UNIVERSIDAD TÉCNICA DE BABAHOYO
FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA
CARRERA DE INGENIERÍA EN SISTEMAS
MODALIDAD PRESENCIAL

DOCUMENTO PROBATORIO (DIMENSIÓN ESCRITA) DEL EXAMEN COMPLEXIVO DE GRADO

PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN SISTEMAS

TEMA:

ANÁLISIS COMPARATIVO ENTRE LAS METODOLOGÍAS DE GESTIÓN DE RIESGOS DE LOS SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI): MAGERIT Y OCTAVE

EGRESADA:
GISSELA ANNABEL CONTRERAS OLEA

TUTOR:
INGENIERO OMAR RODRIGO MONTECÉ MORENO

BABAHOYO – ECUADOR 2022

Resumen

Diariamente, las empresas están tratando de contrarrestar los efectos que implican los constantes avances tecnológicos y el acceso a grandes cantidades de datos, muchas organizaciones experimentan numerosos tipos de ataques informáticos, manipulación de datos y pérdida de información. Es por ello, que el estudio de esta investigación, se efectuó en un análisis comparativo entre las metodologías de gestión de riesgos de los sistemas de gestión de seguridad de la información (SGSI): MAGERIT y OCTAVE, que permita identificar que metodología proporciona la mejor toma de decisiones en cuanto a los activos de información. En tal sentido, se planteó el objetivo principal: Realizar un análisis comparativo entre las metodologías de gestión de riesgos: Magerit y Octave. La indagación se basó en la investigación bibliográfica, referenciada en tesis, repositorios universitarios, bases de datos indexadas y artículos de revistas, consecutivamente, se optó el método analítico y a su vez el tipo de investigación descriptiva. Por consiguiente, se realizó el estudio comparativo con base a los criterios generales de cada una de las metodologías escogidas, es decir, Magerit y Octave, desde las bases de sus conceptos y sus fases, además sus características principales, fortalezas y debilidades. Lo anterior propició a la formulación de las conclusiones, las cuales se consideró que dada las comparaciones de las metodologías en cuestión, MAGERIT a diferencia de OCTAVE, toma procesos más seguros en su ejecución, debido a que su análisis de riesgos es más completo. A pesar de que las dos metodologías tienen su ámbito de aplicación, debido a que una organización las utiliza más que otras, todas dos pueden ser empleadas en empresas, tanto públicas como privadas.

Palabras clave: seguridad de la información, metodologías, gestión de riesgos, magerit, octave.

Abstract

On a daily basis, companies are trying to counteract the effects of constant technological advances and access to large amounts of data, many organizations experience numerous types of computer attacks, data manipulation and information loss. That is why the study of this research was carried out in a comparative analysis between the risk management methodologies of the information security management systems (ISMS): MAGERIT and OCTAVE, which allows identifying which methodology provides the best decision making regarding information assets. In this sense, the main objective was raised: To carry out a comparative analysis between the risk management methodologies: Magerit and Octave. The inquiry was based on bibliographic research, referenced in theses, university repositories, indexed databases and journal articles, consecutively, the analytical method was chosen and in turn the type of descriptive research. Therefore, the comparative study was carried out based on the general criteria of each of the chosen methodologies, that is, Magerit and Octave, from the bases of their concepts and their phases, as well as their main characteristics, strengths and weaknesses. The foregoing led to the formulation of the conclusions, which were considered that given the comparisons of the methodologies in question, unlike OCTAVE, MAGERIT takes safer processes in its execution, due to the fact that its risk analysis is more complete. Although the two methodologies have their scope of application, due to the fact that an organization uses them more than others, both of them can be used in companies, both public and private.

Keywords: information security, methodologies, risk management, magerit, octave.

INTRODUCCIÓN

El presente trabajo de investigación está orientado al desarrollo de una comparativa sobre dos metodologías de gestión de riesgos, tomando como base las metodologías Magerit y Octave. Actualmente, existen diversas metodologías que facilitan las tareas de ejecución en las actividades cotidianas que mantienen las empresas en seguimiento a su desarrollo, puesto que, dado los constantes avances tecnológicos, estas herramientas han ido evolucionando y se han ajustado de acuerdo a los criterios y necesidades de cada organización, en otros términos, la aplicación de estas dos metodologías vanguardistas, sugieren un seguimiento periódico para llevar a cabo el alcance, control y desarrollo de seguridad de la información en las distintas áreas organizacionales.

De hecho, surgen muchas problemáticas a las que se enfrentan diariamente las empresas, como el espionaje, ataques informáticos, divulgación, manipulación de datos, pérdida de información crítica por falta de copias de seguridad, desastres naturales, actos deliberados por terceros, y poca o nula gestión de riesgos; esto sucede precisamente porque las empresas no cuentan con metodologías que contribuyan al procesamiento y tratamiento de la información o porque implica una ardua labor en su implementación, es decir, tiempo y costo. Esencialmente, muchas regulaciones y estándares establecen parámetros para analizar y evaluar fugas de información, ataques a la identidad corporativa, sanciones legales e incluso acciones que pueden conducir al cierre de empresas.

Por las cuestiones antes mencionadas, la objetividad de este caso de estudio es realizar un análisis comparativo entre las metodologías de gestión de riesgos: Magerit y Octave, hecho que permita corroborar y demostrar la validez de argumentos basados en investigaciones y al análisis de la comparación sistemática de los objetos a estudiarse, a partir de lineamientos que permitan demostrar alternativas y disoluciones a los dilemas de una organización, considerando así, la línea

de investigación de la Carrera de Ingeniería en Sistemas: Sistemas de Información y Comunicación, Emprendimiento e Innovación, asociada a la sub-línea de investigación: Redes y Tecnologías Inteligentes de Software y Hardware.

La investigación sostiene un enfoque cualitativo, la cual se asentó en el uso de documentación bibliográfica, como tesis, artículos de revistas, repositorios universitarios, bases de datos indexadas, lo que permitió llegar a una conclusión basada en investigación y discusión actualizada de los fenómenos en cuestión. También se optó anexar el método analítico, considerando estudiar los elementos por separado para su respectivo análisis como parte del desarrollo de la investigación a comparar. Además, se utilizó la investigación descriptiva, la misma que permitió describir las funcionalidades para las que están construidas las metodologías de gestión de riesgos de los sistemas de gestión de seguridad de la información: Magerit y Octave.

DESARROLLO

En la actualidad del pleno siglo XXI la tecnología se ha posicionado como un elemento sustancial en el ámbito de la vida empresarial, de manera similar, dentro de una globalización activa y proactiva, las empresas tienden a canalizarse mediante extensos volúmenes de datos, aumentando el riesgo desde el procesamiento de la información hasta su almacenamiento. En tal sentido, la información es el recurso más valioso que las empresas, organizaciones e instituciones tienen a su servicio, dicho esto, es el activo con más movimiento en el mundo, que permite realizar todas las operaciones, funciones y actividades, teniendo en consideración que, tanto la información como los numerosos datos que poseen tienden a ser vulnerados y manipulados.

Hoy en día, con el avance tecnológico y las nuevas herramientas que existen, nos permiten poner a disposición todos los recursos necesarios para resolver los problemas y desafíos a los que estas se encuentran sin mayor esfuerzo. Asimismo, la tecnología se desarrolla como un curso cambiante, que contribuye con mayor facilidad adaptarse en el marco del nivel de competencia empresarial, motivo por el cual, es imprescindible optar por la aplicación de metodologías, que faciliten a través del análisis, lograr identificar, evaluar y mitigar las posibles amenazas, vulnerabilidades e impacto que sufren las empresas dentro del mundo digital del ciberespacio y por consecuencias naturales.

Es así que la importancia de la investigación y considerando la descripción y el análisis de cada una de las metodologías a tratarse dentro de este apartado, aportará de manera sustancial al desarrollo de la investigación y del investigador, asimismo, contribuirá con fuentes de información necesarias que permitan generar conocimientos acerca del valor que tienen las metodologías en las organizaciones, en búsqueda a su aportación en los aspectos educativos y organizacionales, y de esta forma permita generar concientización sobre el margen del nivel de riesgo que tiene la

seguridad con relación a la información y a una serie de peligros informáticos que se desglosan afectando directa o indirectamente a los sistemas de información que continuamente se encuentran expuestos a los impactos relativos del riesgo.

La ejecución de esta indagación es factible, porque se tiene presente, elementos competentes, tales como fuentes bibliográficas y recursos tecnológicos necesarios para llevar a cabo el aporte de la investigación. Además, al hacer un instrumento viable en su ejecución, conlleva a brindar referencias a las presentes y futuras investigaciones.

El objetivo inicial está encaminado en realizar un análisis comparativo entre las metodologías de gestión de riesgos: Magerit y Octave, consecuentemente, describir cada una de las dos metodologías desde el criterio de sus fases y sus procesos. También se podrá identificar aspectos importantes en cuanto a las metodologías, y finalmente, se permitirá comparar las dos metodologías MAGERIT Y OCTAVE utilizadas para el análisis y la gestión de los riesgos, sobre la base de sus características, fortalezas y debilidades.

Abreviando la teoría, existen dos aspectos importantes que las metodologías consideran como punto clave: la probabilidad que ocasiona el impacto sobre la información y la determinación directa del impacto en la empresa.

Gestión de riesgos

Para (Guerrero Aguiar y otros, 2020) “la gestión de riesgos juega un papel fundamental a nivel organizacional; su administración promueve un enfoque procedimental, uso óptimo de recursos, minimización de costos, y es indicativo de una cultura orientada al establecimiento del control interno”. Considerando lo anterior, la gestión de riesgo comprende identificar, evaluar, disuadir y contrarrestar las incidencias, estos términos se emplean para tomar medidas de protección y establecer salvaguardas a través del conjunto de políticas, herramientas y

metodologías que facilitan las tareas extensas en una empresa, es por ello, que la gestión de riesgo permite cualificar y cuantificar los procesos con respecto a cada interrogante, qué es, cuánto cuesta, y qué tan bien son preservados los datos durante el tratamiento, en síntesis, tiene como objetivo elevar el nivel empresarial.

- ***Identificar el riesgo***

La objetividad de este proceso consiste en identificar el contexto donde se crean los múltiples sucesos que afectan directamente a la organización; por qué se crean, cuándo sucede, dónde sucede, interrogantes que permiten evidenciar la afectación al desarrollo empresarial.

- ***Analizar el riesgo***

El análisis del riesgo es el estudio que permite identificar los activos críticos del sistema y las amenazas que ponen en riesgo la disponibilidad, confidencialidad e integridad, por lo tanto, el análisis del riesgo también es una sucesión de tareas que se deben cumplir, por lo que es necesario cuantificar y medir la responsabilidad del riesgo para saber que tan aceptable puede ser y aplicar medidas de intervención.

- ***Evaluar el riesgo***

Los riesgos se evalúan de forma cualitativa y cuantitativa, estimando la comparabilidad de los niveles de riesgos y los criterios de aceptación, lo que muestra como resultado una lista de vulnerabilidades y amenazas, haciendo énfasis en la prioridad del evento suscitado. Por lo tanto, el riesgo se determina mediante la esquematización del mapa de análisis del riesgo, esta matriz establece la probabilidad de ocurrencia en correspondencia con el impacto, dando como resultado el valor del riesgo a considerarse.

- ***Tratar el riesgo***

(Sierra Mafla & Gambasica Esquivel, 2020) señaló la definición del Instituto Colombiano De Normas Técnicas y Certificación como: "El tratamiento del riesgo, implica tener que elegir entre una o varias opciones, las cuales permitan corregir el riesgo y posteriormente poner en marcha la implementación. Durante esta etapa, es necesario aplicar un proceso cíclico". Es decir, que para gestionar y llevar a cabo el tratamiento de los riesgos es importante abarcar los siguientes aspectos:

- ✓ *Controlar:* aplicar medidas y acciones que permitan controlar su función en el activo.
- ✓ *Transferir o compartir:* eliminar el riesgo, es decir, contratar a una empresa especializada en el tema para que se responsabilice en reducirlo o eliminarlo.
- ✓ *Evitar:* se establecen acciones que permitan eliminar los posibles sucesos amenazantes.
- ✓ *Aceptar:* cuando no se está expuesto a que ocurra un nivel de incidencia alto, es decir, se trata de un riesgo leve por las actividades empresariales.

Metodologías de seguridad de la información

Las metodologías de gestión de seguridad de la información principalmente centradas en llevar el control de planificación para reducir y mitigar los posibles riesgos imperante sobre el activo. Existen muchas metodologías, pero las que se analizaran en este apartado son: MAGERIT y OCTAVE.

MAGERIT

Breve descripción de la metodología

El método Magerit se publicó en 1997, luego de un proceso de revisión y mejora en los sistemas de información, se desarrolla la segunda versión que apareció en el año 2005 y la última versión actualmente es la versión 3.0 que se publicó en el año 2012 (Villareal Ramos, 2018).

Magerit se define como: una metodología ejecutada para el análisis y gestión de riesgos desarrollada por el Consejo Superior de Gobierno Electrónico de España, que permite darse cuenta de que el gobierno y la sociedad en su conjunto dependen cada vez más de las tecnologías de la información para cumplir con su misión. Además esta metodología se integra con la herramienta PILAR (entorno de análisis y gestión de riesgos de un sistema de información) desarrollada por el Centro Criptológico Nacional, orientada a aquellas organizaciones que realizan funciones relativas a la seguridad de las tecnologías de la información y a la protección de los activos. Magerit proporciona cinco bases sistemáticas que garantizan seguridad: confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad (Rivera Anastacio & Valdivia Escobar, 2021). Esta metodología proporciona toda una documentación completa que recopila métodos y ejemplos sobre cómo llevar a cabo el análisis de los riesgos.

Magerit se fundamenta en analizar:

El impacto que una brecha de seguridad puede tener en la empresa tratando de identificar las amenazas que pueden afectar a la organización y las vulnerabilidades que pueden ser aprovechadas por las amenazas, para así lograr una definición clara de las acciones correctivas más adecuadas y las medidas preventivas que reducirán el riesgo.

Objetivos:

Magerit destaca a mantener objetivos como:

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.

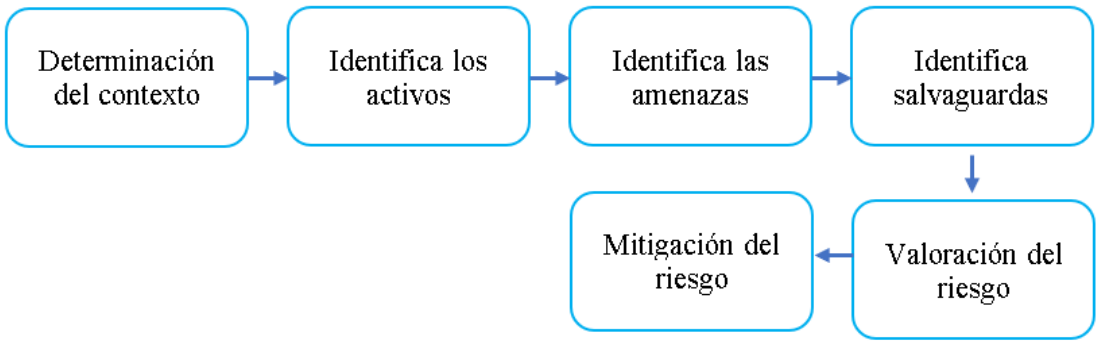
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
- Preparar a la organización para procesos de evaluación, auditoria, certificación o acreditación, según corresponda en cada caso (Campos Cruz & León Tesen, 2020).

Esta metodología dispone de una guía completa, que se divide en tres partes:

- **Libro I:** Métodos, define la estructura que debe llevar a cabo el modelo de gestión de los riesgos y se explica en detalle la metodología.
- **Libro II:** Guía de elementos, es una especie de inventario que utilizan las empresas para enfocar el análisis de riesgos; se agrupa por: tipos de amenazas, tipos de activos, tipos de recursos, de salvaguardas y políticas, dimensión y criterio de evaluación de riesgos.
- **Libro III:** Guía de técnicas, donde se describen las técnicas generales más importantes que son frecuentemente utilizadas para el análisis de riesgos (Cárdenas Luna, 2021).

Figura 1

Fases de la metodología Magerit



Fuente: Elaborado por Gissela Contreras, basado en (Miranda Jiménez, 2021)

El método de gestión de riesgos por Magerit

Para llegar a determinar el riesgo, el análisis y la gestión deben cumplir con los siguientes parámetros:

Fase1.-determinación del contexto, es un requisito de carácter obligatorio que permite definir los puntos estratégicos donde se va a llevar a cabo la mejora de la seguridad, se realiza una determinación de los parámetros internos que permiten desarrollar políticas que se seguirá para gestionar los riesgos. Un elemento a considerar es el alcance del análisis, incluyendo obligaciones propias, así como las relaciones con otras organizaciones, sean para intercambio de información y servicios o de servicios subcontratados.

Fase2.-Identifica los activos, permite identificar los activos más relevantes para la organización separándolos por grupos, de manera que se puedan analizar y conocer sus debilidades ante las amenazas expuestas.

Fase3.-Identifica las amenazas, determina a qué amenazas están expuestos aquellos activos y saber qué tipos de fenómenos existen capaz de vulnerar la información. El catálogo de elementos dispone de una guía de los diferentes tipos de amenazas y que la metodología establece para llevar a cabo el análisis de los riesgos.

Fase4.-Identifica salvaguardas, determina qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.

Fase5.-Valoración del riesgo, estima el impacto del riesgo definido como el daño hacia el activo derivado de la materialización de la amenaza, por lo que, determina si el impacto adquirido permite abordar hechos de debilidad o deficiencia en los sistemas. El riesgo se puede presentar de forma intrínseca (probabilidad de materialización de una amenaza), residual (después de los controles) o efectivo (inicial), por lo tanto, la valoración de riesgos se la puede denotar como irrelevante, bajo, medio, alto, extremo, según sea el efecto.

Fase6.-Mitigación del riesgo, evalúa el impacto ponderado del riesgo con la probabilidad de ocurrencia hacia el activo, facilitando la toma de decisiones con respecto al tratamiento y

mitigación de los riesgos, basándose en ello, se toman medidas de seguridad como la implementación de la metodología.

Después de determinar el impacto y los diversos riesgos a los que se enfrenta una organización, se toman varias decisiones dependiendo de los siguientes factores:

1. La severidad del impacto.
2. Obligaciones a las que legalmente se vincula la organización.
3. Obligaciones a la que la organización debe su posición.
4. Obligaciones a las que la organización está obligada contractualmente.

Desde el momento en que se toma la decisión, se dispone de medidas de seguridad para poder controlar principalmente las amenazas identificadas y, ante ellas, recurrir a:

- ✓ *Admitir el riesgo:* es poco probable que el riesgo suceda.
- ✓ *Transferir el riesgo:* la probabilidad es moderada.
- ✓ *Prevenir el riesgo:* es muy probable que ocurra (Hurtado Cruz, 2018).

OCTAVE

Breve descripción de la metodología

El Instituto de Ingeniería del Software (SEI) hizo partícipe la publicación de la metodología Octave (Evaluación de amenazas, activos y vulnerabilidades operativamente criticas) en 1999. Esta metodología fue desarrollada en Estados Unidos para el departamento de defensa, debido a los grandes dilemas de seguridad a los que se enfrentaba, trabajando juntamente con el Centro de Investigación de Telemedicina y Tecnología Avanzada (Santoja Lillo, 2019).

El objetivo primordial de Octave es que está orientada hacia los aspectos de riesgos operativos y a las prácticas de seguridad y no a la tecnología, esto significa que para que las empresas y organizaciones puedan tomar mejores decisiones con relación a la protección de la

información, con base a los principios de seguridad: confidencialidad, integridad y disponibilidad, la tecnología será sometida a examen de las diferentes prácticas de seguridad. Mediante su aplicación, el personal que labora en los departamentos de TI y áreas operativas, podrán trabajan conjuntamente por medio de talleres u hojas de trabajo acompañados por un especialista capacitado en el área. Esta metodología puede llegar a ser tediosa en algunos casos porque utiliza grandes volúmenes de documentos y además porque se necesita de un alto conocimiento técnico para su implementación (Holguín García & Lema Moreta, 2019).

Para (Silva Miranda & Álvarez Mayorga, 2019) "los procesos que realiza la metodología Octave comienzan con la evaluación de activos asociados a la información. Esto evalúa el nivel empresarial para luego tomar decisiones basadas en los riesgos potenciales encontrados".

Objetivos:

Octave persigue dos objetivos:

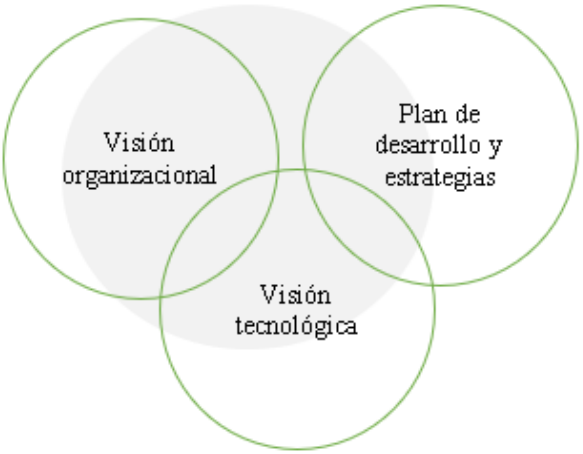
- Informar a la organización que la seguridad informática no es solo un tema técnico.
- Proporcionar estándares internacionales que rigen la implementación de medidas de seguridad para estos aspectos no técnicos.

Versiones de Octave

Hasta el momento, se han publicado 3 versiones de esta metodología: OCTAVE ORIGINAL, utilizada por grandes empresas, permite más de 300 trabajadores, OCTAVE-S, adaptado a pequeñas organizaciones, como las PYMES, con necesidades particulares más pequeñas, cuenta con alrededor de 100 empleados y, OCTAVE ALLEGRO, que permite el análisis de riesgos para mayor enfoque en fuentes de información, cada una de las cuales toma pasos específicos con alguna variación dependiendo de la necesidad (Tejena Macías, 2018).

Figura 2

Fases de la metodología Octave



Fuente: Elaborado por Gissela Contreras, basado en (Miranda Jiménez, 2021)

El método de gestión de riesgos por Octave

Fase1.-Visión organizacional, a nivel operativo, el personal que labora dentro de la compañía, podrá recabar información de todas las áreas que conforman la organización, identificar activos importantes, especialmente los de gran valor y que forman parte de la empresa, identificar los principales perfiles de amenazas, los posibles motivos de preocupación y las estrategias con las que cuente la empresa en ese momento.

Fase 2.-Visión tecnológica*,* engloba todas las vulnerabilidades técnicas, tanto lógicas como física que degradan al activo, los componentes claves que conforman la infraestructura tecnológica, en esta fase, se evalúa toda la infraestructura tanto tecnológica como física que soportan los activos que contienen información, así mismo, se analizan e identifican amenazas y vulnerabilidades.

Fase 3.-Plan de desarrollo y estrategias, esta última fase evalúa todas las amenazas y vulnerabilidades, se identifican y analizan los riesgos efectivos (iniciales) más relevantes y con

mayor incidencia. Para aquellos riesgos más críticos se deberá desarrollar un conjunto de planes de mitigación que permitan disminuir el nivel de riesgo asociado al activo.

Aplicación de las metodologías para el análisis de riesgos

En la actualidad, uno de los factores más importantes que se debe proteger en todo tipo de organizaciones es la seguridad de la información, por lo que esta, es almacenada, procesada y compartida, motivo por el cual, están sometidas a potenciales amenazas. Con base a aquello, surge la necesidad de determinar qué metodologías minimizan los efectos indeseables.

Existen una serie de activos dentro de las organizaciones que se encuentran a posibles amenazas y vulnerabilidades que generan un potencial impacto significativo en el funcionamiento empresarial, por lo que compromete a la afectación de la integridad de la información y en el desarrollo dentro del mercado empresarial competitivo, los siguientes activos con los que cuenta una organización se encuentran expuestos en la siguiente tabla:

Tabla 1

Parámetros aplicados a las metodologías de análisis de riesgos

ACTIVOS	AMENAZAS	VULNERABILIDADES
Personal	Enfermedades	Falta de atención a la salud del personal.
Equipos de computo	Deficiencia de mantenimiento	Falta de mantenimiento preventivo.
Servicios	Filtración de datos	Explotación de los servicios.
Redes de comunicaciones	Perdida de comunicación	Deficiencia de planes de contingencia.
Servidores	Hacker	Brechas de seguridad abiertas.
Documentación	Inundaciones, perdida de información	Falta de un estado de alarma que indique la existencia del riesgo.
Internet	Pérdida de conexión	Falta de seguridad hacia las redes externas.
Antivirus	Virus	Falta de programas de antivirus.

Fuente: Elaborado por Gissela Contreras

Los parámetros anteriores hacen referencia al análisis de riesgo y deben evaluarse bajo los criterios de medición dependiendo de la metodología. Por ejemplo, en la valoración de los activos,

se dan de acuerdo al valor que categorice el impacto: muy alta, alta, media, baja, muy baja. Con respecto a las vulnerabilidades que puedan mostrar los activos, se permite medir el nivel de incidencia cuantificándolo en una escala numérica: extremadamente frecuente (5), muy frecuente (4), frecuente (3), frecuencia normal (2), poco frecuente (1). En la siguiente tabla se denota el criterio de daños que puede tener la organización.

Tabla 2

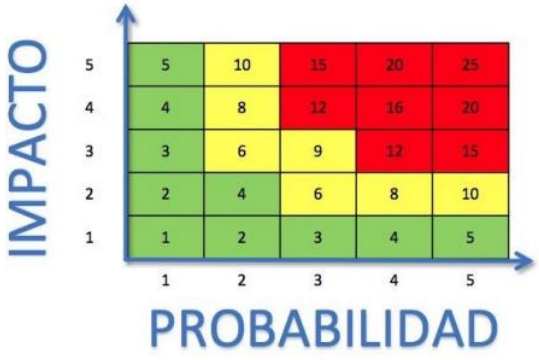
Valoración del riesgo

Valoración cualitativa	Valoración cuantitativa	Criterio
Muy baja	1	Daño irrelevante para la organización
Baja	2	Daño bajo para la organización
Media	3	Daño medio para la organización
Alta	4	Daño grave para la organización
Muy alta	5	Daño muy grave para la organización

Fuente: Elaborado por Gissela Contreras, basado en (Recalde Caicedo, 2019)

Figura 3

Mapa de valoración del riesgo



Fuente: Figura tomada de (Tamayo Reinel, 2020)

Generalmente para calcular el valor del riesgo se denota la función: impacto de la amenaza por la probabilidad de incidencia, muchas veces los resultados muestran la relación costo-beneficio, que es asignar recursos que permitan evitar pérdidas asociadas a los riesgos identificados.

Los parámetros anteriores fueron utilizados en la aplicación de las metodologías: MAGERIT y OCTAVE, cabe destacar que las dos metodologías están enfocadas al mismo objetivo de gestionar los riesgos, pero con diferentes variaciones en sus procedimientos. Con el fin de identificar cuál es la metodología que proporcione la mejor toma de decisiones en cuanto a los activos de información ante los riesgos inminentes, en la **Tabla 3**, se evalúan los diferentes criterios de acuerdo a su funcionamiento.

Tabla 3

Criterios de funcionamiento de las metodologías

Análisis de riesgos		**Magerit**	**Octave**
Análisis	Cualitativo	✓	-
	Cuantitativo	✓	-
Objetivos de seguridad	Confidencialidad	✓	✓
	Disponibilidad	✓	✓
	Integridad	✓	✓
	Trazabilidad	✓	
	Autenticidad	✓	
Riesgos	Intrínseco	✓	
	Residual	✓	
	Efectivo	✓	✓
Elementos de seguridad	Activos	✓	✓
	Vulnerabilidades	✓	✓
	Amenazas	✓	✓
	Salvaguardas	✓	✓
Implementación	Herramienta	✓	

Fuente: Elaborado por Gissela Contreras

En esta tabla se evidencia el funcionamiento que tiene cada una de las metodologías de acuerdo al análisis de riesgo: MAGERIT y OCTAVE, sus parámetros fueron recopilados durante el desarrollo de las mismas, mediante conceptualizaciones, fases y procesos que permitan identificar cual metodología cumple con parámetros completos y genere mayor confianza para la

reducción de los riesgos. MAGERIT en cierta medida, se considera como la metodología principal para el análisis de riesgos más detallado, teniendo en cuenta los principales objetivos de seguridad para la misión de una organización, así como algunos detalles adicionales en cuanto a su funcionamiento y que no permite ilegalidad del personal analista.

METODOLOGÍAS APLICADAS PARA LA RECOLECCIÓN DE INFORMACIÓN

El presente caso de estudio tiene enfoque cualitativo, basado en teorías como soporte a la elaboración de la investigación.

Modalidad de investigación

Investigación bibliográfica

Se optó por implementar la investigación bibliográfica, la cual me permitió acceder a diversas fuentes de información, tomadas de internet, con el objetivo de poder definir con bases sólidas y conceptos competentes las metodologías comprometidas en esta investigación, y con el propósito de recabar y sintetizar información de investigaciones y teorías ya existentes.

Tipo de investigación

Investigación descriptiva

La implementación de la investigación descriptiva me permitió contribuir a la descripción de cada uno de los componentes característicos y comprender mejor las principales temáticas de estudio.

Metodología de investigación

Método analítico

Considerando estudiar los elementos por fragmentos separados para su respectivo análisis como parte del desarrollo de la investigación a comparar, se decidió implementar el método

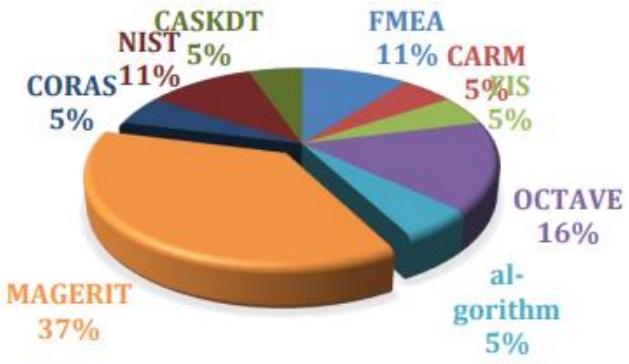
analítico, el cual me permitió descomponer la información, realizando un análisis reflexivo sobre los fundamentos conceptuales obtenidos y posteriormente a la obtención de las conclusiones.

COMPARATIVA ENTRE LAS METODOLOGÍAS MAGERIT Y OCTAVE

Abordando la revisión metódica de las bibliografías, un estudio realizado en el año 2020, se basó en la obtención de información a través de una revisión sistemática de la literatura, donde se pretendió determinar cuál era la metodología más utilizada para el análisis y la gestión de los riesgos, hecho que corroboró en el siguiente detalle visual, producto de la elaboración del RSL (Revisión Sistemática de la Literatura).

Figura 1

Principales metodologías para el análisis y la gestión de los riesgos



Fuente: Figura tomada de (López Rimari, 2020)

En la figura anterior se pueden visualizar las numerosas metodologías existentes y las cuales son usadas para el análisis y la gestión de los riesgos; para el citado autor, la metodología más empleada en el estudio obtenido es MAGERIT con un 37% y luego está OCTAVE con un 16%, y posteriormente se encuentran las demás metodologías.

Cabe señalar que el uso de MAGERIT es imprescindible en las organizaciones porque emplean procesos y criterios de seguridad que permiten abordar los riesgos críticos que puede poseer ciertas

organizaciones, pero también, hay que resaltar que OCTAVE es la segunda metodología más utilizada para los procesos de riesgos.

Cuadro general de la comparativa entre las metodologías de gestión de riesgos Magerit-Octave

Tabla 4

Criterio de comparación en las metodologías MAGERIT-OCTAVE

Completo Medio Nada

Análisis de riesgos		**Magerit**	**Octave**
Análisis	Cualitativo		
	Cuantitativo		
Objetivos de seguridad	Confidencialidad		
	Disponibilidad		
	Integridad		
	Trazabilidad		
	Autenticidad		
Riesgos	Intrínseco		
	Residual		
	Efectivo		
Elementos de seguridad	Activos		
	Vulnerabilidades		
	Amenazas		
	Salvaguardas		
Implementación	Herramienta		

Fuente: Elaborado por Gissela Contreras

Características de las metodologías Magerit-Octave

MAGERIT conlleva una amplia visión con respecto al análisis y la gestión de los riesgos, centrándose en los aspectos más importantes de la organización, ya sean estos, operacionales, financieros, legales o de personal, manteniendo un enfoque interno y externo en la evaluación de los diferentes activos. OCTAVE se enfoca a las prácticas de seguridad y a la toma de decisiones

en relación con la protección de datos, también cubre los riesgos organizacionales y se enfoca en temas estratégicos relevantes para la práctica.

La metodología MAGERIT opera basándose en su herramienta implementada PILAR que facilita la identificación y gestión del manejo de los riesgos, clasificándolos por su orden de afectación, y por lo que permite dar ese gran paso a una certificación por las estandarizaciones ISO. OCTAVE es una metodología autodirigida y flexible, es decir, que puede ser usado por el personal de trabajo para evaluar los riesgos internos dentro de la organización, se basan en la realización de talleres u hojas de trabajo que permiten realizar los procesos paso a paso, pero, muchas veces esto puede resultar tedioso.

El propósito de MAGERIT es contribuir a la división de cada uno de sus activos, motivo por el cual permite a las organizaciones agrupar los numerosos riesgos existentes. En cambio, OCTAVE coopera en la planificación previa de la seguridad, basado en las incidencias de los diferentes riesgos, por lo que, se apoya en la planificación interna que se le hace a la empresa para detectar activos críticos y luego poder asociarlo a un plan de mejora.

Fortalezas y debilidades Magerit-Octave

Tabla 5

Fortalezas y debilidades

Fortalezas	Debilidades	Bibliografía
▪ Proporciona una forma sistemática de identificar riesgos en los Sistemas de Información. ▪ Se puede usar libremente sin autorización para su uso. ▪ Herramienta PILAR ▪ Utiliza un completo análisis cualitativo y cuantitativo. ▪ Usado en pequeñas, medianas y grandes empresas.	▪ El único inconveniente de esta metodología es el alto costo de implementación, ya que el activo se convierte en valor económico.	(Santoja Lillo, 2019)

Fuente: Elaborado por Gissela Contreras

Tabla 6

Fortalezas y debilidades

Fortalezas	Debilidades	Bibliografía
▪ Los cambios iniciales durante el desarrollo del proyecto son más económicos. ▪ Gratis para uso interno. ▪ Compromete al personal de la organización. ▪ Es completa de acuerdo a los procesos, activos, amenazas, vulnerabilidades y salvaguardas.	▪ Solo puede ser implementado por pequeñas y medianas empresas (PYMES) ▪ Costoso para uso externo: Licencia SEI (Instituto de Ingeniería del software)	(Freire Silva & López Sevilla, 2022)

Fuente: Elaborado por Gissela Contreras

CONCLUSIONES

Las dos metodologías vanguardistas creadas específicamente para realizar los procesos de análisis de riesgos son el soporte básico en el contexto del análisis y la gestión de los riesgos, es sustancial que las empresas comiencen a utilizar estas herramientas como medidas de prevención, mediante la creación de planes de contingencia a las posibles amenazas expuestas, y a la continuidad del desarrollo empresarial.

En respuesta al cuadro comparativo general, la metodología MAGERIT cumple funciones muy completas con base al tipo de análisis, objetivos de seguridad, tipos de riesgos, elementos de la metodología e implementación, lo que la hace una metodología robusta para el análisis y gestión de riesgos, al contrario, la metodología OCTAVE no cumple con parámetros prioritarios que satisfagan al desarrollo empresarial como tal y, por lo tanto, muchas veces no puede llegar a ser atractiva para ciertas organizaciones que requieran implementar medidas de seguridad más completas y sujetas a sus necesidades.

Al mismo tiempo, puedo acotar que las características, fortalezas y debilidades marcan un precedente en su uso, ya que muchas empresas se orientan más por una metodología que cumpla con los estándares completos de seguridad para llevar a cabo el alcance de la gestión de los riesgos.

En síntesis, pude deducir que basándome en las diferentes fuentes bibliográficas obtenidas, la metodología MAGERIT a diferencia de OCTAVE, se destaca como la primera metodología a escoger, puesto que, los diferentes activos críticos que dispone una organización, permiten una aproximación más objetiva a los niveles de riesgos y los puntos de inexactitud. A pesar de que las dos metodologías tienen su ámbito de aplicación, debido a que una organización las utiliza más que otras, todas dos pueden ser empleadas en empresas, tanto públicas como privadas.

BIBLIOGRAFÍA

Campos Cruz, C. Y., & León Tesen, D. D. (2020). *Comparativa de las metodologías Magerit y Octave, para determinar la más adecuada en la gestión de riesgos de tecnologías de información en la Unidad de Red Telemática de la Universidad Nacional Pedro Ruiz Gallo [Tesis Ingeniero en Sistemas].* Repositorio Institucional, Universidad Nacional Pedro Ruiz Gallo. https://hdl.handle.net/20.500.12893/8244

Cárdenas Luna, N. (2021). *Estudio comparativo de metodologías de aseguramiento para un servidor local y un servicio en la nube [Monografia en Especialista en Seguridad Informática, Universidad Nacional Abierta y a Distancia UNAD].* Repositoio Universitario UNAD. https://repository.unad.edu.co/handle/10596/42056

Freire Silva, J. E., & López Sevilla, G. M. (2022). *Metodología para mitigar vulnerabilidades de almacenamiento mediante inteligencia de fuentes abiertas (OSINT) en la EEASA[Proyecto de Investigación de Magisterr en Ciberseguridad, Pontificia Universidad Católica del Ecuador].* Repositorio PUCESA. https://repositorio.pucesa.edu.ec/handle/123456789/3528

Guerrero Aguiar, M., Medina León, A., & Nogueira Rivera, D. (2020). Procedimiento de gestión de riesgos como apoyo a la toma de decisiones. *Ingeniería Industrial, 41*(1). http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1815-59362020000100002&lng=es&tlng=es

Holguín García, F. Y., & Lema Moreta, L. M. (2019). Modelo para Medir la Madurez del Análisis de Riesgo de los Activos de Información en el contexto de las Empresas Navieras. *Revista Ibérica de Sistemas e Tecnologias de Informação*(31), 1-17. https://doi.org/DOI: 10.17013/risti.31.1–17

Hurtado Cruz, M. L. (2018). Gestion de riesgo, metodologías Magerit y Octave. *Repositorio de la Universidad Piloto de Colombia, 80*. http://polux.unipiloto.edu.co:8080/00004420.pdf

López Rimari, R. P. (2020). *Metodologías para el análisis de riesgo de la seguridad de la información. Una revisión sistemática de la literatura[Tesis de Grado en Académico de Bachiller en Ingeniería de Sistemas, Universidad Peruana Unión].* Repositorio de Tesis, Universidad Peruana Unión. http://hdl.handle.net/20.500.12840/3699

Miranda Jiménez, J. N. (2021). *Mapeo sistemático de metodologías de Seguridad de la Información para el control de la gestión de riesgos informáticos[Tesis de Grado en Ingeniera en Sistemas, Universidad Politécnica Salesiana Sede Guayaquil].* Repositorio Institucional de la Universidad Politécnica Salesiana . http://dspace.ups.edu.ec/handle/123456789/20966

Recalde Caicedo, J. P. (2019). *Plan de implementación de un SGSI y aplicación de controles críticos en el centro de operaciones de seguridad en la empresa GMS[Tesis en Ingeniera en Sistemas Informáticos y de Computación, Escuela Politécnica Nacional].* Repositorio Digital - EPN, Escuela Politécnica Nacional. http://bibdigital.epn.edu.ec/handle/15000/20530

Rivera Anastacio, D. K., & Valdivia Escobar, J. H. (2021). 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. *[Tesis en Ingeniero en Ssitemas]*. Repositorio Institucional UNHEVAL. https://hdl.handle.net/20.500.13080/7066

Santoja Lillo, J. (2019). *Análisis y correlación entre probabilidad e impacto de los riesgos[Trabajo Fin de Máster en Ciberseguridad, Universidad de Alicante]*. Repositorio Institucional de la Universidad de Alicante. http://hdl.handle.net/10045/93271

Sierra Mafla, S., & Gambasica Esquivel, A. (2020). *Análisis y plan de tratamiento de riesgos para los activos de información del cuerpo de bomberos voluntarios de Tunja[Tesis de Grado en Contador P´úblico, Universidad Santo Tomás]*. Repositorio Institucional CRAIUSTA, Universidad Santo Tomás. https://doi.org/http://dx.doi.org/10.15332/tg.pre.2020.00183

Silva Miranda, O., & Álvarez Mayorga, E. H. (2019). *Auditoría Informática aplicando la metodología OCTAVE de los procesos de recaudaciones y permisos en el Gobierno Autónomo Descentralizado (GAD) de San Pedro de Pelileo[Tesis en Ingeniero en Sistemas Computacionales e Informáticos]*. Repositorio Digital, Universidad Técnica de Ambato. https://repositorio.uta.edu.ec/jspui/handle/123456789/30111

Tamayo Reinel, J. A. (2020). *Adaptación de una Metodología Para el Análisis y Gestión de Riesgos Informáticos Para Organizaciones del Sector Salud en Colombia[Tesis de Grado en Magister en Gestión de Tecnología de Información, Universidad Nacional Abierta y a Distancia]*. Repositorio UNAD, Universidad Nacional Abierta y a Distancia . https://repository.unad.edu.co/handle/10596/35868

Tejena Macías, M. (2018). Análisis de riesgos en seguridad de la información. *Revista Científico-Académica Multidisciplinaria*, *3*(4). https://doi.org/10.23857/pc.v3i4.809

Villareal Ramos, V. B. (2018). *Comparación de metodologías para auditoría informática: Caso de estudio detección de valores anómalos para la prevención de fraudes [Tesis de Ingeniera en Contabilidad y Auditoria, Universidad Central del Ecuador]* . Repositorio Digital de la Universidad Central del Ecuador. http://www.dspace.uce.edu.ec/handle/25000/17628

ANEXOS

Anexo 1

Guía de evaluación de criterios

Nº	Criterios a evaluar	Si	No	Comentarios
1	¿Se hizo énfasis en las fases y procesos que abarca cada metodología?	X		Se señalaron aspectos importantes sobre los procesos de gestión de riesgos de cada una de las metodologías.
2	¿Estas metodologías son accesibles para las organizaciones?	X		Son herramientas de fácil acceso para diversas organizaciones.
3	¿Las metodologías tienen un alto costo en su implementación?	X		Octave requiere de una licencia para uso externo y Magerit tiene un alto costo de implementación sobre el activo crítico.
4	¿Estas metodologías eliminan al 100% los riesgos?		X	Las metodologías nombradas implementan un plan de mitigación para reducir y tratar el riesgo, más no los elimina.
5	¿Ambas metodologías son implementadas en las PYMES?	X		El uso de estas metodologías es que pueden ser implementadas sin problema alguno sobre las PYMES.

Fuente: Elaborado por Gissela Contreras