistemas de información, proporcionando una orientación sistemática de como mitigar los riesgos expuestos. A pesar de que existe diferencia entre ellos, las dos metodologías analizadas toman como referencia y guía la norma ISO 27001.

Así mismo podemos indicar algunas ventajas y desventajas de cada metodología.

Magerit:

Ventajas

- Utiliza los análisis de riesgos de modo cualitativos y cuantitativos.
- Es libre uso, no requiere licenciamiento.
- Divide los activos de una organización para identificar los riesgos y aplicar salvaguardias.
- Posee documentación en sus tres versiones.

- Sus tres objetivos se centran en la concientización de la existencia del riesgo, un análisis sistemático para analizarlos y planifica y descubre medidas para mantenerlas minimizadas.

Desventajas

- No involucra procesos ni vulnerabilidades dentro de su modelo.

NIST SP 800-30:

Ventajas

- Se proveen guías para las valoraciones y nos permite mitigar los riesgos.
- Ayuda a mejora la administración con los resultados de análisis.
- Es aplicable en todas las etapas del proceso

Desventajas

- No contemplan los elementos ni activos del sistema de información.

6. Conclusiones

La revisión documental de las metodologías Magerit y NIST SP 800-30 ha permitido distinguir las bondades de cada una de estas herramientas, con la finalidad de visibilizarlas como posibles opciones al momento de analizar el riesgo de los sistemas de información que tiene una organización.

Es esencial poner de manifiesto que ambas herramientas son basadas o llevan adelante los más altos estándares de calidad como la norma ISO 27001. Lo que garantiza que han sido pensadas y creadas para lograr una estabilidad en la evaluación de riesgos que permita confiar en resultados cercanos a la realidad y con la mayor cantidad de elementos involucrados posibles.

En cuanto al análisis de riesgos, estas son una excelente herramienta a nivel organizacional, tanto Magerit como NIST SP 800-30 son metodologías aplicables en cualquier organización que requiera minimizar riesgos dentro de un sistema de información. Las metodologías de análisis de riesgos analizadas siguen los tres pasos fundamentales, que son:

- Identificación de Amenazas
- Identificación de Vulnerabilidades
- Determinación del Riesgo

Por lo que, las metodologías analizadas ayudaran a contar con un control sobre los activos de las organizaciones tratando de minimizar las amenazas contando con medidas de seguridad que garantice su disponibilidad.

Por su parte, Magerit como metodología realiza el análisis de activos inventariados de la organización con la que les asigna un valor según su importancia, brindando documentos complementarios para lograr las recomendaciones apropiadas en cada caso. Su disponibilidad en idioma español asegura que las empresas de habla hispana vean en esta una solución a su medida. Aunque no incluye recomendaciones de control, lo que hace que se deba recurrir a un segundo nivel de análisis para lograr las recomendaciones del caso.

Por su parte la NIST SP 800-30, incluye un detalle importante de elementos que se disgregan al momento de su implementación, considera ambientes laborales y su visión es integradora y transversal a la operación de la organización, por lo que podría volverse más compleja su implementación. Sin embargo, incorpora recomendaciones de control y análisis de riesgos que garantiza un ciclo completo dentro de un mismo ejercicio, volviéndola efectiva, pero con un tiempo más prolongando de implementación.

Todo se basa en la utilidad que requiera la organización y que tan aplicable se complementa en sus procesos y marco de trabajo.

Referencias

Aditya Putra Fatri, Setiawan Hermawan, & Rifa Pradana Anggi. (2017). Design of Information Security Risk Management Using ISO/IEC 27005 and NIST SP 800-30 Revision1: A Case Study at Communication Data Applications of XYZ Institute. International Conference on Information Technology Systems and Innovation (ICITSI).

coordinación de contenidos, E., General de Modernización Administrativa, D., & Impulso de la Administración Electrónica, P. (s. d.). Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método. http://administracionelectronica.gob.es/

Hurtado, M. (s. d.). GESTIÓN DE RIESGO METODOLOGÍAS OCTAVE y MAGERIT.

Muñoz Mata, M. A., & Institute of Electrical and Electronics Engineers. (s. d.). Applications in software engineering: proceedings of the 7th International Conference on Software Process Improvement (CIMPS 2018): Guadalajara, Jalisco, México, October 17-19, 2018.

Santos Olmo Parra, A., Sanchez Crespo, L. E., Alvarez, E., Huerta, M., & Fernandez Medina Paton, E. (2016). Methodology for Dynamic Analysis and Risk Management on ISO27001. IEEE Latin America Transactions, 14(6), 2897-2911. https://doi.org/10.1109/TLA.2016.7555273

Aditya Putra Fatri, Setiawan Hermawan, & Rifa Pradana Anggi. (2017). Design of Information Security Risk Management Using ISO/IEC 27005 and NIST SP 800-30 Revision1: A Case Study at Communication Data Applications of XYZ Institute. *International Conference on Information Technology Systems and Innovation (ICITSI)*.

coordinación de contenidos, E., General de Modernización Administrativa, D., & Impulso de la Administración Electrónica, P. (s. d.). *Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método*. http://administracionelectronica.gob.es/

Hurtado, M. (s. d.). *GESTIÓN DE RIESGO METODOLOGÍAS OCTAVE y MAGERIT*.

Muñoz Mata, M. A., & Institute of Electrical and Electronics Engineers. (s. d.). *Applications in software engineering: proceedings of the 7th International Conference on Software Process Improvement (CIMPS 2018): Guadalajara, Jalisco, México, October 17-19, 2018*.

Santos Olmo Parra, A., Sanchez Crespo, L. E., Alvarez, E., Huerta, M., & Fernandez Medina Paton, E. (2016). Methodology for Dynamic Analysis and Risk Management on ISO27001. *IEEE Latin America Transactions*, *14*(6), 2897-2911. https://doi.org/10.1109/TLA.2016.7555273

Seguridad de la Información, versión 1. (2021). *Autor: Seguridad de la Información*.

Syalim, A., Hori, Y., & Sakurai, K. (2009). Comparison of risk analysis methods: Mehari, magerit, NIST800-30 and microsoft's security management guide. *Proceedings - International Conference on Availability, Reliability and Security, ARES 2009*, 726-731. https://doi.org/10.1109/ARES.2009.75

Tejena-Macías, M. A. (2018). Análisis de riesgos en seguridad de la información. *Polo del Conocimiento*, *3*(4), 230. https://doi.org/10.23857/pc.v3i4.809

Seguridad de la Información, versión 1. (2021). Autor: Seguridad de la Información.
Syalim, A., Hori, Y., & Sakurai, K. (2009). Comparison of risk analysis methods: Mehari, magerit, NIST800-30 and microsoft's security management guide. Proceedings - International Conference on Availability, Reliability and Security, ARES 2009, 726-731. https://doi.org/10.1109/ARES.2009.75
Tejena-Macías, M. A. (2018). Análisis de riesgos en seguridad de la información. Polo del Conocimiento, 3(4), 230. https://doi.org/10.23857/pc.v3i4.809
Aditya Putra Fatri, Setiawan Hermawan, & Rifa Pradana Anggi. (2017). Design of Information Security Risk Management Using ISO/IEC 27005 and NIST SP 800-30 Revision1: A Case Study at Communication Data Applications of XYZ Institute. *International Conference on Information Technology Systems and Innovation (ICITSI)*.
coordinación de contenidos, E., General de Modernización Administrativa, D., & Impulso de la Administración Electrónica, P. (s. d.). *Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método*. http://administracionelectronica.gob.es/
Hurtado, M. (s. d.). *GESTIÓN DE RIESGO METODOLOGÍAS OCTAVE y MAGERIT*.
Lambrinoudakis, Costas., Gritzalis, Stefanos., Xenakis, Christos., Katsikas, Sokratis., Karyda, Maria., Tsochou, Aggeliki., Papadatos, Kostas., Rantos, Konstantinos., Pavlosoglou, Yiannis., Gasparinatos, Stelios., Pantazis, Anastasios., Zacharis, Alexandros., & European Union Agency for Cybersecurity. (s. d.). *Compendium of risk management frameworks with potential interoperability: supplement to the interoperable EU risk management framework report.*
Muñoz Mata, M. A., & Institute of Electrical and Electronics Engineers. (s. d.). *Applications in software engineering: proceedings of the 7th International Conference on Software Process Improvement (CIMPS 2018): Guadalajara, Jalisco, México, October 17-19, 2018*.
Santos Olmo Parra, A., Sanchez Crespo, L. E., Alvarez, E., Huerta, M., & Fernandez Medina Paton, E. (2016). Methodology for Dynamic Analysis and Risk Management on ISO27001. *IEEE Latin America Transactions*, *14*(6), 2897-2911. https://doi.org/10.1109/TLA.2016.7555273
Seguridad de la Información, versión 1. (2021). *Autor: Seguridad de la Información*.
Syalim, A., Hori, Y., & Sakurai, K. (2009). Comparison of risk analysis methods: Mehari, magerit, NIST800-30 and microsoft's security management guide. *Proceedings - International Conference on Availability, Reliability and Security, ARES 2009*, 726-731. https://doi.org/10.1109/ARES.2009.75
Tejena-Macías, M. A. (2018). Análisis de riesgos en seguridad de la información. *Polo del Conocimiento*, *3*(4), 230. https://doi.org/10.23857/pc.v3i4.809

Cabrejos, R. (2020). *INFLUENCIA DE LA METODOLOGÍA MAGERIT V3 EN LA SEGURIDAD DE INFORMACIÓN DE LA EMPRESA DECO INTERIORS SAC.* Universidad Señor de Sipán.
Calles-García, J., y González-Pérez, P. (2011). *La Biblia del Footprinting.*
Florentino Galindo, E., Morales Morales, J., y Peña Velázquez, J. (2015). *Aplicación de la metodología MAGERIT en el análisis de riesgo del flujo de información en el área de gestión de una empresa dedicada a la aplicación de exámenes de control de confianza.* https://tesis.ipn.mx/handle/123456789/14873

Guevara, D., y Bonilla, J. (2021). *Análisis de seguridad de la información aplicando la metodología NIST SP 800-30 y NIST 800-115 para la Empresa Textiles JHONATHEX.* https://repositorio.uta.edu.ec/handle/123456789/32301

Guevara, G., Verdesoto, A., y Castro, N. (2020). Metodologías de investigación educativa (descriptivas, experimentales, participativas, y de investigación-acción). *Revista científica Mundo de la investigación y del conocimiento*, 163-173. https://doi.org/http://recimundo.com/index.php/es/article/view/860

Gutierrez, C. (2019). *Aplicación de la metodología Magerit para el análisis del riesgo informático al departamento informático del Gobierno Autónomo Descentralizado Municipal del Cantón La Libertad utilizando la herramienta Pilar.* https://doi.org/https://repositorio.espe.edu.ec/xmlui/handle/21000/20405

Hernández, R., Fernández, C., y Baptista, M. (2019). *Metodología de la investigación.* https://www.uca.ac.cr/wp-content/uploads/2017/10/Investigacion.pdf

Lopez, J. (2021). *Gestión de riesgos con metodología NIST SP 800-30 a la seguridad en redes inalámbricas en la empresa Servintecomp Ucayali-Pucallpa:2018.* http://repositorio.unu.edu.pe/handle/UNU/4982

Machuca Ordoñez, C., y Peña Cruz, A. (2021). *Propuesta de un modelo de gestión de riesgos para mejorar la seguridad de la información de las dependencias de la Marina de Guerra del Perú, aplicando metodología Magerit.* https://repositorio.utp.edu.pe/handle/20.500.12867/6571

Martínez, C. (2020). *Diseño de investigación, muestreo y métodos de recolección de datos.* https://escueladedatos.online/diseno-de-investigacion-muestreo-y-metodos-de-recoleccion-de-datos/#:~:text=El%20dise%C3%B1o%20de%20investigaci%C3%B3n%20proporciona,a%20las%20preguntas%20de%20investigaci%C3%B3n.

Martínez, M., y Vivas, A. (2022). *Guía de Modalidad de proyecto factible.* http://estudios.umc.cl/wp-content/uploads/2023/01/Gu%C3%ADa-de-Modalidad-de-Proyecto-Factible_-Mart%C3%ADnez-Vivas_-2022_LED-UMC_compressed.pdf

Ministerio de Salud. (2014). *REGLAMENTO A LA LEY ORGANICA DE SALUD.* https://www.salud.gob.ec/wp-content/uploads/downloads/2014/09/Reglamento-a-la-Ley-Org%C3%A1nica-de-Salud.pdf

Ministerio de Trabajo. (2018). *Acuerdo MDT Norma técnica de medición de clima laboral del servicio público*. https://www.trabajo.gob.ec/wp-content/uploads/2018/07/MDT-2018-0138.pdf?x42051

Pazmiño, F., y Aldaz, N. (2021). *PROPUESTA DE UN PLAN DE CONTINGENCIA PARA SALVAGUARDAR LOS ACTIVOS DE INFORMACIÓN EN EL DEPARTAMENTO DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN DE LA EMPRESA PÚBLICA MUNICIPAL DE RESIDUOS SÓLIDOS RUMIÑAHUI-ASEO EPM EMPLEANDO LA METODOLOGÍA MAGERIT.* https://dspace.ups.edu.ec/bitstream/123456789/19865/1/UPS%20-%20TTS276.pdf

QuestionPro. (2020). *Muestreo no probabilístico.* https://www.questionpro.com/blog/es/muestreo-no-

probabilistico/#:~:text=El%20muestreo%20no%20probabil%C3%ADstico%20es,hacer%20la%20selecci%C3%B3n%20al%20azar.

Rivera , D., y Valdivia , J. (2022). *Implementación de la metodología Magerit V3 para mejorar la gestión de riesgos de Seguridad de la Información y propuesta de políticas de seguridad basadas en norma técnica peruana ISO/IEC 27001:2014 en la Dirección Regional de Trabajo y Promoción del Emp.* https://repositorio.unheval.edu.pe/handle/20.500.13080/7066?show=full

www.elhacker.net. (s.f.). *www.elhacker.net*. https://www.elhacker.net/trucos_google.html