EDITORIAL GRUPO AEA

FORTALECIMIENTO METODOLÓGICO DE LA SEGURIDAD INFORMÁTICA EN POSGRADOS: ANÁLISIS Y ESTRATEGIAS DE MEJORA

Juan Antonio Picoy Gonzales
Rosaura Huarcaya Taype
Omar Hans Contreras Canto
Amanda Omonte Vilca

Fortalecimiento Metodológico de la Seguridad Informática en Posgrados: Análisis y Estrategias de Mejora.

Autor/es:

Picoy-Gonzales Juan Antonio

Huarcaya-Taype Rosaura

Contreras-Canto Omar Hans

Omonte-Vilca Amanda

© Publicaciones Editorial Grupo AEA Santo Domingo – Ecuador
Publicado en: https://www.editorialgrupo-aea.com/
Contacto: +593 983652447; +593 985244607 **Email**: info@editorialgrupo-aea.com

Título del libro:

Fortalecimiento Metodológico de la Seguridad Informática en Posgrados: Análisis y Estrategias de Mejora

Libro Producto de Investigación Científica

Libro Digital, Primera Edición, 2023
Editado, Diseñado, Diagramado y Publicado por Comité Editorial del Grupo AEA, Santo Domingo de los Tsáchilas, Ecuador, 2023

ISBN: 978-9942-651-12-9

https://doi.org/10.55813/egaea.l.2022.56

Como citar: Picoy-Gonzales, J. A., Huarcaya-Taype, R., Contreras-Canto, O. H. & Omonte-Vilca, A. (2023). Fortalecimiento Metodológico de la Seguridad Informática en Posgrados: Análisis y Estrategias de Mejora. Primera edición. Editorial Grupo AEA. Ecuador. https://doi.org/10.55813/egaea.l.2022.56

Palabras Clave: Amenazas, Impacto, Salvaguardas.

Cada uno de los textos de Editorial Grupo AEA han sido sometido a un proceso de evaluación por pares doble ciego externos (double-blindpaperreview) con base en la normativa del editorial.

Revisores:

Ing. Francisco Marcelo Ramos Secaira, Mgs. — Pontificia Universidad Católica del Ecuador

Ing. Alex Fernando Erazo Luzuriaga, Mgs — Escuela Superior Politécnica de Chimborazo

Los libros publicados por **"Editorial Grupo AEA"** cuentan con varias indexaciones y repositorios internacionales lo que respalda la calidad de las obras. Lo puede revisar en los siguientes apartados:

Editorial Grupo AEA

http://www.editorialgrupo-aea.com

Editorial Grupo AeA

editorialgrupoaea

Editorial Grupo AEA

Aviso Legal:

La información presentada, así como el contenido, fotografías, gráficos, cuadros, tablas y referencias de este manuscrito es de exclusiva responsabilidad del/los autor/es y no necesariamente reflejan el pensamiento de la Editorial Grupo AEA.

RESEÑA DE AUTORES

AUTORES

Picoy-Gonzales Juan Antonio

Universidad Nacional de Huancavelica

antonio.picoy@unh.edu.pe

https://orcid.org/0000-0003-0372-6328

Formación profesional en ciencias de la educación, ingeniería de sistemas e informática y traductor de idiomas; reconocido como docente investigador CONCYTEC por la producción de diversos artículos científicos, autor de registro de marca y diseñador industrial a nivel INDECOPI; con experiencia en docencia a nivel universidad, instituto y educación básica regular estando asignado en diferentes programas de estudios de ciencias de la salud y de ciencias de la educación; ocupando cargos como: director de gestión académica, procesos de autoevaluación con fines de acreditación de programas profesionales, miembro de comité de múltiples programas profesionales, director de unidad de calidad, consultor en procesos de calidad, licenciamiento de universidades y procesos de acreditación, director de gestión de calidad.

Huarcaya-Taype Rosaura

Universidad Nacional de Huancavelica

rosaura.taype@unh.edu.pe

https://orcid.org/0009-0002-4803-021X

Formación profesional en ciencias empresariales con especialidad en administración a nivel pregrado, a nivel postgrado gestión pública, y con estudios de doctorado en ciencias de la Educación, así como contar con 2 diseñados industriales a nivel INDECOPI; con experiencia en docencia a nivel universidad pública y trabajos en entidades públicas y privadas.

RESEÑA DE AUTORES

AUTORES

Contreras-Canto Omar Hans

Universidad Nacional Hermilio Valdizan

ocontreras@unheval.edu.pe

https://orcid.org/0000-0002-4871-0912

Catedrático en la Escuela Profesional de Educación Física, Doctor en Ciencias de la Educación, Magíster en Investigación e Innovación Pedagógica, Título de Segunda Especialidad Profesional en Informática Educativa, Licenciado en Educación Física. Adscrito al Departamento Académico Pedagógico de Ciencias Sociales y Humanidades de la Facultad de Ciencias de la Educación de la Universidad Nacional Hermilio Valdizán de Huánuco, Perú. En la actualidad, es docente de la Escuela Profesional de Educación Física. Asimismo, dicta los cursos de Competencias en Investigación Científica, Tesis I y Tesis II en la Escuela de Posgrado de la UNHEVAL. Ha sido Director de la Biblioteca Central de la UNHEVAL por un año. Cuenta con publicaciones en revistas científicas y libros de Educación Física, asimismo, tiene participaciones en diferentes congresos nacionales e internacionales (participante, ponente y comunicaciones).

Omonte-Vilca Amanda

Universidad Nacional Hermilio Valdizan

aomonte@unheval.edu.pe

https://orcid.org/0009-0001-6090-1826

Formación profesional en Ciencias de la Educación con especialidad en Educación Inicial a nivel pregrado, con estudios en postgrado con mención en Gestión y Planeamiento Educativo con grado de doctor en Ciencias de la Educación, además de contar con experiencia en proyectos como: Influencia de la metodología activa en el rendimiento escolar, relación entre hábitos de lectura y la comprensión lectora en los estudiantes, gestión de calidad educativa y actitud del docente, predominancia de los cuadrantes cerebrales y sus repercusiones en el aprendizaje de los estudiantes, enseñanza de la filosofía, estilos de aprendizaje y rendimiento académico, entre otros.

Índice

Índice de Tablas

Índice de Figuras

Introducción

En la actualidad, las instituciones de educación superior y posgrado no se escapan de esta realidad; por lo que deben de estar en constante renovación de las tecnologías utilizadas para el proceso de enseñanza aprendizaje. Los alumnos, docentes y personal administrativo de las instituciones que brindan servicios de enseñanza de posgrado, necesitan de tecnologías de información y comunicación que sean confiables y actualizados. El equipamiento en las instituciones de posgrado con aulas de cómputo y redes de internet, obligan al docente sistemáticamente a reaccionar ante la necesidad de utilizar los recursos disponibles y empiezan a interactuar con sus alumnos tanto en la parte académica como administrativa.

En la Escuela de posgrado de la Universidad Nacional Hermilio Valdizán, en el semestre académico 2016 - I se contaba con mil doscientos alumnos matriculados y el semestre académico 2017 - I con 1475 alumnos matriculados; este incremento preocupó a las autoridades y equiparon más aulas con computadores y puntos de acceso a internet; pizarras interactivas y proyectores multimedia. También se incrementaron equipos de cómputo para las labores administrativas; pero hasta allí nomas. Lo que no se tomó en cuenta es la seguridad; por lo que hasta la actualidad no existe es un análisis de riesgo de la seguridad de toda la información académica y administrativa; y mucho menos una propuesta de mejora.

La realidad que presenta la Escuela de Post Grado es preocupante debido a que se presentan casos de extravío y/ o pérdida de recursos, algunas veces la información supuestamente transmitida por los alumnos, docentes y personal administrativo no es la misma que recibe el destinatario o no llega al destinatario, o llega a la persona equivocada; causando incumplimiento de las tareas académicas, funciones laborales y obligaciones al no entregar sus trabajos o la información a tiempo. Esto genera mal clima laboral e incomodidad de las personas que estudian y que laboran en la escuela de posgrado; por ende, es importante que toda organización pública tenga políticas de seguridad de los sistemas de información.

CAPITULO 1

EL PROBLEMA, SU IMPORTANCIA Y MARCO TEÓRICO

El problema, su importancia y marco teórico

Actualmente, vivimos un ritmo de vida con la constante estimulación de lo nuevo, práctico y funcional que podemos observar en todos los ámbitos del desarrollo y de nuestra vida: transporte, vivienda, comunicaciones, servicios, medicina y educación, que ya sea formal o escapa informalmente a este constante bombardeo de ciencia y tecnología aplicada a la vida moderna.

Las instituciones que ofrecen servicios de educación superior y de posgrado no escapan a esta realidad; Por lo tanto, las tecnologías utilizadas para el proceso de enseñanza-aprendizaje deben renovarse constantemente. El estudiante, los profesores y el cuerpo administrativo de las instituciones que ofrecen servicios de educación de posgrado necesitan tecnologías de información y comunicación confiables y actualizadas. El equipamiento de las instituciones de educación superior con laboratorios de computación y redes de Internet obliga a los profesores a reaccionar sistemáticamente ante la necesidad de utilizar los recursos disponibles y comenzar a interactuar con sus estudiantes tanto académica como administrativamente.

La Escuela Superior de la Universidad Nacional Hermilio Valdizán, en el semestre académico 2016-I hubo 1.200 alumnos matriculados y en el semestre académico 2017-I con 1.475 alumnos matriculados; Este incremento ha preocupado a las autoridades, quienes han equipado más aulas con computadoras y puntos de acceso a Internet; pizarras interactivas y proyectores multimedia. También se ha incrementado el equipamiento informático para tareas administrativas; pero hasta entonces nomas. Lo que no se ha tenido en cuenta es la seguridad; Porque lo que hoy no existe es un análisis de los riesgos de seguridad de toda la información académica y administrativa; mucho menos una propuesta de mejora.

La realidad que presenta la Escuela de Doctorado es preocupante, pues existen casos de pérdida y/o malversación de recursos, en ocasiones la información supuestamente transmitida por estudiantes, profesores y personal administrativo no es la misma que recibe el destinatario o no. destinatario, o llega a la persona

equivocada; haciendo que pierda tareas académicas, asignaciones y obligaciones al no entregar su trabajo o información a tiempo. Esto genera un mal ambiente laboral y malestar para las personas que estudian y trabajan en la educación superior; por ello es importante que todas las organizaciones públicas cuenten con políticas de seguridad de los sistemas de información.

En este sentido, el posgrado presenta vulnerabilidades, quebrantando la seguridad de la información, atacando su confidencialidad, integridad y disponibilidad. Si no se realiza un análisis para proteger los recursos del programa de posgrado, considerando la información como el activo más importante; Lo más probable es que se enfrenten a una situación en la que la entrega de un documento digital sea de extrema importancia o en tiempo y termine siendo dañado, causándoles serios problemas, que van desde faltas y despidos docentes hasta sanciones. personal administrativo, administrativo, además de un ambiente de trabajo caótico.

Por tal motivo, se tiene previsto determinar la metodología a utilizar para analizar y proponer mejoras en la seguridad de los sistemas de información en la escuela de doctorado de la UNHEVAL, para lo cual únicamente se ha tenido en cuenta la metodología MAGERIT y la metodología OCTAVE en el análisis de riesgo para optimizar la información. seguridad mediante la aplicación de la metodología adecuada. La aplicación del análisis de riesgos a través de estas metodologías nos permitirá evaluar la seguridad de nuestros sistemas, cuantificar y comparar los requisitos de seguridad de la información, determinar los activos y sus características de mayor valor, teniendo en cuenta los criterios ACID (autenticación, confidencialidad, integridad, disponibilidad y no repudio), identificar las salvaguardas existentes, las amenazas, su origen y el tipo de vulnerabilidad que puede afectar la estimación y evaluación de los impactos, concluyendo con la evaluación de los riesgos a los que están expuestos los bienes de la Escuela de Doctorado.

1.1. Objetivo general

Determinar la mejor metodología para el análisis de riesgo y propuesta de mejora en la Escuela de posgrado de la Universidad Nacional Hermilio Valdizan.

1.1.1. Objetivos específicos

- Determinar la mejor metodología que identifica las amenazas en el análisis de riesgo en la Escuela de posgrado.
- Determinar la mejor metodología que identifica las vulnerabilidades en el análisis de riesgo en la Escuela de posgrado.
- Determinar la mejor metodología que identifica los impactos en el análisis de riesgo en la Escuela de posgrado.
- Describir la propuesta de mejoras en la seguridad de la Información de la escuela de posgrado.

1.2. Hipótesis

1.2.1. Hipótesis general

MAGERIT es la mejor metodología para el Análisis de riesgo y proponer mejoras en la Escuela de posgrado de la Universidad Nacional Hermilio Valdizán.

1.2.2. Hipótesis específicas

- MAGERIT es la mejor metodología que identifica las amenazas en el análisis de riesgo en la Escuela de posgrado.
- MAGERIT es la mejor metodología que identifica las vulnerabilidades en el análisis de riesgo en la Escuela de posgrado.
- MAGERIT es la mejor metodología que identifica los impactos en el análisis de riesgo en la Escuela de posgrado.

La aplicación de la propuesta de mejora en la seguridad de la Información de la escuela de posgrado mejorará la seguridad de la Información.

1.3. Marco teórico

La Escuela de Posgrado de la Universidad Nacional Hermilio Valdizán de Huánuco no cuenta con políticas de seguridad y mecanismos de resguardo capaces de gestionar los riesgos a los que se encuentran expuestos sus más

valiosos activos, como Escuela de Posgrado en proceso de acreditación, ha desarrollado sus actividades encaminadas a mejorar la calidad de la educación, parte de ella involucra la evaluación de la seguridad de la información, la protección y el desempeño efectivo de los activos para evitar la duplicidad de actividades. Adecuada y oportuna toma de decisiones y uso eficaz y eficiente de la información a través del análisis de riesgos.

1.4. Análisis de riesgo

Identificación de amenazas a o relacionadas con varios componentes del sistema de información (conocidos como "activos"); determinar la vulnerabilidad del sistema frente a estas amenazas y evaluar el impacto o el alcance de los daños en la organización por falta de seguridad mediante la obtención de información sobre el riesgo desencadenado (MAGERIT, 1997).

1.4.1. Razones para realizar el análisis de riesgos

Actualmente, existen motivos para aplicar el análisis de riesgos en todo tipo de organizaciones, ya que es una técnica que, entre otras cosas permite:

- Identificar los activos y controles de seguridad.
- Gestionar las alertas de los riesgos próximos.
- Identificar la necesidad de acciones correctivas.
- Proporcionar una guía de cara a los gastos de recursos.
- Relacionar el programa de control con la misión de la organización.
- Proporcionar criterios para diseñar y evaluar planes de contingencia y continuidad de negocios.
- Mejorar la concienciación global sobre la seguridad a todos los niveles.

1.4.2. Tipos de análisis de riesgos

Existen dos enfoques principales para realizar una evaluación de riesgos completa, uno cuantitativo y otro cualitativo.

1.4.2.1. Enfoque cualitativo

Un enfoque cualitativo del análisis de riesgos es muy común en estos días, especialmente en las nuevas firmas de consultoría de seguridad que se especializan en seguridad lógica, firewalls, pruebas de penetración y similares. Es mucho más simple e intuitivo que el cuantitativo porque no implica probabilidades exactas, sino simplemente estimaciones de posibles pérdidas. El método o enfoque cualitativo es más adecuado para instalaciones más pequeñas y es el más utilizado en la actualidad. Se pueden medir algunos parámetros:

Riesgo de peligros utilizando escalas tales como alto, medio, bajo. • Gravedad de la epilepsia basada en escalas como 1, 2, 3. • Daño utilizando escalas como: esencial, crítico, importante, conveniente, informativo. No se requieren datos de probabilidad para este análisis, solo se utiliza el daño potencial estimado. En lugar de números concretos, utilice métricas más matizadas para los valores de los activos, la frecuencia de las amenazas y la eficacia del control. Utiliza un conjunto de elementos interrelacionados tales como:

- Amenazas
- vulnerabilidades
- Control S. Hay cuatro tipos de controles

Desalientos Reducen la probabilidad de un ataque intencional. Controles preventivos. Protegen las vulnerabilidades y frustran un ataque o reducen su impacto. Controles correctivos. Reducir el impacto del ataque. control de investigacion Detectan ataques e implementan controles proactivos, también conocidos como proactivos o correctivos, así como reactivos. Con la ayuda de estos cuatro elementos, obtenemos un indicador cualitativo del nivel de riesgo asociado con un determinado activo en la organización, que se considera como la probabilidad de que la amenaza para el activo se materialice y tenga un efecto determinado.

1.4.2.2. Enfoque cuantitativo

El enfoque cuantitativo es, con mucho, el menos utilizado porque en muchos casos implica cálculos complejos o datos difíciles de estimar. Se basa en dos

parámetros fundamentales, que son la probabilidad de que ocurra un evento y una estimación del costo o pérdida, en caso de que ocurra. El producto de los dos términos se llama costo anual estimado.

Tabla 1

Enfoques cualitativos y cuantitativos

	Ventajas	Inconvenientes
Cualitativo	Enfoque lo amplio que se desee. Plan de trabajo flexible y reactivo. Se concentra en la identificación de eventos. Influyen factores intangibles. No se necesita cuantificar la frecuencia de las amenazas. El proceso para alcanzar resultados creíbles y un consenso consume menos tiempo. Permite una visibilidad y entendimiento del ranking de riesgos.	Depende fuertemente de la habilidad y calidad del personal involucrado. Pueden excluir riesgos significantes desconocidos. Insuficiente diferenciación entre los riesgos importantes. Dificultad de justificar la inversión en la implantación del control, debido a la no existencia de una base de análisis costes/ beneficios. Los resultados son dependientes de la calidad del equipo de gestión de riesgos. No es fiable para eventos raros o impactos impensables.
Cuantitativo	Es objetivo, independiente del proceso. Base sólida para un análisis de costes y beneficios de las salvaguardas. Enfoca pensamientos mediante el uso de números. Facilita la comparación de vulnerabilidades muy distintas. Proporciona una cifra justificante para cada contramedida.	En la mayoría de los casos, es difícil de enumerar todos los tipos de eventos y obtener datos con significado sobre la probabilidad e impacto. Es difícil de estimar el valor de un activo intangible, en concreto, la disponibilidad de la información para la que se diseñó el sistema. Estimación de las pérdidas potenciales sólo si son valores cuantificables. Metodología estándar. Consume mucho tiempo y es costoso a la hora de hacerlo bien. Dependencia de un profesional.

Nota: Autores (2023)

1.4.3.Seguridad de información

La seguridad de la información, según ISO 27001 (2013), consiste en preservar su confidencialidad, integridad y disponibilidad, así como los sistemas involucrados en su procesamiento, dentro de una organización. Por lo tanto, estos tres términos forman la base sobre la que descansa todo el edificio de seguridad de la información:

- Confidencialidad: la información no se pone a disposición ni se revela a personas, entidades o procesos no autorizados.
- Integridad: mantenimiento de la exactitud e integridad de la información y sus métodos de procesamiento.
- Disponibilidad: acceso y uso de la información y sus sistemas de procesamiento por parte de personas, entidades o procesos autorizados cuando sea necesario.

Para garantizar que la seguridad de la información se gestione correctamente, se debe utilizar, documentar y conocer en toda la organización un proceso sistemático desde una perspectiva de riesgo empresarial. Este proceso es lo que constituye un SGSI.

1.4.4.Metodología OCTAVE

El método OCTAVE fue la primera metodología consistente que se introdujo. El enfoque está definido por una guía de implementación del método (procedimientos, guías, fichas, catálogos de información) y capacitación. El método se aplica en una serie de talleres dirigidos y facilitados por un equipo interdisciplinario de análisis de unidades de negocio en toda la organización (por ejemplo, la alta dirección, el área de operaciones y los directores de personal) y miembros del departamento de TI (Caralli, Stevens, Young, & Wilson, 2007).

El público objetivo del método OCTAVE son grandes organizaciones con 300 o más personas.

Más concretamente, está dirigido a organizaciones que:

- Tener una jerarquía de varios niveles.
- Mantenga su propia infraestructura de TI.

- Tener la capacidad de ejecutar herramientas de evaluación de vulnerabilidades.
- Tener la capacidad de interpretar los resultados de las evaluaciones de vulnerabilidad.

1.4.4.1. OCTAVE-S

El desarrollo de OCTAVES fue apoyado por el programa de Inserción, Demostración y Evaluación (TIDE) de SEI 4 con el objetivo de brindar un enfoque basado en octavas a las pequeñas empresas manufactureras. La versión más reciente del enfoque OCTAVE-S está diseñada específicamente para organizaciones de 100 personas o menos.

De acuerdo con los criterios de OCTAVE, el enfoque OCTAVE-S.

Consta de tres fases similares. Sin embargo, OCTAVE-S está liderado por un equipo de análisis que tiene un conocimiento profundo de la organización. Por lo tanto, OCTAVE-S no se basa en talleres formales de captación de conocimientos para recopilar información, ya que se espera que el equipo de análisis (generalmente de tres a cinco) tenga un conocimiento práctico de los activos importantes relacionados con la información, los requisitos de seguridad, las amenazas y la seguridad. practicas organización.

1.4.4.2. OCTAVE Allegro

El enfoque de OCTAVE Allegro presentado en este documento técnico está diseñado para permitir una evaluación integral del entorno de riesgo operativo de una organización para lograr resultados más sólidos sin la necesidad de un conocimiento extenso de evaluación de riesgos. Este enfoque define los enfoques anteriores de OCTAVE, centrándose principalmente en cómo se utilizan los recursos de texto, dónde se almacenan, transportan y procesan, y cómo están expuestos a las amenazas, vulnerabilidades e interrupciones resultantes. Al igual que los métodos anteriores, OCTAVE Allegro se puede ejecutar en un entorno colaborativo y se complementa con hojas de trabajo y cuestionarios, que se incluyen en los apéndices de este documento.

Sin embargo, el OCTAVE Allegro también es adecuado para personas que deseen realizar una evaluación de riesgos sin una participación, experiencia o aportes significativos en la organización.

1.4.4.2.1. Fase de la metodología OCTAVE allegro

1) Establecer criterios de medición del riesgo

Los impulsores organizacionales se establecen para evaluar los efectos de un riesgo en la misión y los objetivos comerciales de una organización. Estos factores se reflejan en un conjunto de métricas de riesgo que se crean y guardan como parte de este primer paso.

El método Allegro OCTAVE proporciona un conjunto de plantillas estándar para crear estos criterios en varios dominios de impacto y establecer prioridades. Las zonas de impacto consideradas son:

- Confidencialidad, reputación/cliente
- Financiero
- Productividad
- Salud y seguridad
- Sanciones legales
- Definición de zonas de impacto de usuarios

Las áreas de impacto deben priorizarse de la más importante a la menos importante.

2) Desarrollar un perfil de Activos de Información

La metodología OCTAVE Allegro se enfoca en los activos informacionales de la organización para lo cual se realiza el proceso de creación de un perfil de estos activos. Un perfil es una representación informativa de un activo que describe sus características únicas, cualidades, características y valor. Para desarrollar el perfil, se deben considerar las siguientes actividades:

- Identificar el grupo de activos de información para los que se realizará el perfilado.
- Centrarse en los recursos de información más críticos

- Obtener la información necesaria para comenzar a estructurar el proceso de análisis de riesgo de activos.

3) Identificar los contenedores de los activos de la información

Los contenedores describen los lugares donde se almacena, transporta y procesa la información. Los activos de información residen no solo en contenedores dentro de los límites de una organización, sino también en contenedores que no están bajo el control directo de la organización.

tipos de contenedores:

- Contenedores técnicos: Están bajo el control directo de la organización o son gestionados fuera de la organización.
- Contenedores físicos: la información puede estar dentro o fuera de la empresa.
- Persona contenedora: Persona interna o externa a la organización que tiene conocimiento detallado del bien.

4) Identificar las áreas de interés

En este paso, el proceso de identificación de riesgos se lleva a cabo mediante una lluvia de ideas sobre las condiciones o situaciones que pueden poner en peligro los activos de información de la organización. Estos escenarios del mundo real se relacionan con áreas de preocupación y pueden representar amenazas y sus correspondientes resultados no deseados.

5) Identificar las situaciones de amenaza

En la primera mitad del Paso 5, las áreas de preocupación identificadas en el paso anterior se desarrollan en escenarios de amenazas. Varios escenarios de amenazas se pueden representar visualmente en una estructura de árbol comúnmente conocida como árbol de amenazas.

6) Identificar los riesgos

Luego de identificar la amenaza en el paso anterior, en este paso se identificarán las consecuencias en la organización. Las amenazas pueden tener varios impactos potenciales en una organización. Por ejemplo, una falla en el sistema

de comercio electrónico de una organización puede afectar la reputación de la organización con los clientes y la salud financiera.

7) Analizar los riesgos

Calcula una medida cuantitativa de la exposición de una organización a las amenazas. Esto se hace considerando el escenario de amenaza y sus consecuencias. Luego asigna un valor de impacto (bajo, medio, medio) a cada área de influencia. Finalmente, se calculan los valores de impacto de cada área para analizar los riesgos, ayudando a la organización a determinar la mejor estrategia para gestionar ese riesgo.

8) Seleccione enfoque de mitigación

Las organizaciones desarrollan estrategias para determinar cuáles de los riesgos que identifican necesitan ser mitigados. Las organizaciones deben clasificar cada riesgo identificado mediante evaluaciones que les ayuden a tomar decisiones informadas sobre su estado de mitigación. Luego, a cada riesgo se le debe asignar un enfoque de mitigación y, finalmente, se debe desarrollar una estrategia de mitigación para mitigar el riesgo. Estas hojas de trabajo han sido cuidadosamente diseñadas para traducirse fácilmente a otros formatos electrónicos.

1.4.5.Metodología MAGERIT

Desde España, desarrolló y popularizó MAGERIT (Método para el Análisis y Gestión de Riesgos de los Sistemas de Información en las Administraciones Públicas) como respuesta a la percepción de que los órganos de gobierno (y la sociedad en general) dependen cada vez más de la información técnica para lograr sus objetivos de servicio. Por tanto, la razón de ser de MAGERIT está directamente relacionada con la proliferación de medios electrónicos, informáticos y telemáticos, que aportan evidentes beneficios a los ciudadanos; pero también implica ciertos riesgos que es necesario mitigar mediante medidas de seguridad. Estas medidas de seguridad garantizan la autenticación, confidencialidad, integridad y disponibilidad de los sistemas de información y generan confianza en el uso de dichos activos. Una organización no podrá lograr sus objetivos, tareas y misión si no cuenta con los elementos informáticos

básicos y necesarios dentro de sus capacidades para ayudar y apoyar la toma de decisiones (Consejo Superior de Administración Electrónica, 2012).

1.4.5.1. Conceptualización

MAGERIT es un método formalizado para investigar los riesgos que representan los Sistemas de Información y para recomendar las medidas adecuadas a tomar para controlar estos riesgos.

MAGERIT permite:

- Estudiar los riesgos que soporta un sistema de información y el entorno asociado al mismo. MAGERIT ofrece realizar un análisis de riesgo que consiste en evaluar el impacto que tiene una brecha de seguridad en la organización; reporta los riesgos existentes, identifica las amenazas que amenazan el sistema de información y determina la vulnerabilidad del sistema para prevenir estas amenazas, obteniendo resultados.
- Los resultados del análisis de riesgos permiten a la gerencia de riesgos recomendar las medidas adecuadas que se deben adoptar para conocer, prevenir, prevenir, reducir o controlar los riesgos identificados y así minimizar su potencial o su posible daño.

1.4.5.2. Activos

Un componente o función de un sistema de información que puede ser atacado intencional o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos de gestión, recursos materiales y recursos humanos (UNE 71504:2008).

1.4.5.3. FASES DE MAGERIT VERSIÓN 3

- **Identificación de activos informáticos**

Se identifica los activos informáticos existentes en la organización.

- **Catálogos de amenazas**

En este punto se han identificado las amenazas y estas amenazas se agrupan por origen industrial, error, error accidental y ataque intencionado.

- **Caracterización**

En la descripción, denotamos amenazas que podrían afectar cada característica de la computadora; asimismo, obtenemos la probabilidad de que estas amenazas puedan dañar estos activos informáticos. Estas categorías se evalúan para cada amenaza que contiene esta característica.

- **Impacto**

Conoce el efecto de cada dimensión y para cada activo informático realiza la operación derivada del valor de la dimensión, que se realiza en el identificador del activo utilizando el valor de la dimensión derivado de la tabla de propiedades.

- **Mapa de riesgos**

Relación de las amenazas a que están expuesto los activos.

- **Salvaguardas**

En esta tarea las salvaguardas están agrupados tipos de protección.

1.4.6.Diseño factorial

Es un diseño experimental en el que a cada variable independiente se le llama factor y los números indican el nivel de cada variable, también se definen como experimentos que investigan simultáneamente dos o más factores y forman un tratamiento. usando combinaciones de diferentes niveles de cada factor (kuehl, 2001).

1.4.6.1. Tres efectos de los factores

- **Efecto de un factor**: Es un cambio en la respuesta producida cuando pasamos de un nivel a otro.
- **Efectos simples:** Son las comparaciones entre los niveles de un factor a un solo nivel del otro.
- **Efectos principales:** Es un factor son comparaciones entre los niveles de un factor promediados para todos los niveles de otro factor.

1.4.6.2. Modelo estadístico para dos factores

Modelo de medias de las celdas.

El factor de axb con r replicas, en un diseño totalmente aleatorizado.

$$y_{ijk} = \mu_{ij} + e_{jk}$$

$$i = 1, 2, \dots, a \quad j = 1, 2, \dots, b \quad k = 1, 2, \dots, r$$

Donde:

μ_{ij} = media de la combinación de los tratamiento A, B

e_{jk} = Errores experimentales aleatorios con media 0 y varianza σ^2

Estimaciones de las medias de celdas con el método de mínimos cuadrados.

$$ss\ Error = \sum_{i=1}^{a} \sum_{j=1}^{b} \sum_{k=1}^{r} \hat{e}_{ijk}^2 = \sum_{i=1}^{a} \sum_{j=1}^{b} \sum_{k=1}^{r} (y_{ijk} - \hat{\mu}_{ij})^2$$

Los estimadores de mínimos cuadrados para μ_{ij} son las medias de celdas observadas de las combinaciones del tratamiento

$$\hat{\mu}_{ij} = \frac{y_{ij}}{r} = \bar{y}_{ij}$$

$$1 = 1, 2, \dots, a \quad j = 1, 2, \dots, b$$

1.5. Definiciones conceptuales

- **Activo:** Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos. (UNE 71504, 2008).
- **Impacto**: Consecuencia que sobre un activo tiene la materialización de una amenaza (MAGERIT, 1997).
- **Integridad** Característica que previene contra la modificación o destrucción no autorizadas de activos del dominio (MAGERIT, 1997).
- **Plan de seguridad**: Conjunto de proyectos de seguridad que permiten materializar las decisiones de gestión de riesgos.

- **Probabilidad**: (likelihood) – Posibilidad de que un hecho se produzca (UNE-ISO Guía 73, 2010).
- **Políticas de seguridad**: Es una o más reglas de seguridad, procedimientos, prácticas o directrices impuestas por una organización sobre sus operaciones. (MAGERIT, 1997)
- **Riesgo**: Posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la Organización (MAGERIT, 1997).
- **Salvaguarda:** Procedimiento o mecanismo tecnológico que reduce el riesgo. Control: Medida que modifica un riesgo (UNE-ISO Guía 73, 2010).
- **Seguridad de la información**: Confianza en que los sistemas de información están libres y exentos de todo peligro o daño inaceptables (UNE 71504, 2008).
- **Vulnerabilidad:** Defecto o debilidad en el diseño, implementación u operación de un sistema que habilita o facilita la materialización de una amenaza. Propiedades intrínsecas de que algo se produzca como resultado de una sensibilidad a una fuente de riesgo que puede conducir a un suceso con una consecuencia (UNE-ISO Guía 73, 2010).
- **Amenaza:** Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización (UNE 71504, 2008).
- **Análisis de impacto**: Estudio de las consecuencias que tendría una parada de X tiempo sobre la Organización (UNE 71504, 2008).
- **Análisis de riesgos:** Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización. Análisis del riesgo Proceso que permite comprender la naturaleza del riesgo y determinar el nivel de riesgo (UNE-ISO Guía 73, 2010).
- **Autenticidad**: Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos (UNE 71504, 2008).

- **Confidencialidad** Propiedad o característica consistente en que la información ni se pone a disposición ni se revela a individuos, entidades o procesos no autorizados (UNE 71504, 2008).
- **Degradación de valor de un activo** Pérdida de valor de un activo como consecuencia de la materialización de una amenaza.
- **Disponibilidad:** Característica que previene contra la denegación no autorizada de acceso a activos del dominio (MAGERIT, 1997).
- **Frecuencia:** Tasa de ocurrencia de una amenaza. Número de sucesos o de efectos en una unidad de tiempo (ISO Guide 73, 2009).
- **Gestión de riesgos**: Selección e implantación de las medidas o 'salvaguardas' de seguridad adecuadas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios. La gestión de riesgos se basa en los resultados obtenidos en el análisis de los riesgos (MAGERIT, 1997).

CAPITULO 2

MATERIALES Y MÉTODOS

Materiales y métodos

La aplicación del análisis de riesgos a través de las metodologías MAGERIT Y OCTAVE nos permitirá evaluar la seguridad de nuestros sistemas, cuantificar y comparar los requisitos de seguridad de la información, determinar los activos y sus características de mayor valor, teniendo en cuenta los criterios de ACID (Autenticación, Confidencialidad, Integridad, Disponibilidad y No repudio), identificar las salvaguardas existentes, las amenazas, su origen y el tipo de vulnerabilidad que puede afectar la estimación y evaluación de los impactos, concluyendo con una evaluación de los riesgos a los que los activos de la empresa están expuestos. De esta forma, se pretende determinar en qué medida la metodología MAGERIT es mejor que la metodología OCTAVE en el análisis de riesgo a optimizar la seguridad de la información aplicando la metodología adecuada y así, previa investigación, proponer resguardos, estrategias de protección y la implementación de las medidas de seguridad declaradas en las políticas de seguridad, teniendo en cuenta las normas y reglamentos vigentes para controlar, enfrentar, gestionar el riesgo minimizándolo a niveles aceptables y conociendo los beneficios, costos y oportunidades involucrados.

2.1. Metodología utilizada en el proceso de investigación científica

El método de inducción se refiere al método de obtención del concepto de proposiciones generales mediante la observación de hechos específicos, es decir, el método de determinación de principios generales mediante el estudio y análisis de los hechos. y especialmente los fenómenos que han surgido.

2.2. Tipo de investigación

El tipo de investigación es aplicada por que busca conocer la mejor metodología para el análisis de riesgo en la Escuela de Pos Grado para hacer un correcto diagnóstico de la seguridad de los sistemas de información de la misma.

2.3. Diseño de la investigación

Un diseño de investigación es experimental en el sentido de que su objetivo es averiguar si ciertos factores afectan la variable de interés y, de ser así, cuantificar ese efecto.

2.4. Diseño de experimentos

Diseños factorial con dos factores, con replica (Porras, 2000) Un diseño de experimentos factorial o arreglo factorial es el conjunto de tratamientos que pueden formarse considerando todas las posibles combinaciones de los niveles de los factores.

Tabla 2

Variables

Variable independiente B	Variable independiente A	
	A_1	A_2
B_1	A_1B_1	A_2B_1
B_2	A_1B_2	A_2B_2

Nota: Picoy (2017)

2.4.1. Modelo estadístico

$$Y_{ijk} = \mu + \alpha_i + \beta_j + (\alpha\beta)_{ij} + E_{ijk}$$

$$i = 1, 2, \dots, a \; j = 1, 2, \dots, b \; k = 1, 2, \dots, n$$

2.5. Población y muestra

- **Población**

La población está constituida por todos los activos de la Escuela de Pos Grado de la Universidad Nacional Herminio Valdizán - Huánuco.

Población N=76 activos (Tipificado por nombre)

La muestra está constituida por todos los activos que hacen uso y manejo de la información en Escuela de Pos Grado de la Universidad Nacional Hermilio Valdizán - Huánuco.

- **Muestra**

Para hallar la muestra se utilizó el método de muestreo no probabilístico de tipo Muestreo intencional o de conveniencia: Este tipo de muestreo se caracteriza por un esfuerzo deliberado de obtener muestras "representativas" en este caso los activos que hacen uso y manejo de la información en Escuela de Pos Grado.

Muestra n=22 activos (tipificado por nombre)

2.6. Variables

a) Variable independiente

Las metodologías.

b) Variable dependiente

Análisis de Riesgo y Propuesta de Mejora.

c) Variable interviniente

Escuela de posgrado.

2.7. Técnicas de recojo, procesamiento y presentación de datos

2.7.1. Técnicas para la recolección de datos

Para la recolección de los datos se utilizó la Técnica de la Entrevistas aplicado a dos estratos:

Tabla 3

Recolección de datos

Estratos	Finalidad	Cantidad

Formato 1	Personal Administrativo	Obtener información general de la facultad y algunos datos básicos de la misma	2
Formato 2	Jefe del área de Informática, Bienes patrimoniales, Personal administrativo	Obtener información acerca de los activos que poseen	5

Nota: Picoy (2017)

Con el objeto de conocer específicamente los activos de la Escuela de Pos Grado, para identificar las diferentes vulnerabilidades y amenazas de la Escuela de Pos Grado, y así brindarles un análisis de riesgo efectivo.

2.7.2.Técnicas para los procesamientos de datos

Se utilizaron:

- **Revisión y consistencia de la información:** Este paso consiste básicamente en depurar la información mediante la revisión de los datos contenidos en los instrumentos de trabajo de campo con el objetivo de corregir los denominados datos brutos (juicio de expertos).
- **Preparar plantillas en Excel 2013 Activos:** Prepare plantillas de Excel de acuerdo con los parámetros de los métodos MARGERIT y OCTAVE para permitir el ingreso, procesamiento y análisis de datos relacionados con los activos lanzados utilizando los métodos anteriores.
- **Elaboración de plantilla Excel 2013 - Diseño Factorial:** Se ha elaborado una plantilla Excel según Diseño Factorial e Interacción para poder procesar y analizar los datos recogidos en base al uso de los métodos MARGERIT y OCTAVE del colegio. estudiante graduado**.**

2.7.3. Presentación de datos

2.7.3.1. Análisis descriptivo

En cuanto al análisis descriptivo de cada una de las variables se tuvo en cuenta las medidas de dispersión para las variables.

2.7.3.2. Análisis inferencial

En el análisis inferencial de los datos se utilizó el coeficiente de correlación de Pearson con el fin de medir la relación entre las variables en estudio. Se tuvo en cuenta una significación de 0,05.

2.8. Experimentación

1.1.1 Diseño factorial de 2x2 con 2 réplicas:

a) Diseño de tratamientos

Se usó un arreglo factorial con los factores "METODOLOGIAS" y "DIMENSIONES". Existen dos niveles de METODOLOGIAS - A, A1 (MAGERIT) y A2, (OCTAVE)- y dos niveles de DIMENSIONES - B, B1 (VULNERABILIDAD) y B2 (IMPACTO).

b) Diseño del experimento

Se construyeron dos réplicas de especímenes y se probaron las ocho combinaciones. Los 16 especímenes se prepararon y probaron en orden aleatorio para un diseño totalmente aleatorizado.

El modelo estadístico para este diseño es el siguiente:

$$\boldsymbol{Y_{ijk} = \mu + \alpha_i + \beta_j + (\alpha\beta)_{ij} + e_{ijk}}$$

$$\boldsymbol{i = 1, 2, \dots, a \quad j = 1, 2, \dots, b \quad k = 1, 2, \dots, r}$$

Donde:

$\boldsymbol{\alpha_i} = es\ el\ efecto\ del\ factor\ metodologias, i = 1;\ 2;\ I = 2$

$\boldsymbol{\beta_j} = es\ el\ efecto\ del\ factor\ dimensiones, i = 1;\ 2;\ I = 2$

$(\boldsymbol{\alpha\beta})_{ij} = es\ el\ efecto\ de\ la\ interacción\ entre\ ambos\ factores.$

$\boldsymbol{i} = numero\ de\ niveles$

$\boldsymbol{j} = numero\ de\ factores$

$\boldsymbol{r} = numero\ de\ replicas$

$\boldsymbol{n = abr} = numero\ de\ observaciones$

El número de parámetros de este modelo es, ab + 1 y el número de observaciones es abr.

En tal caso nuestros valores son los siguientes:

$\boldsymbol{i} = 2 \quad \boldsymbol{j} = 2 \quad \boldsymbol{r} = 2 \quad \boldsymbol{n = 2\ x\ 2\ x\ 2} = 8$

1) Estimación de los parámetros del modelo

Para estimar estos parámetros se calculan las medias de cada casilla y las medias de cada fila y cada columna.

Los estimadores máximos verosímiles de los parámetros del modelo son:

$$\hat{\boldsymbol{\mu}} = \bar{\boldsymbol{y}} \ldots , \qquad \hat{\boldsymbol{\alpha}}_{\boldsymbol{i}} = \bar{\boldsymbol{y}}_{\boldsymbol{i}}.. - \bar{\boldsymbol{y}} .., \qquad \widehat{\boldsymbol{\beta}_{\boldsymbol{J}}} = \bar{\boldsymbol{y}}_{\boldsymbol{j}.} - \bar{\boldsymbol{y}} \ldots$$

$$\left(\widehat{\boldsymbol{\alpha\beta}}\right)_{\boldsymbol{ij}} = \bar{\boldsymbol{y}}_{\boldsymbol{ij}.} - \bar{\boldsymbol{y}}_{\boldsymbol{i}} .. - \bar{\boldsymbol{y}}_{\boldsymbol{.j}.} + \bar{\boldsymbol{y}} \ldots$$

Donde:

- $\bar{\boldsymbol{y}}_{\boldsymbol{ij}.} = es\ la\ media\ de\ las\ r\ observaciones\ en\ la\ celdilla\ ij$:

$$\bar{\boldsymbol{y}}_{\boldsymbol{ij}.} = \frac{(\sum_{\boldsymbol{k}} \boldsymbol{y}_{\boldsymbol{ijk}})}{\boldsymbol{r}}$$

Operando:

$$\bar{\boldsymbol{y}}_{\boldsymbol{11}} = \frac{\boldsymbol{4+3}}{\boldsymbol{2}} = \boldsymbol{3.5}$$

$$\bar{\boldsymbol{y}}_{\boldsymbol{12}} = \frac{\boldsymbol{3+2}}{\boldsymbol{2}} = \boldsymbol{2.5}$$

$$\bar{\boldsymbol{y}}_{\boldsymbol{21}} = \frac{\boldsymbol{3+5}}{\boldsymbol{2}} = \boldsymbol{4}$$

$$\bar{\boldsymbol{y}}_{\boldsymbol{22}} = \frac{\boldsymbol{5+4}}{\boldsymbol{2}} = \boldsymbol{4.5}$$

- $\bar{\boldsymbol{y}}_{\boldsymbol{i}}.. = \ es\ la\ media\ de\ las\ observaciones\ del\ nivel\ i\ del\ factor\ A$:

$$\bar{\boldsymbol{y}}_{\boldsymbol{i}}.. = \frac{(\sum_{\boldsymbol{j,k}} \boldsymbol{y}_{\boldsymbol{ijk}})}{(\boldsymbol{br})} \ ; \boldsymbol{i = 1, \ldots, a}$$

Operando:

$$\bar{y}_{1..} = \frac{3.5 + 2.5}{2} = 3$$

$$\bar{y}_{2..} = \frac{4 + 4.5}{2} = 4.3$$

- $\bar{y}_{.j.} = es\ la\ media\ de\ las\ observaciones\ del\ nivel\ j\ del\ factor\ B$:

$$\bar{y}_{.j.} = \frac{(\sum_{i,k} y_{ijk})}{(ar)}; j = 1, \dots, b$$

Operando:

$$\bar{y}_{.1.} = \frac{3.5 + 4}{2} = 3.8$$

$$\bar{y}_{.1.} = \frac{2.5 + 4.5}{2} = 3.5$$

- $\bar{y}\ \dots = es\ la\ media\ total\ de\ las\ observaciones$

$$\bar{y}\ \dots = \frac{(\sum_{i,j,k} y_{ijk})}{r}$$

Operando:

$$\bar{y}\ \dots = \frac{3.8 + 3.5 + 3 + 4.3}{2} = 7.3$$

Obteniendo el siguiente cuadro:

Tabla 4

Cuadro de estimación de los parámetros

$\bar{y}_{ij}$	Vulnerabilidad		Impacto		Medias marginales (A) $\bar{y}_{i"}$
MAGERIT	4 3	3,5	3 2	2,5	3
OCTAVE	3 5	4	5 4	4,5	4,3

Medias marginales (B) $\bar{y}_{*j}$	3,8	3,5	$\bar{y}$ ... = 7,3

Nota: Autores (2023)

Se calculan los parámetros del modelo utilizando:

$$\hat{\mu} = \bar{y} \ldots , \quad \hat{\alpha}_i = \bar{y}_{i\cdot\cdot} - \bar{y} \ldots, \quad \widehat{\beta_j} = \bar{y}_{\cdot j\cdot} - \bar{y} \ldots$$

$$\left(\widehat{\alpha\beta}\right)_{ij} = \bar{y}_{ij\cdot} - \bar{y}_{i\cdot\cdot} - \bar{y}_{\cdot j\cdot} + \bar{y} \ldots$$

Operando

$$\left(\widehat{\alpha\beta}\right)_{11} = 3.5 - 3 - 3.8 + 7.3 = 4$$

$$\left(\widehat{\alpha\beta}\right)_{12} = 2.5 - 3 - 3.5 + 7.3 = 3.3$$

$$\left(\widehat{\alpha\beta}\right)_{21} = 4 - 4.3 - 3.8 + 7.3 = 3.3$$

$$\left(\widehat{\alpha\beta}\right)_{22} = 4.5 - 4.3 - 3.5 + 7.3 = 4$$

$$\hat{\alpha}_1 = 3 - 7.3 = -4.3$$

$$\hat{\alpha}_2 = 4.3 - 7.3 = -3$$

$$, \quad \widehat{\beta_j} = 3.8 - 7.3 = -3.5$$

$$, \quad \widehat{\beta_j} = 3.5 - 7.3 = -3.8$$

Obteniendo el siguiente cuadro:

Tabla 5

Cuadro de estimación de MAGERIT y OCTAVE

$\widehat{\alpha\beta}_{ij}$	Vulnerabilidad	Impacto	$\hat{\alpha}_j$
MAGERIT	4.0	3.3	-4.3
OCTAVE	3.3	4.0	-3.0
$\hat{\beta}_j$	-3.5	-3.8	

Nota: Autores (2023)

Se calculan las predicciones a partir de:

$$\hat{y}_{ij} = \hat{\mu} + \hat{\alpha}_i + \hat{\beta}_j + \widehat{(\alpha\beta)}_{ij} = \bar{y}_{ij\cdot}$$

Operando

$$\hat{y}_{11} = 7.3 + (-4.3) + (-3.5) + 4 = 3.5$$

$$\hat{y}_{12} = 7.3 + (-4.3) + (-3.5) + 3.3 = 2.5$$

$$\hat{y}_{21} = 7.3 + (-3) + (-3.5) + 3.3 = 4$$

$$\hat{y}_{22} = 7.3 + (-3) + (-3.8) + 4 = 4.5$$

Obteniendo el siguiente cuadro:

Tabla 6

Predicciones =medias casillas

$\hat{y}_{ij}$	Vulnerabilidad	Impacto
MAGERIT	3.5	2.5
OCTAVE	4.0	4.5

Nota: Picoy (2017)

Los residuos de este modelo se calculan como:

$$e_{ijk} = y_{ijk} - \hat{y}_{ijk} = y_{ij} - \hat{\mu} - \hat{\tau}_i - \hat{\beta}_j - \widehat{\tau\beta}_{ij} = y_{ijk} - \bar{y}_{ij.}\ i, j = 1,2$$

Operando

$$e_{111} = 4 - 3.5 = 0.5$$

$$e_{121} = 3 - 3.5 = -0.5$$

$$e_{212} = 3 - 2.5 = 0.5$$

$$e_{222} = 2 - 2.5 = -0.5$$

$$e_{211} = 3 - 4 = -1$$

$$e_{212} = 5 - 4 = 1$$

$$e_{212} = 5 - 4.5 = 0.5$$

$$e_{222} = 4 - 4.5 = -0.5$$

Obteniendo el siguiente cuadro:

Tabla 7

Residuos

	Dimensiones (B)	
Metodología (A)	**Vulnerabilidad**	**Impacto**
MAGERIT	0.5	0.5
	-0.5	-0.5
OCTAVE	-1.0	0.5
	1.0	-0.5

Nota: Picoy (2017)

Se verifica que todos los residuos de una celdilla deben sumar cero, es decir, en cada celdilla hay r − 1 residuos independientes. Por lo tanto, en total habrá ab (r − 1) residuos independientes.

La varianza residual tiene la siguiente expresión:

$$\hat{S}_R^2 = \frac{\sum_{i=1}^{a} \sum_{j=1}^{b} \sum_{k=1}^{c} e_{ijk}^2 \, m}{ab(r-1)}$$

2.8.1. Descomposición de la variabilidad

La ecuación básica del análisis de la varianza es:

$$\sum_{i.j.k} (y_{ijk} - \bar{y}\ldots)^2$$

$$= br \sum_{i=1}^{a} (\bar{y}_{i..} - \bar{y}\ldots)^2 + ar \sum_{j=1}^{b} (\bar{y}_{.j.} - \bar{y}\ldots)^2$$

$$+ r \sum_{i,j} \left(y_{ijs} - \bar{y}_{i..} - \bar{y}_{.j.} + \bar{y}\ldots\right)^2 + \sum_{i,j,k} \left(y_{ijk} - \bar{y}_{ij.}\right)^2$$

Que simbólicamente podemos escribir: **SCT = SCA + SCB + SC (AB) + SCR.** Estas sumas de cuadrados también se pueden expresar como:

- $SCT = \sum_{i,j,k} y_{ijk}^2 - \left(\frac{y^2..}{r}\right) : Suma\ total\ de\ cuadrados$
- $SCA = \frac{(\sum_i y_{i..}^2)}{(br)} - \left(\frac{y^2...}{abr}\right) : S.C.\ entre\ niveles\ de\ A$
- $SCB = \frac{\left(\sum_j y_{.j.}^2\right)}{(ar)} - \left(\frac{y^2...}{abr}\right) : S.C.\ entre\ niveles\ de\ B$

- $SC(AB) = \frac{\left(\sum_{i,j} y_{ij.}^2\right)}{r} - \left(\frac{y^{2}...}{abr}\right) - SCA - SCB$: *S.C de la interacción A X B*
- $SCR = SCT - SCA - SSCB - SC(AB)$: $S.C.del\ error$

A partir de la ecuación básica del ANOVA se pueden construir los cuadrados medios definidos como:

- Cuadrado medio total : $CMT = \frac{(SCT)}{n-1}$
- Cuadrado medio de A : $CMA = \frac{(SCA)}{a-1}$
- Cuadrado medio de B : $CMB = \frac{(SCB)}{b-1}$
- Cuadrado medio de la interacción A X B : $CM(AB) = \frac{(SC(AB))}{(a-1)(b-1)}$
- Cuadrado medio residual : $CMR = \frac{(SCR)}{(ab(r-1))}$

Cálculo de las sumas de cuadrados:

$SCA = SC(metodologias) = 3.125$

$SCA = SC(dimensiones) = 0.125$

$SCAB = 1.125$

$SCE = 3.500$

$SCT = 7.8750$

La Tabla **ANOVA** que se obtiene en este problema es la siguiente:

Tabla 8

Tabla de ANOVA

		G.L	SC	S^2 Varianza CM Ajust.	F	P
scA	FACTOR A	1	3.1250	3.1250	3.57	0.132
scB	FACTOR B	1	0.1250	0.1250	0.14	0.725
scAB	INTERACCION AB	1	1.1250	1.1250	1.29	0.320
scE	ERROR	4	3.5000	3.5000		
scT	TOTAL	7	7.8750	7.8750		

Nota: Autores (2023)

Coeficientes de Determinación que se obtienen son:

$$R^2(A) = R^2(metodologias) = \frac{SCA}{SCT} = \frac{3.1250}{7.8750} = 0.3968 = 39.68\%$$

$$R^2(B) = R^2(dimensiones) = \frac{SCB}{SCT} = \frac{0.1250}{7.8750} = 0.0159 => 1.59\%$$

$$R^2(AB) = R^2(interaccion) = \frac{SC(AB)}{SCT} = \frac{1.1250}{7.8750} = 0.1429 => 14.29\%$$

$$R^2 = R^2(A) + R^2(B) + R^2(AB) = 0.3968 + 0.0159 + 0.1429 =$$

$$= 0{,}5556 => 55.56\%$$

2.8.2.Diseño unifactorial

a) Diseño de tratamientos

Se usó un arreglo Unifactorial con los factores "METODOLOGIAS". Existen dos niveles de METODOLOGIAS - A, A1 (MAGERIT) y A2 (OCTAVE).

b) Diseño del experimento

Los 44 especímenes se prepararon y probaron en orden aleatorio para un diseño totalmente aleatorizado.

Tabla 9
Diseño del experimento

	Metodologías			M(Yi)			
Activos (A)	**MAGERIT**	**OCTAVE**	**A (Yj)**	**M**	**O**	**M*M**	**O*O**
Equipo de computo	21	12	1	21	12	441	144
Estabilizador de energía	9	8	2	9	8	81	64
Impresora	9	13	3	9	13	81	169
Pizarra interactiva	12	10	4	12	10	144	100
Armario	8	8	5	8	8	64	64
Laptop	24	16	6	24	16	576	256
Gabinete de red	7	15	7	7	15	49	225
Modem	11	12	8	11	12	121	144
Switch (cisco)	16	10	9	16	10	256	100
Cableado de red	8	12	10	8	12	64	144
Cuadernos y libros (Datos físicos)	12	30	11	12	30	144	900
Datos almacenados	17	33	12	17	33	289	1089
Libro de reclamos	11	28	13	11	28	121	784

Dirección de la EPG	7	20	14	7	20	49	400
Personal responsable (secretaria)	6	20	15	6	20	36	400
Software de plataforma (Windows 8.1)	17	28	16	17	28	289	784
Software de documentación (Microsoft Office)	16	33	17	16	33	256	1089
Software de seguridad (Antivirus-Not 32)	12	28	18	12	28	144	784
Administración de permisos	17	21	19	17	21	289	441
Pagina web de la EPG	18	14	20	18	14	324	196
Internet	7	14	21	7	14	49	196
Extintor	7	9	22	7	9	49	81
			$y_i = \sum_{j=1}^{23} y_{ij} =$	272	73984	394	155236	3916	8554
					666			12470	

Nota: Picoy (2017)

Definición de variables de estudios y de la hipótesis a probar

Variable de estudio: análisis de riesgo

$$H_0: \mu_1 = \mu_2 (No\ existe\ diferencia\ en\ el\ analisis\ de\ riesgo\ entre\ las\ metodología)$$

$$H_1: \mu_1 \neq \mu_2 (Existe\ diferencia\ en\ el\ analisis\ de\ riesgo\ entre\ las\ metodología)$$

El significado verbal de la hipótesis es:

H0: la metodología no influye en el análisis de riesgo o no existe diferencia significativa en el análisis de riesgo entre las metodologías de MAGERIT y OCTAVE.

H1: La metodología influye en el análisis de riesgo o hay diferencia significativa en el análisis de riesgo entre las metodologías de MAGERIT y OCTAVE.

Datos:

Tratamiento (Metodologías) a=> 2

Número de observaciones por metodología n => 22

Número total de observaciones por metodología N => 44

$$i = 1,2; j = 1,2,\dots,23$$

Totales

$$y_i = \sum_{j=1}^{23} y_{ij}$$

$$y_1 = \sum_{j=1}^{23} y_{ij} = 272$$

$$y_2 = \sum_{i=1}^{2} \sum_{j=1}^{23} y_{ij} = 666$$

$$y_2 = \sum_{i=1}^{23} y_{ij} = 394$$

(Picoy, 2017)

Suma de cuadrados

$$SS_T = \sum_{i=1}^{2} \sum_{j=1}^{23} y_{ij}^2 - \frac{y^2..}{N} = 2389,18$$

$$SS_E = SS_T - SS_{Tr} = 2050,91$$

$$SS_{Tr} = \frac{\sum_{i=1}^{2} y^2}{n} - \frac{y^2..}{N} = 338,2727$$

Medias de cuadradas

$$MS_{Tr} = \frac{SS_{Tr}}{a-1} = 338,2727$$

$$MS_E = \frac{SS_E}{N-a} = 48,83117$$

Estadística

$$F_o = \frac{MS_{Tr}}{MS_E} = 6,927394$$

Tabla 10
Tabla de ANOVA con chi cuadrados

Fuente de variación	Suma de cuadrados	G.L	Cuadrados medios	F	P	Valor crítico para F

Metodologías	338,27	1	338,2727273	6,927394	0,1018	4,0762
Error	2050,91	42	48,83116883			
Total	2389,18	43				

Nota: Autores (2023)

Utilizando un nivel de significancia del 5% $(\alpha = 0{,}05)$, para encontrar el $F_{(0{,}05.3{,}16)}$ (tabla Fisher) con 1 grados de libertad (a-1) en el numerador y 42 grados de libertad (N-a) en el denominador.

$$F_{(\alpha,a-1,N-a)} = F_{(0{,}05,1,42)} = 4{,}0726$$

Comparando el $F_{(0)}$ calculado en el análisis de varianza y el $F_{(0{,}05.3{,}16)}$ se puede observar que $F_{(0)}$ cae en la zona de rechazo:

$$F_{(0)} = F_{(0.05,1,42)}$$

$$0{,}1018 > 0{,}05$$

Conclusión

La metodología no incluye en el análisis de riesgo o no hay diferencia significativa en el análisis de riesgo entre las metodologías (Picoy, 2017).

CAPITULO 3

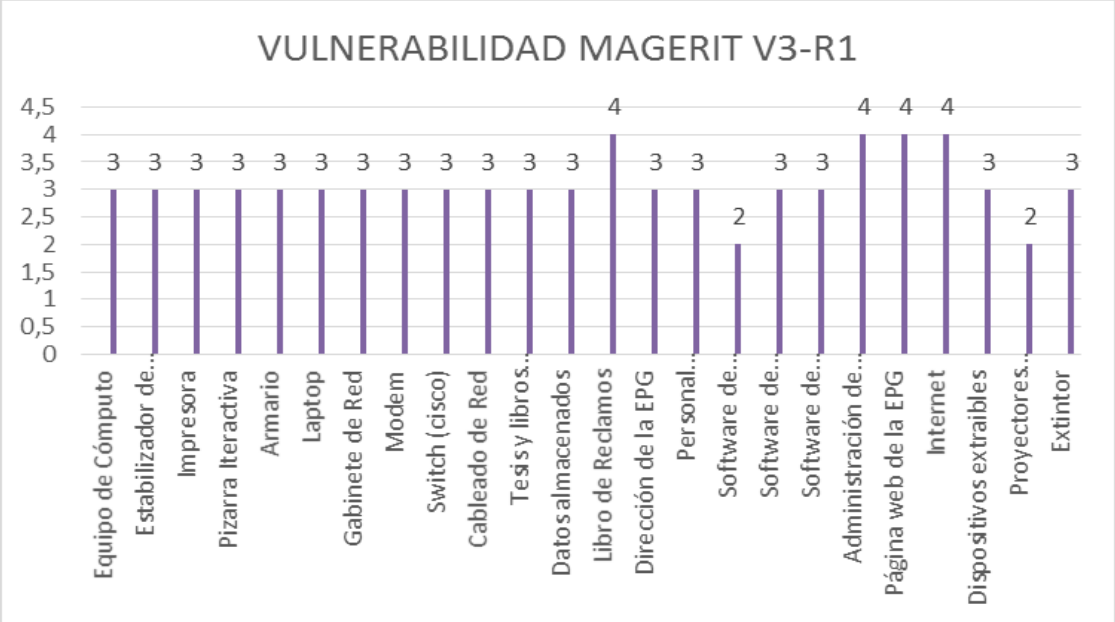
ANÁLISIS DE RESULTADOS

Análisis de resultados

1) Resultados de vulnerabilidad e impacto de la primera replica (R1), MAGERTI V3 Y OCTAVE Allegro

Figura 1

Vulnerabilidades MAGERIT V3-R1

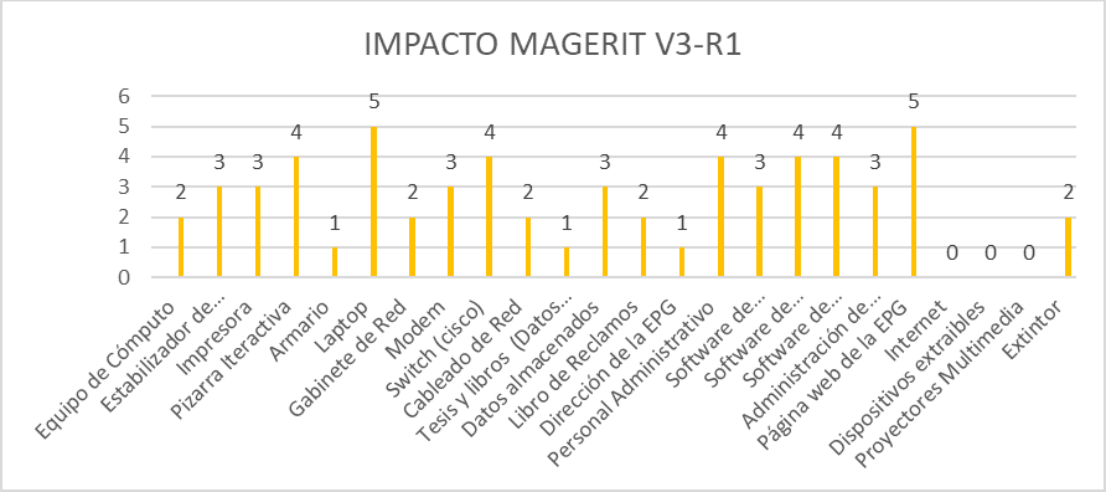


Nota: Picoy (2017)

En la figura 1 observamos el resultado de la valoración de cada activo con respecto a las vulnerabilidades de la primera replica (R1) mediante la metodología MAGERIT V3.

Figura 2

Impacto MAGERIT V3-R1

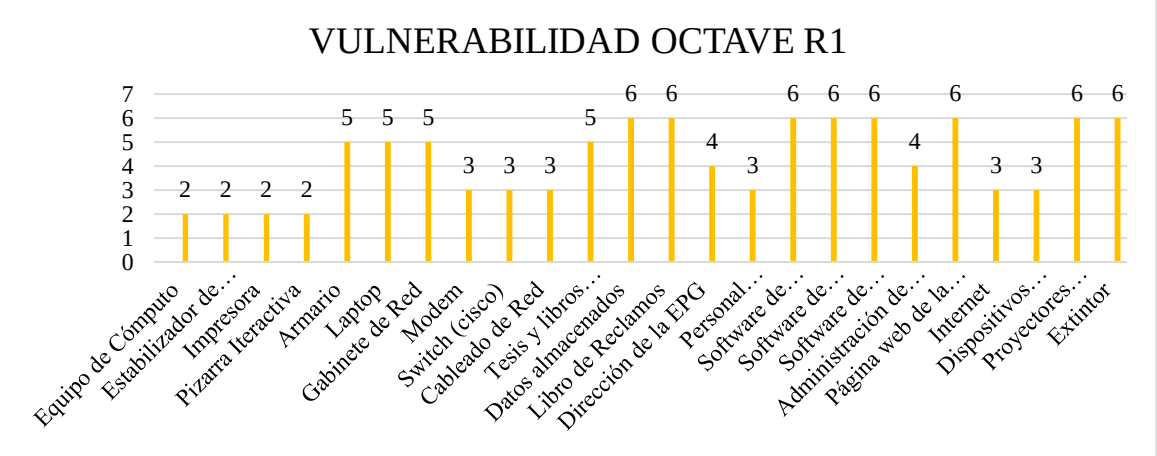


Nota: Picoy (2017)

En la figura 2 observamos el resultado de la valoración de cada activo con respecto al Impacto de la primera replica (R1) mediante la metodología MAGERIT V3.

Figura 3

Vulnerabilidades OCTAVE-R1

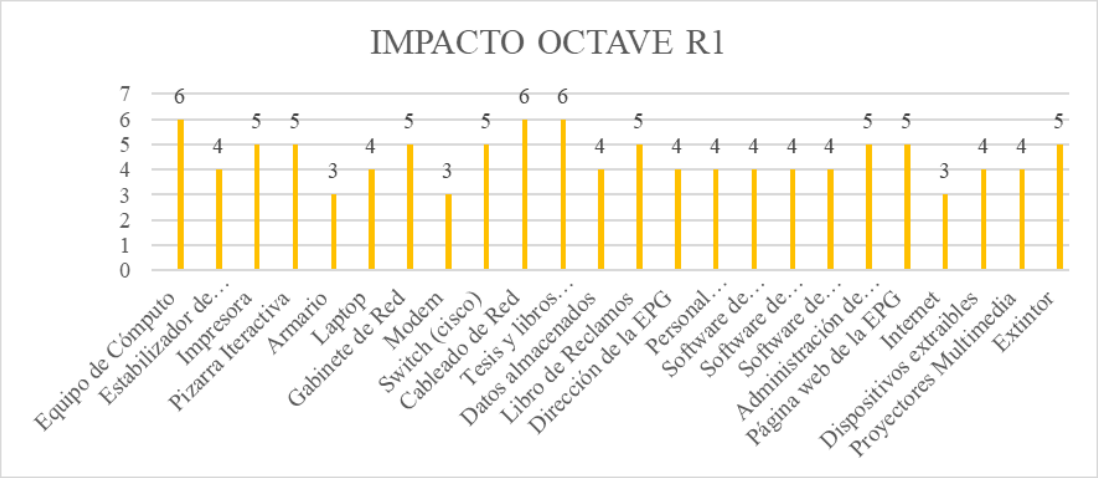


Nota: Picoy (2017)

En la figura 3 observamos el resultado de la valoración de cada activo con respecto a las vulnerabilidades de la primera replica (R1) mediante la metodología OCTAVE.

Figura 4

Impacto OCTAVE -R1



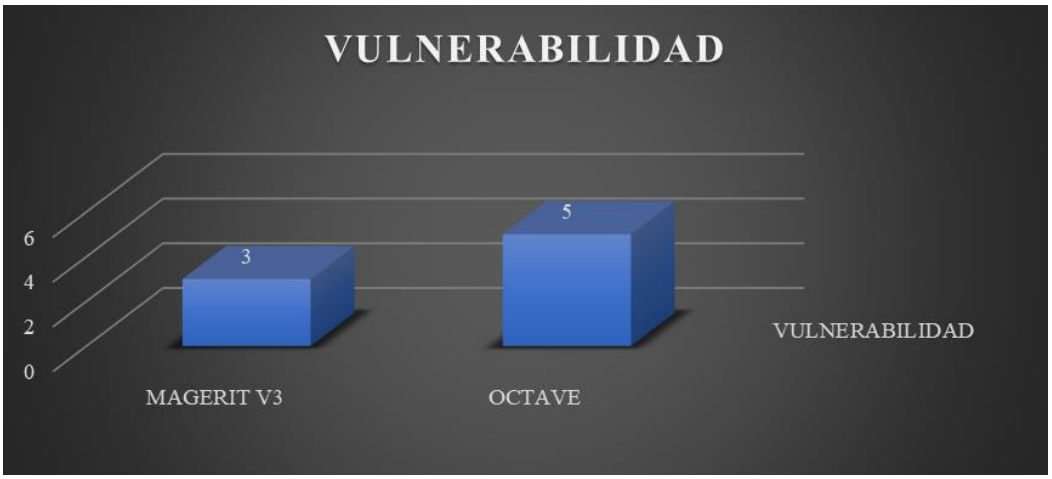
Nota: Picoy (2017)

En la figura 4 observamos el resultado de la valoración de cada activo con respecto al Impacto de la primera replica (R1) mediante la metodología OCTAVE.

2) Vulnerabilidad de la primera replica (R1), MAGERTI V3 Y OCTAVE

Figura 5

Vulnerabilidades MAGERIT-OCTAVE



Nota: Picoy (2017)

En la figura 5 observamos el resultado de la valoración general del activo con respecto a la vulnerabilidad de la primera replica (R1) mediante las metodologías MAGERIT V3 y OCTAVE.

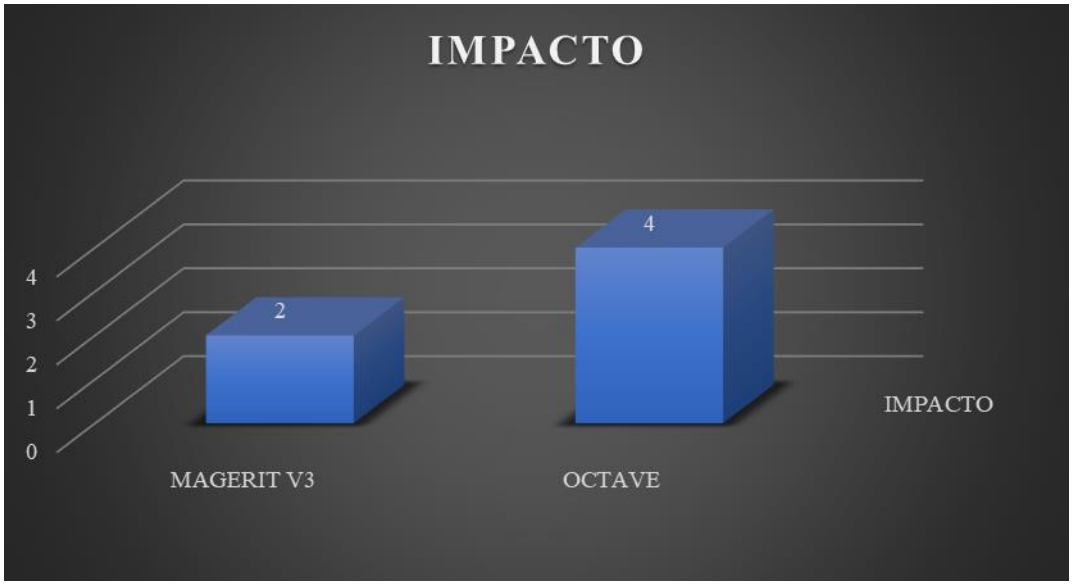
Con respecto a MAGERIT V3 el resultado es 3 lo que nos indica de acuerdo a la escala de valoración de vulnerabilidades ya dadas por la metodología “3= posible”, es de decir la probabilidad de ocurrencia de una amenaza es “posible”.

Con respecto a OCTAVE el resultado es 5 lo que nos indica de acuerdo a la escala de valoración de vulnerabilidades ya dadas por la metodología “5= Medio-Alto”, es de decir la probabilidad de ocurrencia de una amenaza es “Medio-Alto”.

3) Impacto de la primera replica (R1), MAGERTI V3 Y OCTAVE.

Figura 6

Impacto MAGERIT- OCTAVE.



Nota: Picoy (2017)

En la figura 6 observamos el resultado de la valoración general de los activos con respecto al impacto de la primera replica (R1) mediante las metodologías MAGERIT V3 y OCTAVE.

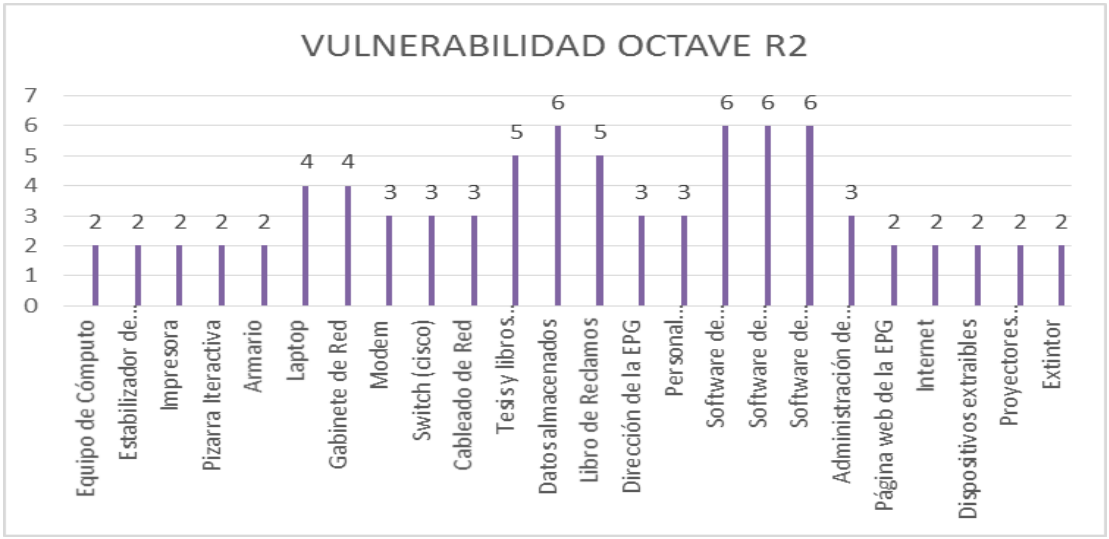
Con respecto a MAGERIT V3 el resultado es 2 lo que nos indica de acuerdo a la escala de valoración del impacto ya dadas por la metodología “2= menor”, es de decir la Materialización de una amenaza que conlleva a resultados desfavorables sobre un activo de la Escuela de Pos Grado es “menor”.

Con respecto a OCTAVE el resultado es 4 lo que nos indica de acuerdo a la escala de valoración del impacto ya dadas por la metodología “4= Medio”, es de decir la Materialización de una amenaza que conlleva a resultados desfavorables sobre un activo de la Escuela de Pos Grado es “Medio”.

4) Vulnerabilidad e Impacto de la segunda replica (R2), MAGERTI V3 Y OCTAVE Allegro

Figura 7

Vulnerabilidades OCTAVE -R^2

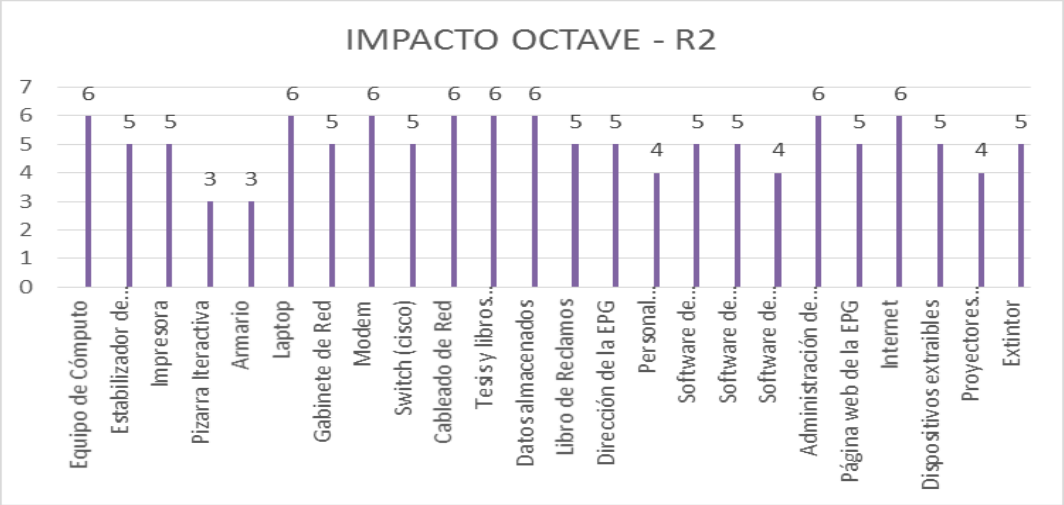


Nota: Picoy (2017)

En la figura 7 observamos el resultado de la valoración de cada activo con respecto a las vulnerabilidades de la segunda replica (R^2) mediante la metodología OCTAVE.

Figura 8

Impacto OCTAVE -R²

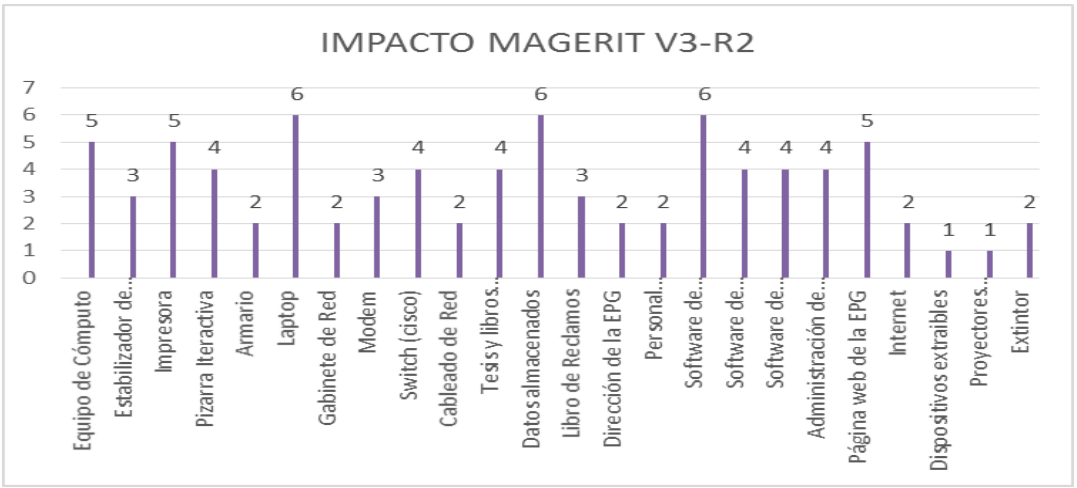


Nota: Picoy (2017)

En la figura 8 observamos el resultado de la valoración de cada activo con respecto al Impacto de la segunda replica (R^2) mediante la metodología OCTAVE.

Figura 9

Impacto MAGERIT V3 –R2

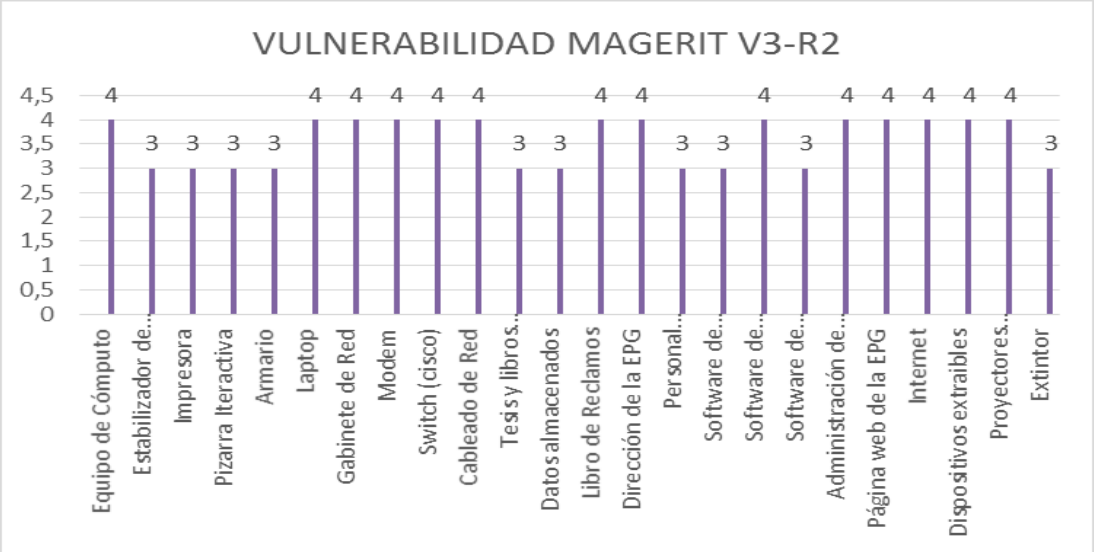


Nota: Picoy (2017)

En la figura 9 observamos el resultado de la valoración de cada activo con respecto al Impacto de la segunda replica (R^2) mediante la metodología MAGERIT V3.

Figura 10

Vulnerabilidades MAGERIT-R2



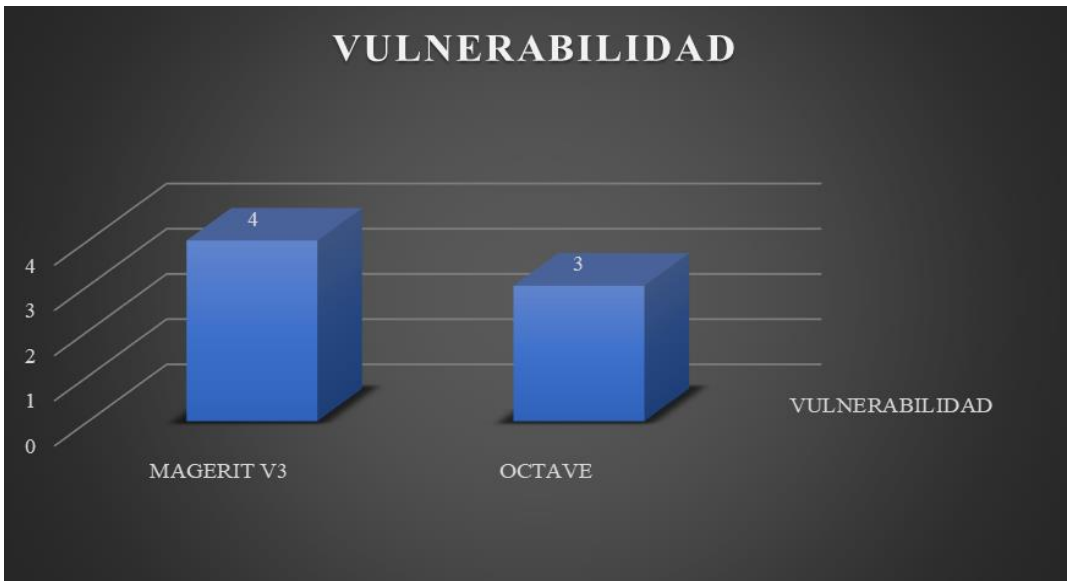
Nota: Picoy (2017)

En la figura 10 observamos el resultado de la valoración de cada activo con respecto a las vulnerabilidades de la segunda replica (R^1) mediante la metodología OCTAVE.

5) Vulnerabilidad de la segunda replica (R^2), MAGERTI V3 Y OCTAVE.

Figura 11

Vulnerabilidades MAGERIT OCTAVE



Nota: Picoy (2017)

En la figura 11 observamos el resultado de la valoración general de los activos con respecto a la vulnerabilidad de la segunda replica (R^2) mediante las metodologías MAGERIT V3 y OCTAVE.

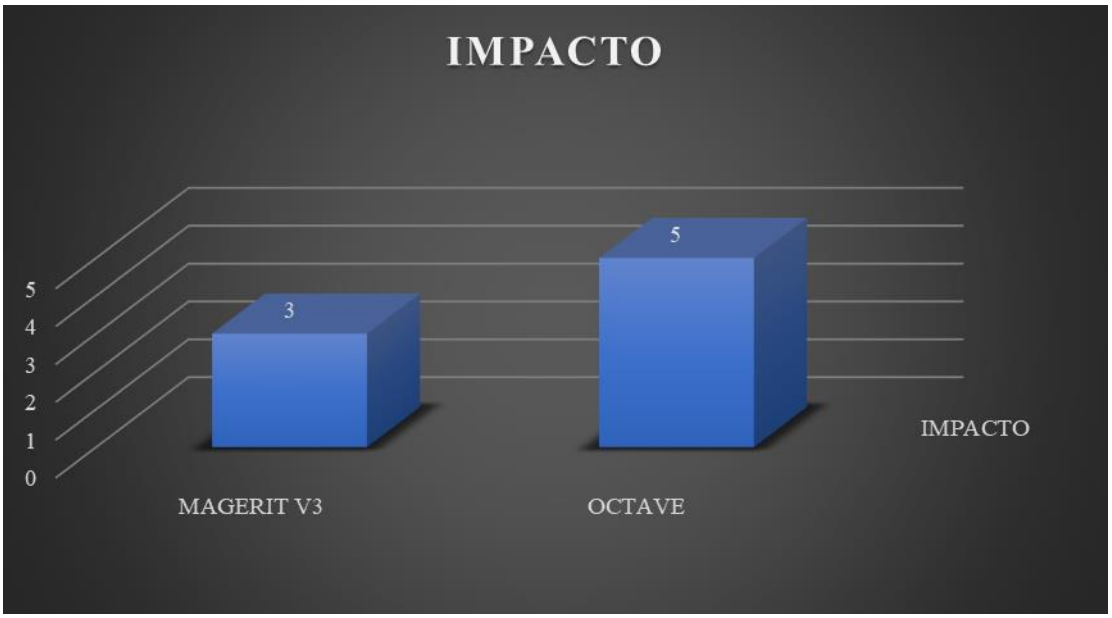
Con respecto a MAGERIT V3 el resultado es 3 lo que nos indica de acuerdo a la escala de valoración de vulnerabilidades ya dadas por la metodología “4= probable”, es de decir la probabilidad de ocurrencia de una amenaza es “probable”.

Con respecto a OCTAVE el resultado es 3 lo que nos indica de acuerdo a la escala de valoración de vulnerabilidades ya dadas por la metodología “3= Medio-Bajo”, es de decir la probabilidad de ocurrencia de una amenaza es “Medio-Bajo”

6) Impacto de la segunda replica (R^1), MAGERTI V3 Y OCTAVE.

Figura 12

Impacto MAGERIT V3- OCTAVE



Nota: Picoy (2017)

En la figura 12 observamos el resultado de la valoración general de los activos con respecto al impacto de la segunda replica (R^2) mediante las metodologías MAGERIT V3 y OCTAVE.

Con respecto a MAGERIT V3 el resultado es 2 lo que nos indica de acuerdo a la escala de valoración de impacto ya dadas por la metodología “2= menor”, es de

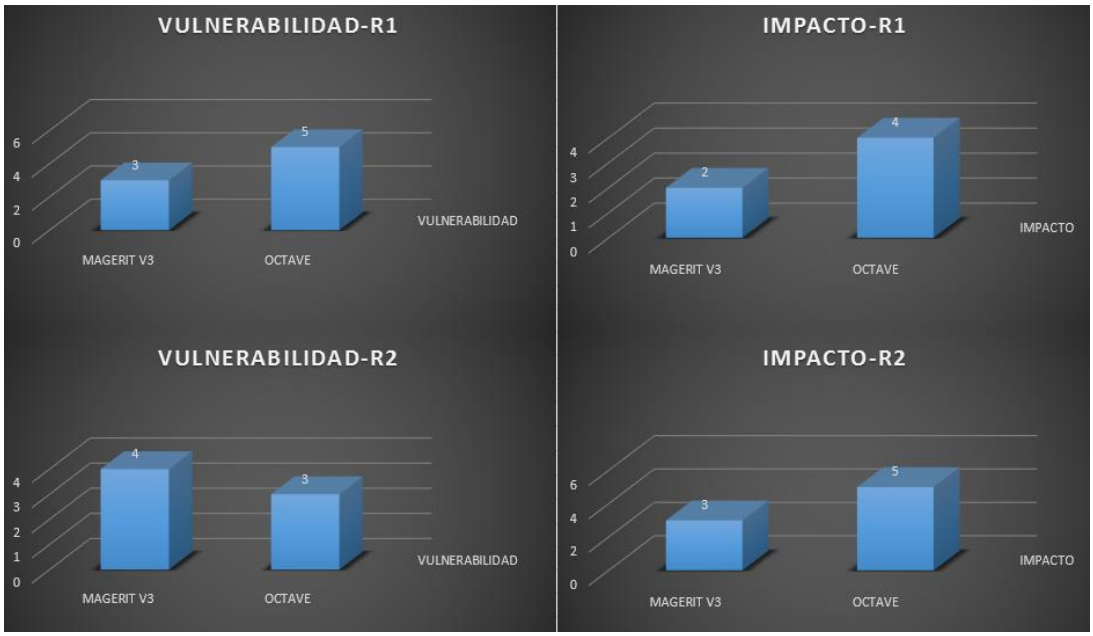
decir la Materialización de una amenaza que conlleva a resultados desfavorables sobre un activo de la Escuela de Pos Grado es “menor”.

Con respecto a OCTAVE el resultado es 5 lo que nos indica de acuerdo a la escala de valoración de impacto dadas por la metodología “5= Alto”, es de decir la Materialización de una amenaza que conlleva a resultados desfavorables sobre un activo de la Escuela de Pos Grado es “Alto”.

7) Vulnerabilidades e impacto de la primera y segunda replica, MAGERIT V3 Y OCTAVE

Figura 13

Resultado final de vulnerabilidad e impacto MAGERIT-OCTAVE



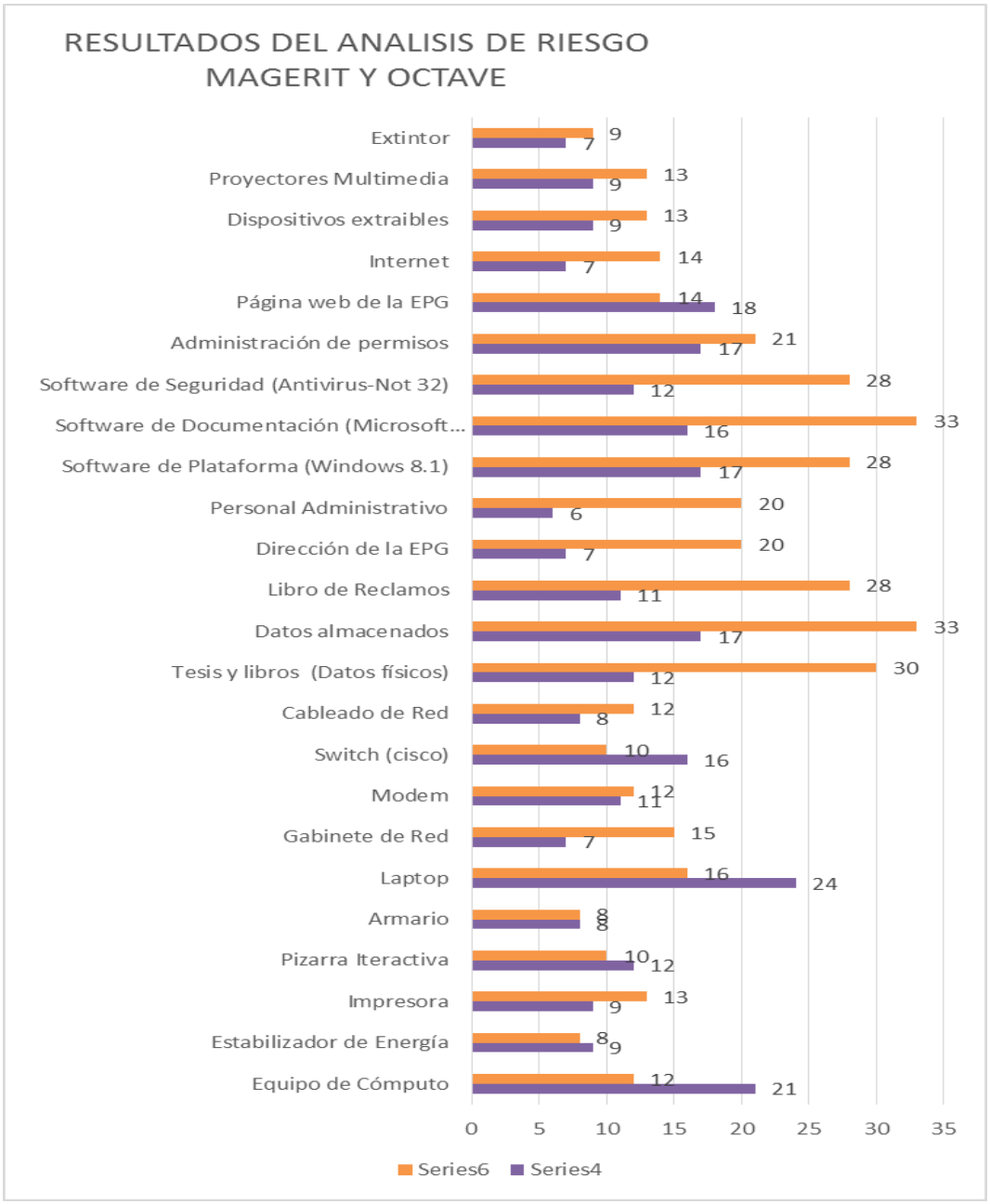
Nota: Picoy (2017)

Mediante los resultados de la figura 13 obtenidos de la aplicación de las metodologías MAGERIT V3 Y OCTAVE, se realizó la experimentación para determinar en qué medida la metodología MAGERIT es mejor a la metodología OCTAVE en el Análisis de riesgo; para así haber aplicado la metodología idónea para optimizar la seguridad de la información.

3.1. Gráficos de resultado de análisis de riesgo de Magerit y Octave

Figura 14

Análisis de riesgo MAGERIT y OCTAVE



Nota: La figura muestra el análisis de riesgo MAGERIT y OCTAVE. Picoy (2017)

- Magerit color lila
- Octave color naranja

En la figura 14 observamos el resultado final del análisis de riesgo, es decir el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la mediante las metodologías MAGERIT V3 y OCTAVE.

Mediante estos resultados la aplicación de las metodologías MAGERIT V3 Y OCTAVE, se realizó la experimentación para determinar en qué medida la metodología MAGERIT es mejor a la metodología OCTAVE en el Análisis de riesgo; así haber aplicado la metodología idónea para optimizar la seguridad de la información.

Obteniendo como resultado final de la experimentación; las siguientes tablas ANOVA.

a) Diseño factorial

Tabla 11

Diseño factorial

		G.L	SC	S^2 Varianza CM Ajust.	F	P
scA	FACTOR A	1	3.1250	3.1250	3.57	0.132
scB	FACTOR B	1	0.1250	0.1250	0.14	0.725
scAB	INTERACCION AB	1	1.1250	1.1250	1.29	0.320
scE	ERROR	4	3.5000	3.5000		
scT	TOTAL	7	**7.8750**	7.8750		

Nota: Picoy (2017)

- En la primera hipótesis nula del diseño:

$$H_0{}^{(1)}: \text{"El factor metodología no influye"}$$

El p-valor es mayor al nivel de confianza, es decir:

$$0.132 > 0.05$$

En vista del p-valor es mayor al nivel de confianza, se rechaza la hipótesis nula y se acepta la hipótesis alterna.

$$H_A{}^{(1)}: \text{"El factor metodología influye"}$$

- En la segunda hipótesis nula del diseño:

$H_0{}^{(2)}$: "El factor dimensiones no influye"

El p-valor es mayor al nivel de confianza, es decir:

$$0.725 > 0.05$$

En vista del p-valor es mayor al nivel de confianza, se rechaza la hipótesis nula y se acepta la hipótesis alterna.

$H_A{}^{(2)}$: "El factor dimensiones influye"

- En la tercera hipótesis nula del diseño:

$H_0{}^{(3)}$: "La interacción de los dos factores no influye"

El p-valor es mayor al nivel de confianza, es decir:

$$0.320 > 0.05$$

En vista del p-valor es mayor al nivel de confianza, se rechaza la hipótesis nula y se acepta la hipótesis alterna.

$H_A{}^{(3)}$: "La interacción de los dos factores influye"

3.2. Diseño unifactorial

Tabla 12

Diseño unifactorial

Fuente de variación	Suma de cuadrados	G.L	Cuadrados medios	F	P	Valor crítico para F
Metodologías	338,27	1	338,2727273	6,927394	0,1018	4,0762
Error	2050,91	42	48,83116883			
Total	2389,18	43				

Nota: Picoy (2017)

- En la hipótesis nula del diseño:

H_0: $No\ existe\ diferencia\ en\ el\ analisis\ de\ riesgo\ entre\ las\ metodologias$

El p-valor es mayor al nivel de confianza, es decir:

$$0.1018 > 0.05$$

En vista del p-valor es mayor al nivel de confianza, se rechaza la hipótesis nula y se acepta la hipótesis alterna.

$$H_1: \textit{Existe diferencia en el analisis de riesgo entre las metodologias}$$

3.3. Contrastación de las hipótesis

Contrastes que se deducen la tabla ANOVA son los siguientes:

3.3.1. Diseño factorial de 2 x 2

- ***Sobre la influencia del factor-tratamiento metodologías:***

$$H_0{}^{(1)}\text{: "El factor metodología no influye"}$$

$$A_i = 0;\ \text{i} = 1{,}2$$

$$\hat{F}_A: \frac{\widehat{S^2}_A}{\widehat{S^2}_E} = \frac{3.1250}{0.8750} = 3.57 \sim F_{1,4} => p - valor = 0.132$$

$$F_{(\alpha,\, a-1,\, N-a)} = F_{(0.05,\, 0\,,7)} = 0{,}132$$

$$0.132 < 3.57$$

Se acepta la hipótesis nula de no influencia del factor metodologías, en el análisis de riesgos.

- ***Sobre la influencia del factor-tratamiento Dimensiones:***

$$H_0{}^{(2)}\text{: "El factor dimensiones no influye"}$$

$$B_i = 0;\ \text{j} = 1{,}2$$

$$\hat{F}_A: \frac{\widehat{S^2}_B}{\widehat{S^2}_E} = \frac{0.1250}{0.8750} = 0.14 \sim F_{1,4} => p - valor = 0.725$$

$$F_{(\alpha,\, b-1,\, N-a)} = F_{(0.05,\, 0\,,7)} = 0{,}725$$

$$0.725 > 0.14$$

Se rechaza la hipótesis nula de no influencia del factor dimensiones, en el análisis de riesgos.

- ***Sobre la influencia de la interacción de los dos factores.***

$$H_0{}^{(3)}\text{: "La interacción de los dos factores no influye"}$$

$$(AB)_{ij} = 0;\ \text{i,j} = 1,2$$

$$\hat{F}_A : \frac{\widehat{S^2}_{AB}}{\widehat{S^2}_E} = \frac{1.1250}{0.8750} = 0.14 \sim F_{1,4} => p - valor = 0.320$$

$$F_{(\alpha,\ ab-1,\ N-a)} = 0.320$$

$$0.320 < 4.0726$$

Se acepta la hipótesis nula de no influencia de la interacción de los factores en el análisis de riesgos.

Lo que significa que no influye el efecto simple de las metodologías|, si influye el efecto simple de las dimensiones y no influye el efecto de interacción entre las metodologías (Magerit y octave) y las dimensiones (vulnerabilidad e impacto), con una confianza estadística del 95%

3.3.2.Diseño unifactorial

- Considerando las siguientes hipótesis nula y alterna, respectivamente.

$$H_0\text{: } \mu_1 = \mu_2\ (No\ existe\ diferencia\ en\ el\ analisis\ de\ riesgo\ entre\ las\ metodologias)$$

$$H_1\text{: } \mu_1 \neq \mu_2\ (\ Existe\ diferencia\ en\ el\ analisis\ de\ riesgo\ entre\ las\ metodologias)$$

Utilizando un nivel de significancia del 5% ($\alpha = 0.05$), para encontrar el $F_{(0,05:3;16)}$ (Tablas Fisher) con1 grados de libertad (a-1) en el numerador y 42 grados de libertad (N-a) en el denominador.

$$F_{(\alpha,\ a-1,\ N-a)} = F_{(0.05,\ 1\ ,42)} = 4{,}0726$$

Comparando el $F_{(0)}$ calculado en el análisis de varianza y el $F_{(0,05:3;16)}$, se puede observar que $F_{(0)}$ cae en la zona de rechazo:

$$F_{(0)} > F_{(0.05,\ 1\ ,42)}$$

$$6{,}9273 > 4{,}0726$$

Por tanto, se rechaza la hipótesis nula y se acepta la hipótesis alterna.

Propuesta de mejora para minimizar los riesgos en la seguridad de la información

Figura 15

Propuesta de mejora para minimizar los riesgos en la seguridad de la información

	N°	CAPA	CÓDIGO	ACTIVO	UN	COSTO UNITARIO	COSTO TOTAL	DIMENSIONES				
								[D]	[I]	[C]	[A]	[T]
ACTIVOS ESENCIALES [essential]	AED1	DATOS [da	[dal]	Datos almacenados	-	-	-	6	6	5		
	AED2	INFORMACIÓN [info]	[cyl]	Tesis y Libros (Datos físicos)	-	-	-	5	4	3		
	AED3		[ldr]	Libro de Reclamos	-	-	-	5		2	1	
	AED4	SERVICIO [service	[adp]	Administración de permisos	-	-	-	3			5	5
APLICACIONES INFORMÁTICAS [apps]	APS1	SOFTWARE [SW]	[sdp]	Software de Plataforma (Windows 8.	-	-	-	4			5	8
	APS2		[sdd]	Software de Documentación (Microf	-	-	-	4		4		
	APS3		[sps]	Software de estadística (SPSS)	-	-	-	4		4		
	APS4		[ags]	Software de Información Geográfica	-	-	-	4		4		
	APS5		[sds]	Software de Seguridad (Antivirus - ES	-	-	-	3	5			
	APS6		[web]	Página web (http://posgrado.unheva	-	-	-	8	4	2	4	4
EQUIPOS INFORMÁTICOS [einf]	EIH1	HARDWARE [HW]	[edc]	Equipo de Cómputo	-	-	-	6	5	5		
	EIH2		[imp]	Impresora	-	-	-	3				
	EIH4		[lap]	Laptop	-	-	-	6	5	7		
	EIH5		[mod]	Modem	-	-	-	4	2		2	
	EIH6		[swt]	switch (Cisco)	-	-	-	6	5	3	4	2
	EIH7		[svd]	Servidor	-	-	-	6	5	5		
COMUNICACIONES	CRC1	REDES DE COMU	[int]	Internet	-	-	-	4	2	1	1	
SOPORTE DE INFORMATICO	SIS1	SOPORTE [med]	[ext]	Dispositivo Extraible (CD/DVD, USB)	-	-	-	1	1	1		1
	SIS2		[cmr]	Cámara de video	-	-	-	1	1			1
	SIS3		[pro]	Proyector multimedia	-	-	-	1	1			1
EQUIPAMIENTO AUXILIAR [eax]	EAE1	EQUIPAMIENTO [aux]	[est]	Estabilizador de energía	-	-	-	5	3			1
	EAE2		[cab]	Cableado de red	-	-	-	3		1		
	EAE3		[ext]	Extintor	-	-	-	3	3			1
INSTALACIONES [ins]	INI1	INSTALACIONES	[arm]	Armario	-	-	-		3	2	1	
	INI2		[gab]	Gabinete de Red	-	-	-	4	2			1
PERSONAL [per]	PSP1	PERSON	[ddf]	Director de la Escuela de Posgrado	-	-	-		2	2	2	
	PSP2		[sec]	Personal Administrativo	-	-	-	3	1			

Nota: Picoy (2017)

CAPITULO 4

DISCUSIÓN, CONCLUSIONES Y RECOMENDACIONES

Discusión, conclusiones y recomendaciones

Una vez finalizado el trabajo de investigación y haber desarrollado el diseño experimental factorial y Unifactorial, obtuvimos los siguientes resultados:

- **Resultado del diseño factorial 2x2**

Trabajando con las siguientes hipótesis nula y alterna, respectivamente.

$H_0{}^{(1)}$: "El factor metodología no influye"

$H_0{}^{(2)}$: "El factor dimensiones no influye"

$H_0{}^{(3)}$: "La interacción de los dos factores no influye"

$H_A{}^{(1)}$: "El factor metodología influye"

$H_A{}^{(2)}$: "El factor dimensiones influye"

$H_A{}^{(3)}$: "La interacción de los dos factores influye"

Después de haber demostrado que p-valor (0.132) de la primera y p-valor (0.320) de la tercera hipótesis son menores al F calculado (3.57) de la primera y al F calculado (1.29) de la tercera hipótesis), aceptamos las hipótesis nulas y, rechazamos la segunda hipótesis nula debido a que p-valor (0.725) es mayor al F calculado (0.14), teniendo como significa verbal o resultado final; lo siguiente:

$H_c{}^{(1)}$: $El\ factor\ metodologías\ no\ influye\ significativamente\ en\ el\ análisis\ de\ riesgos.$

$H_c{}^{(2)}$: $El\ factor\ dimensiones\ influye\ significativamente\ en\ el\ análisis\ de\ riesgos.$

$H_c{}^{(3)}$: $la\ interaccion\ de\ los\ factores\ no\ influyen\ significativamente\ en\ el\ análisis\ de\ riesgos.$

- **Resultado del diseño Unifactorial**

Trabajando con las siguientes hipótesis nula y alterna, respectivamente.

H_0: $No\ existe\ diferencia\ en\ el\ analisis\ de\ riesgo\ entre\ las\ metodologias$

H_1: *Existe diferencia en el analisis de riesgo entre las metodologias*

Después de haber demostrado que p-valor (0.1018) es mayor al nivel de confianza (0.05), aceptamos la hipótesis nula teniendo como significa verbal o resultado final; lo siguiente:

H_0: *La metodología no influye en el análisis de riesgo o no hay diferencia significativa en el análisis de riesgo entre las metodologías de MAGERIT Y OCTAVE.*

En base al resumen de los resultados mostrados en este capítulo, rechazamos las siguientes hipótesis:

Hipótesis general:

La metodología MAGERIT es mejor que la metodología OCTAVE en el Análisis de riesgo en la Escuela de Pos Grado de la Universidad Nacional Hermilio Valdizan Huánuco 2017.

Hipótesis Específicas

- La metodología MAGERIT identifica mejor las amenazas en el análisis de riesgo que la metodología OCTAVE, en la Escuela de Pos Grado de la Universidad Nacional Hermilio Valdizan Huánuco 2017.
- La metodología MAGERIT identifica mejor las vulnerabilidades en el análisis de riesgo que la metodología OCTAVE, en la Escuela de Pos Grado de la Universidad Nacional Hermilio Valdizan Huánuco 2017.
- La metodología MAGERIT identifica y tipifica mejor los impactos en el análisis de riesgo que la metodología OCTAVE, en la Escuela de Pos Grado de la Universidad Nacional Hermilio Valdizan Huánuco 20162016.

Determinamos que tanto la metodología magerit como la metodología octave, no tienen diferencia significativa en el análisis de riesgo, por lo que es indiferente el uso de cualquiera de ellas para la identificación de amenazas, vulnerabilidades e impactos en el análisis de riesgo para la administración de la seguridad de la información en la Escuela de Pos Grado o cualquier otra de la misma índole.

De tal manera que para la ejecución del análisis de riesgos se adopta el ciclo de mejora continua PHVA como lo recomienda la norma ISO/IEC 27001, el cual consta de 3 etapas:

Etapa 1: La primera etapa fue un reconocimiento de infraestructura física y tecnológica, así como la recolección de documentación e información relevante para el desarrollo del proyecto.

Etapa 2: En esta fase luego de comprender la estructura organizacional y su manera de operación, basada en el modelo de negocio (actividad principal) de la institución, se clasifican activos por criticidad, se definen planes para realizar y obtener datos sobre el estado de seguridad a nivel hardware y software de equipos, servicios, procesos y procedimientos; además de conseguir información con respecto a instalaciones físicas.

Etapa 3: Con la información obtenida y el otorgamiento de acceso restringido sobre ciertos servicios, equipos o servidores y conociendo el direccionamiento e infraestructura tecnológica, se procede con el montaje de un escenario de pruebas, basado en herramientas de escaneo y análisis para detectar posibles vulnerabilidades a nivel de servicios, protocolos o puertos; pruebas sobre conformación de contraseñas, modos de acceso y en general test que se encaminan a determinar el estado actual de seguridad en la infraestructura de red e información a nivel general.

Obteniendo como resultado un sistema de uso interno para registrar las reservas de los salones de clases, salas de conferencia, salas de cómputo y demás salas de reuniones que existen dentro de la Institución. Es un SIGAA, la aplicación web con PHP y MySQL/pgsql/SQLSERVER, es de acceso público ya que cualquier persona puede acceder para consultar este sistema desde cualquier terminal conectado a la red de la Institución para obtener información actualizada de salas, laboratorios y salones de clase, su disponibilidad y ocupación en un momento dado.

Es así que con los activos más importantes previamente identificados se procede a realizar la evaluación de riesgos. Proceso base para poder identificar su nivel de importancia y criticidad dentro del modelo de negocio de la Universidad Nacional Hermilio Valdizán de Huánuco.

No se tienen definidos procedimientos para realizar mantenimiento correctivo y preventivo a nivel técnico, cada persona de soporte procede según el problema o incidencia de acuerdo a su experiencia y conocimiento, pero muchas veces la solución, aunque puede ser exitosa no es la más efectiva o la más eficaz, por lo tanto, se deben normalizar todos los procedimientos técnicos.

Así como no se tienen definidas restricciones para el uso de dispositivos de almacenamiento tipo USB, aunque se tiene un sistema de protección contra virus y spyware para minimizar los riesgos por contagio de virus, las unidades de almacenamiento USB pueden infectar fácilmente un sistema.

También ante una falla irrecuperable de hardware en un equipo de cómputo de uso crítico, no se tienen estipulados planes de contingencia que permitan hacer un proceso de recuperación de una manera rápida y más grave aún es que no solo se pueda recuperar la información que se pueda comprometer.

Así mismo no se tienen procedimientos definidos, ni registros de la aplicación de actualizaciones de software o parches de seguridad en los sistemas base críticos

En cuanto a la red se encuentra segmentada física y lógicamente en la totalidad en nuestro campus, en la facultad de Veterinaria y Agronomía no se efectúa la segmentación de las diferentes subredes, lo cual además de ayudar a mejorar la seguridad de la red, mejora el rendimiento y reduce el tráfico innecesario. Se debe realizar esta actividad cuanto antes para disminuir la probabilidad de que se materialice cualquier amenaza.

En el campus y en las dos facultades que se encuentra fuera; se comunican por medio de un enlace de fibra óptica a 30Mbps y antena, en cuanto a servicios de red específicos institucionales y se provee el servicio de internet también por este medio. La redes en cada local son diferentes a nivel de direccionamiento y los enlaces a servicios o servidores específicos son administrados por medio de mapeo interno de direcciones entre los Firewall y VLANs en los Switches, el problema ocasionado por este modelo de infraestructura tecnológica implementado, es que se crean cuellos de botella en el firewall-UTM (Unified Theat Management) que se tiene en funcionamiento, ya que no está diseñado para soportar el nivel de carga y tráfico de red actual. Es necesario replantear el esquema y modelo de red actual con el fin de unificar la red en los diferentes

locales con el fin de mejorar en rendimiento, facilidad de administración y eliminación de posibles puntos de falla.

Así como en el campus principal el estado del cableado estructurado no es la adecuada en su totalidad, aunque existe cableado tipo UTP categoría 6 casi en el 80% de la edificación, este no cumple con las normas mínimas de instalación en algunos casos; por ejemplo, los armarios de cableado, patchpanel y patch-cord están en malas condiciones, desorganizados y sin seguridad alguna (Cualquier persona tiene acceso al cableado o switches dentro del armario). El cableado de red y eléctrico en el campus principal no está certificado por la norma RETIE (Reglamento Técnico de Instalaciones Eléctricas) y a nivel de red de datos en ANSI/TIA 568A-B.

Aporte científico de la investigación

Nuestro resultado se asemeja a lo planteado por la metodología COBIT (4) ya que podemos afirmar que: La política de seguridad de la información debe ser revisada regularmente a intervalos planeados o si ocurren cambios significativos para asegurar la continua idoneidad, eficiencia y efectividad, siendo un objetivo de control de la metodología COBIT.

También se deben de identificar y revisar regularmente los requerimientos de confidencialidad o los acuerdos de no-divulgación reflejando las necesidades de la organización para la protección de la información, tal como lo afirma COBIT en sus acuerdos de confidencialidad.

Así como para la protección contra software malicioso se deben implementar controles de detección, prevención y recuperación para protegerse de códigos malicioso y se deben implementar procedimientos de conciencia apropiados, en sus controles.

Y finalmente se deben identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con los medios de procesamiento de la información, obteniendo así un perímetro de seguridad física.

Se concluye que la Universidad Nacional Hermilio Valdizán de Huánuco actualmente presenta un nivel de riesgo informático considerable, que con el

apoyo de las directivas (alta gerencia) y de todo el personal es posible contrarrestar.

Como aporte científico de investigación, concretamos señalando que ambas metodologías no tienen diferencia significativa en su aplicación en el análisis de riesgo, por lo que el uso de cualquiera de ellas es indiferente en la obtención de los resultados planteados en un trabajo de investigación o proyecto.

4.1. Conclusiones

- Luego de revisar y desarrollar investigaciones sobre el análisis de riesgos, hemos determinado lo siguiente:
- Las metodologías MAGERIT y OCTAVE identifican amenazas de manera similar en el análisis de riesgo de los sistemas de información de la Escuela de Posgrado de la Universidad Nacional Hermilio Valdizan, Huánuco.
- La metodología MAGERIT también identifica vulnerabilidades en el análisis de riesgo de los sistemas de información de la Escuela Superior de la Universidad Nacional Hermilio Valdizan, Huánuco.
- La metodología OCTAVA de igual forma identifica y caracteriza los impactos en el análisis de riesgo de los sistemas de información de la Escuela Superior de la Universidad Nacional Hermilio Valdizan, Huánuco.

4.2. Recomendaciones

A partir de los resultados obtenidos, se recomienda lo siguiente:

A los profesionales y/o estudiantes, interesados en desarrollar algún trabajo relacionado al análisis de riesgos en alguna Escuela de Pos Grado o institución académica, el decidir trabajar con la metodología MAGERIT u OCTAVE, es irrelevante, debido a que ambos miden de forma similar las amenazas, vulnerabilidades e impactos, para la realización de un correcto análisis de riesgos.

Referencias Bibliográficas

Referencias Bibliográficas

Caralli, R., Stevens, J., Young, L., & Wilson, W. (2007). Introducción a Octave Allegro: Mejora del Proceso de Evaluación de Riesgos de Seguridad de la Información. El Instituto de Ingeniería de Software.

Consejo Superior de Administración Electrónica. (2012). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Colección: administración electrónica.

Gallardo Piedra, M., & Jácome Cordones, P. (2011). Análisis de Riesgos Informáticos y Elaboración de un Plan de Contingencia T.I. para la Empresa Eléctrica Quito S.A. Tesis.

Gaona Vásquez, K. (10 de 2013). Aplicación de la Metodología MAGERIT para el Análisis y Gestión de Riesgos de la Seguridad de la Información Aplicado a la Empresa Pesquera e Industrial Bravito S.A. En La Cuidad De Machala. Universidad Politécnica Salesiana.

Garcia Hanson, J., & Salazar Escobar, P. (2005). Métodos De Administración Y Evaluación De Riesgos. Universidad de Chile.

ISO 27001. (2013). Sistema de Gestión de la Seguridad de la Seguridad.

ISO Guide 73. (2009). Risk management — Vocabulary.

kuehl, R. (2001). Diseño de experimentos.

Lucero G., A., & Valverde P., J. (2012). “Análisis y gestión de los sistemas de la Cooperativa de Ahorro y Crédito Jardín Azuayo, utilizando la metodología MAGERIT. Tesis.

MAGERIT. (1997). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Madrid.

Perafán Ruiz, J., & Caicedo Cuchimba, M. (2014). Análisis de Riesgos de la Seguridad de la Información para la Institución. Tesis.

Porras, L. (2000). Diseño Estadístico de Experimentos, Análisis de la Varianza y Temas Relacionados: Tratamiento Informático mediante SPSS. Proyecto Sur de Ediciones.

Talavera Álvarez, V. (2015). Diseño de un Sistema de Gestión de Seguridad de la Información para una Entidad Estatal de Salud de Acuerdo a la ISO/IEC 27001:2013. Tesis.

UNE 71504. (2008). “Metodología de análisis y gestión de riesgos para los sistemas de información”.

UNE-ISO Guía 73. (2010). “Gestión del riesgo. Vocabulario”..

RESUMEN

El libro de investigación, contiene el informe sistematizado sobre el análisis de riesgos de la seguridad de la información para la Universidad Nacional Hermilio Valdizán de Huánuco, tuvo como objetivo realizar el análisis de riesgos que permita generar controles para minimizar la probabilidad de ocurrencia e impacto de los riesgos asociados con las vulnerabilidades y amenazas de seguridad de la información existentes en la Universidad Nacional Hermilio Valdizán de Huánuco. El método aplicado tuvo la finalidad de profundizar el análisis e interpretación de los resultados en donde se utilizó el tipo de investigación aplicada de diseño no experimental, descriptivo, se trabajó con una muestra total de los activos informáticos de la Universidad Nacional Hermilio Valdizán de Huánuco, seleccionados mediante el tipo de muestreo no probabilístico intencional. Para estimar los estadígrafos se usó la estadística descriptiva e inferencial. Obteniendo como resultado la disminución del riesgo actual de los activos informáticos a su nivel mínimo.

Palabras Clave: amenazas, impacto, salvaguardas.

http://www.editorialgrupo-aea.com

Editorial Grupo AeA

editorialgrupoaea

Editorial Grupo AEA

ISBN: 978-9942-651-12-9