UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN

ESCUELA DE POSGRADO

DETERMINACIÓN DE LA METODOLOGÍA PARA ANALIZAR Y PROPONER MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN DE LA ESCUELA DE POS GRADO DE LA UNIVERSIDAD NACIONAL HARMILIO VALDIZAN, 2017

TESIS PARA OPTAR EL GRADO ACADÉMICO DE DOCTOR EN CIENCIAS DE LA EDUCACIÓN

TESISTA: JUAN ANTONIO PICOY GONZALES

ASESOR: DR. GERARDO GARAY ROBLES

HUÁNUCO – PERU

2017

DEDICATORIA

A mi esposa e hijos por ser la razón de mi superación en todos los campos de mi vida.

AGRADECIMIENTO

A los docentes de la UNHEVAL por haberme asesorado para la elaboración de la tesis.

A la Escuela de Pos Grado por facilitarme la información necesaria;

A la ing. Kiausia Arianna Retiz Taboada por el apoyo en la valoración de las metodologías empleadas.

RESUMEN

La ejecución de la presente investigación, contiene el informe sistematizado sobre el análisis de riesgos de la seguridad de la información para la Universidad Nacional Hermilio Valdizán de Huánuco, siendo un aporte científico. Tiene 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 uso la estadística descriptiva e inferencial y para la contrastación de la hipótesis se aplicó la prueba de correlaciones. Obteniendo como resultado la disminución del riesgo actual de los activos informáticos a su nivel mínimo.

PALABRAS CLAVES: Amenazas, Impacto, Salvaguardas.

SUMMARY

The execution of the present investigation contains the systematized report on the risk analysis of information security for the National University Hermilio Valdizán de Huánuco, being a scientific contribution. Its objective is: Perform the risk analysis that allows the generation of controls to minimize the probability of occurrence and impact of the risks associated with the security vulnerabilities and threats existing in the National University Hermilio Valdizán de Huánuco. The applied method had the purpose of deepening the analysis and interpretation of the results in which the type of applied non-experimental, descriptive design research was used, with a total sample of the computer assets of the National University Hermilio Valdizán de Huánuco, selected by the type of intentional non-probabilistic sampling. To estimate the statisticians, descriptive and inferential statistics were used and for the test of the hypothesis the correlation test was applied. Obtaining as a result the reduction of the current risk of the computer assets to its minimum level.

KEY WORDS: Threats, Impact, Safeguard.

RESUMO

A execução da presente investigação contém o relatório sistematizado sobre a análise de risco da segurança da informação para a Universidade Nacional Hermilio Valdizán de Huánuco, sendo uma contribuição científica. O objetivo é: Realizar a análise de risco que permite a geração de controles para minimizar a probabilidade de ocorrência e impacto dos riscos associados às vulnerabilidades de segurança e ameaças existentes na Universidade Nacional Hermilio Valdizán de Huánuco. O método aplicado teve como objetivo aprofundar a análise e interpretação dos resultados em que foi utilizado o tipo de pesquisa de projeto descritivo não experimental experimental, com uma amostra total dos ativos informáticos da Universidade Nacional Hermilio Valdizán de Huánuco, selecionados pelo tipo de amostragem intencional não-probabilística. Para estimar os estatísticos, foram utilizadas estatísticas descritivas e inferenciais e, para o teste da hipótese, o teste de correlação foi aplicado. Obtendo, como resultado, a redução do risco atual de ativos de computador para seu nível mínimo.

PALAVRAS-CHAVE: Ameaças, Impacto, Salvaguardas.

INTRODUCCIÓN

Las instituciones que brindan servicios de educación superior y de Pos Grado 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. El alumno, los docentes y el personal administrativo de las instituciones que brindan servicios de enseñanza de Pos Grado, necesitan de tecnologías de información y comunicación que sean confiables y actualizados. El equipamiento en las instituciones de Pos Grado 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 Pos Grado 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 Pos 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 Pos Grado; por ende es importante que toda organización pública tenga políticas de seguridad de los sistemas de información

ÍNDICE

CAPITULO I

EL PROBLEMA DE INVESTIGACIÓN

1.1 DESCRIPCIÓN DEL PROBLEMA.

En la actualidad, vivimos un ritmo de vida con el constante acicate de lo novedoso, práctico y funcional que podemos observar en todos los ámbitos del desarrollo y de nuestra vida: transporte, vivienda, comunicaciones, servicios, medicina…La educación ya sea formal e informal no escapa a este constante bombardeo de la ciencia y la tecnología aplicad7a a la vida moderna.

Las instituciones que brindan servicios de educación superior y de Pos Grado 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. El alumno, los docentes y el personal administrativo de las instituciones que brindan servicios de enseñanza de Pos Grado, necesitan de tecnologías de información y comunicación que sean confiables y actualizados. El equipamiento en las instituciones de Pos Grado 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 Pos Grado de la Universidad Nacional Hermilio Valdizán, en el semetre académico 2016_I se contaba con mil doscientos alumnos matriculados y el semetre 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 Pos 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 genra mal clima laboral e incomodidad de las personas que estudian y que laboran en la escuela de Pos Grado; por ende es importante que toda organización pública tenga políticas de seguridad de los sistemas de información.

En tal sentido, la Escuela de Pos Grado, tiene vulnerabilidades que se hacen presente quebrantando la seguridad de la información atacando su confidencialidad, integridad y disponibilidad de la información, Si no se realiza un análisis para salvaguardar los recursos de la Escuela de Pos Grado, considerando como activo más importante la información; lo más probable es que se les presente una situación en la que la entrega de un documento digita sea de suma importancia o en los plazos establecidos y resulte que este está dañado, ocasionándoles problemas graves, desde calificaciones desaprobatorias por los docentes y despidos hasta sanciones administrativas al personal administrativo, además de un clima laboral caótico.

Por esta razón se pretende determinar la metodología que se debe usar para analizar y proponer mejoras en la seguridad de los sistemas de información en la Escuela de Pos Grado de la UNHEVAL para el cual solo se consideró: la metodología MAGERIT y la metodología OCTAVE en el Análisis de riesgo para optimizar la seguridad de la información aplicado la metodología idónea, La aplicación del análisis de riesgo mediante estas metodologías nos permitirá evaluar qué tan seguros son nuestros sistemas, cuantificando y comparando los requerimientos de seguridad de la información, determinar los activos y sus características de mayor valor, considerando los criterios del ACID (Autenticación, Confidencialidad, Integridad, Disponibilidad y No Repudio), identificar salvaguardas existentes, amenazas, su origen y el tipo de vulnerabilidad que pueden afectar la estimación y valoración

de impactos, concluyendo en la evaluación de riesgos a los que se encuentran expuestos los activos de la Escuela de Pos Grado.

1.2 FORMULACIÓN DEL PROBLEMA.

1.2.1 Problema general.

¿Qué metodología es mejor para el análisis de riesgo y proponer mejoras en la seguridad de la información de la Escuela de Pos Grado de la Universidad Nacional Hermilio Valdizán, 2017?

1.2.2 Problemas específicos

- ¿Qué metodología identifica mejor las amenazas para el análisis de riesgo en la Escuela de Pos Grado?
- ¿Qué metodología identifica mejor las vulnerabilidades para el análisis de riesgo en la Escuela de Pos Grado?
- ¿Qué metodología identifica mejor los impactos para el análisis de riesgo en la Escuela de Pos Grado?
- ¿Cuáles es la propuesta de mejoras en la seguridad de la Información de la escuela de Pos Grado?

1.3 OBJETIVO GENERAL Y OBJETIVOS ESPECÍFICOS.

1.3.1 Objetivo General

Determinar la mejor metodología para el análisis de riesgo, y propuesta de mejora en la Escuela de Pos Grado de la Universidad Nacional Hermilio Valdizan, 2017.

1.3.2 Objetivo Específicos

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

1.4 HIPÓTESIS Y/O SISTEMA DE HIPÓTESIS.

1.4.1 Hipótesis General

MAGERIT es la mejor metodología para el Análisis de riesgo y proponer mejoras en la Escuela de Pos Grado de la Universidad Nacional Hermilio Valdizán, 2017.

1.4.2 Hipótesis Específicas

- MAGERIT es la mejor metodología que identifica las amenazas en el análisis de riesgo en la Escuela de Pos Grado.
- MAGERIT es la mejor metodología que identifica las vulnerabilidades en el análisis de riesgo en la Escuela de Pos Grado.

- MAGERIT es la mejor metodología que identifica los impactos en el análisis de riesgo en la Escuela de Pos Grado.

- La aplicación de la propuesta de mejora en la seguridad de la Información de la escuela de Pos Grado, mejorará la seguridad de la Información

1.5 VARIABLES

1.5.1 Variable Independiente

Las metodologías.

1.5.2 Variable Dependiente

Análisis de Riesgo y Propuesta de Mejora.

1.5.3 Variable Interviniente

Escuela de Pos Grado.

1.6 JUSTIFICACIÓN E IMPORTANCIA.

La Escuela de Pos Grado de la Universidad Nacional Hermilio Valdizán de Huánuco, no cuenta con políticas de seguridad y mecanismos de salvaguarda que puedan gestionar los riesgos a los que se encuentran expuestos sus activos de mayor valor, como Escuela de Pos Grado en proceso de acreditación, viene desarrollando sus actividades orientadas a la mejora de la calidad educativa, parte de ello, involucra la evaluación de la seguridad de la información, protección y desempeño efectivo de los activos para evitar la duplicación de actividades. Una adecuada y oportuna toma de decisiones y el uso eficaz y eficiente de la información a través del análisis de riesgo.

La aplicación del análisis de riesgo mediante las metodologías MAGERIT Y OCTAVE nos permitirá evaluar qué tan seguros son nuestros sistemas, cuantificando y comparando los requerimientos de seguridad de la información, determinar los activos y sus características de mayor valor, considerando los criterios del ACID (Autenticación, Confidencialidad, Integridad, Disponibilidad y No Repudio), identificar salvaguardas existentes, amenazas, su origen y el tipo de vulnerabilidad que pueden afectar la estimación y valoración de impactos, concluyendo en la evaluación de riesgos a los que se encuentran expuestos los activos de la Escuela de Pos Grado. De esta manera, el trabajo de investigación se justifica porque constituye un aporte para la Escuela de Pos Grado de la Universidad Nacional Hermilio Valdizán de Huánuco, porque se pretende determinar la medida en la que la metodología MAGERIT es mejor a la metodología OCTAVE en el Análisis de riesgo para optimizar la seguridad de la información aplicado la metodología idónea y de esta manera posteriormente a la investigación plantear salvaguardas, estrategias de protección y un despliegue de medidas de seguridad declaradas en políticas de seguridad, considerando estándares y normativas vigentes para controlar, confrontar, gestionar el riesgo minimizándolo hasta niveles aceptables y para conocer los beneficios, costos y oportunidades que esto implica.

1.7 DELIMITACIONES

Se establece la limitación de la investigación sobre las características con las que debe disponer el sistema y los métodos especializados que existen para el desarrollo del mismo.

1.7.1 Limitación Temporal

La investigación se desarrolló en un periodo de cinco meses. Para elaborar un diagnóstico correcto del análisis de riesgo de los activos utilizando las metodologías MAGERIT Y OCTAVE para determinar cuál es la mejor metodología en la Escuela de Pos Grado-UNHEVAL, es un tiempo prudente para lograr los objetivos planteados inicialmente. .

1.7.2 Limitación Espacial

En las instalaciones de la Escuela de Pos Grado -UNHEVAL

1.8. LIMITACIONES

Se tuvo limitaciones en el acceso a la información de los recursos para poder contrastar con el inventario físico de la Escuela de Pos Grado porque los trabajadores utilizan en el horario de trabajo dichos recursos; por lo que se optó en coordinar con el responsable de los equipos informáticos de la Escuela de Posgrado para registrar las características de los equipos los domingos por la tarde.

CAPITULO III

MARCO TEÓRICO

2.1. ANTECEDENTES.

2.1.1. A nivel Internacional

- (Garcia Hanson & Salazar Escobar, 2005) en su tesis titulado "MÉTODOS DE ADMINISTRACIÓN Y EVALUACIÓN DE RIESGOS", tiene como objetivo describir los métodos de administración y evaluación de riesgos describiendo sus características, ventajas desventajas de su aplicación. Sus principales conclusiones son: primero. Dada la especificación de los métodos principales de administración y evaluación de riesgos y realizado el cruce comparativo de la forma como ellos se desarrollan, podemos entregar algunas conclusiones necesarias de tomar en consideración al momento de pensar en implementar en una entidad, un proceso de administración de riesgos. Segundo. se debe considerar las características de la entidad a la cual se desea aplicar el método de evaluación, con el fin de

seleccionar aquel método que más se adecue a sus necesidades y que ayude a lograr de manera más eficiente al resultado esperado. Tercero. Al respecto cabe destacar que no basta sólo con seleccionar aquel enfoque que más aportará al cumplimiento de los objetivos de la entidad, sino que también debe tomarse en consideración los recursos tanto materiales como de personal con los que cuenta la entidad para poder llevar a cabo el proceso completo de administración y evaluación de riesgos.

- (Gaona Vásquez, 2013) en su tesis titulado “APLICACIÓN DE LA METODOLOGIA NMAGERIT 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 CIUDAD DE MACHALA”, tiene como objetivo aplicar 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 ciudad de Machala. Su principal conclusión es que al aplicar la metodología Magerit se realizó en análisis y la gestión de riesgos obteniendo resultados realistas del estado de riesgo actual en la empresa.

- (Lucero G. & Valverde P., 2012)Lucero en la tesis denominada “Análisis y gestión de los sistemas de la Cooperativa de Ahorro y Crédito Jardín Azuayo, utilizando la metodología MAGERIT”, platea como objetivo el análisis de la situación actual y especificación de necesidades funcionales de seguridad para el diseño de los mecanismos de salvaguarda, centrado en el

departamento Informático de la Cooperativa de Ahorro y Crédito Jardín Azuayo, oficina de Coordinación y Cuenca. La investigación concluye que la prevención, detección y mitigación de los riesgos es imprescindible, razón por la que se deberá aplicar una metodología con su respectiva herramienta, usando perfiles de seguridad y salvaguardas adecuadas como lo recomienda la herramienta PILAR basic. Actualmente, en nuestro medio no se pone real énfasis en temas referentes al análisis y gestión de riesgos de los sistemas de información, lo que ocasiona que no se tenga un conocimiento adecuado de dichos temas y no se cuente con el personal especializado para realizar dicho análisis.

- (Perafán Ruiz & Caicedo Cuchimba, 2014) en la tesis denominada, “Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor del Cauca”, se planteó como objetivo realizar un 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 Institución Universitaria Colegio Mayor del Cauca; concluyendo que el análisis de riesgo aplicado, permite conocer de manera global el estado actual de la seguridad informática dentro de la Institución Universitaria Colegio Mayor del Cauca y los controles y políticas de seguridad de la información resultado

de este análisis de riesgos, pueden ser tomados como soporte para la implementación del SGSI.

- (Gallardo Piedra & Jácome Cordones , 2011)En la tesis denominada “Análisis de Riesgos Informáticos y Elaboración de un Plan de Contingencia T.I. para la Empresa Eléctrica Quito S.A.” se planteó como objetivo la identificación de los principales riesgos informáticos y en base a ellos elaborar un plan de contingencia T.I. para la Empresa Eléctrica Quito. Por ese motivo, el trabajo comienza analizando las principales metodologías que existen, para realizar en primer lugar, la identificación de los riesgos informáticos que puedan existir en la empresa. Posteriormente se realizó el análisis de las metodologías o guías existentes para elaborar el respectivo plan de contingencia, en donde se realizó una descripción y comparación de las mismas, para de esta manera, seleccionar la más idónea para realizar el trabajo.

  Una vez seleccionadas las metodologías se procedió a realizar el respectivo análisis de riesgos informáticos, principalmente dentro del departamento de TIC de la EEQ basándonos en la metodología escogida, que en este caso fue OCTAVE la que involucra desde el comienzo a los principales niveles organizacionales de la empresa como son los altos directivos, directivos de ares operativos y personal en general. Garantizado de este modo una participación activa y por ende un análisis de riesgo más objetivo y en base a las necesidades actuales de la

empresa. Tomando este precedente se consiguió recopilar el conocimiento y criterio de los participantes en lo referente a los activos que consideran más importantes dentro delas empresa, principales áreas de interés, requerimiento de seguridad, prácticas de estrategias de protección actual y vulnerabilidades que existen dentro de la misma, logrando de esta manera una selección acertada de los activos críticos, que para la empresas son fundamentales para su normal funcionamiento.

2.1.2. A nivel Nacional

- (Talavera Álvarez , 2015) en la tesis denominada “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”, tiene como objetivo Diseñar un sistema de gestión de seguridad de la información para una institución estatal de salud, de acuerdo a la norma ISO/IEC 27001:2013., porque en la actualidad, los problemas de la seguridad de la información se manifiestan en torno a la alineación de las Tecnologías de Información y Comunicación con los procesos de la organización, convirtiéndose en un aspecto muy crítico cuyo tratamiento es de vital consideración, es por ello que en el desarrollo del estudio, los tesista concluye que la no elaboración de documentos en los cuales se describen los procedimientos, políticas de seguridad a utilizar y controles que permitan garantizar la autenticidad, confidencialidad y

disponibilidad de los datos de los usuarios, puede en un futuro ser un peligro latente, ya que la El Instituto Nacional Materno Perinatal – INMP está creciendo de forma considerada.

2.2. BASES TEÓRICAS.

2.2.1. Análisis de riesgo:

(MAGERIT, 1997) Identificación de las amenazas que acechan a los distintos componentes pertenecientes o relacionados con el sistema de información (conocidos como 'activos'); para determinar la vulnerabilidad del sistema ante esas amenazas y para estimar el impacto o grado de perjuicio que una seguridad insuficiente puede tener para la organización, obteniendo cierto cono-cimiento del riesgo que se corre.

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.

Tipos de análisis de riesgos

Existen dos enfoques básicos para realizar un completo análisis de riesgos, uno cuantitativo y otro cualitativo.

Enfoque cualitativo:

El enfoque cualitativo de análisis de riesgos es de uso muy común en la actualidad, especialmente entre las nuevas empresas consultoras de seguridad, en aquéllas más especializadas en seguridad lógica, cortafuegos, test de intrusión y similares. Es mucho más sencillo e intuitivo que el cuantitativo, ya que no entran en juego probabilidades exactas sino, simplemente, una estimación de pérdidas potenciales.

El método o enfoque cualitativo es más apropiado para instalaciones menores y es el más utilizado en la actualidad. Se pueden medir ciertos parámetros:

- Riesgo de amenazas, empleando escalas como: elevado, medio, bajo.
- Gravedad del ataque, en base a escalas como 1, 2, 3.
- Daño, utilizando escalas como: vital, crítico, importante, conveniente, informativo.

Para éste análisis, no se requieren datos de probabilidad y sólo se utiliza la pérdida potencial estimada. En lugar de utilizar números exactos, utiliza métricas más difusas para los valores de los activos, la frecuencia de las amenazas y la efectividad del control. Utiliza un conjunto de elementos interrelacionados, como son:

- Amenazas
- Vulnerabilidades
- Controles. Existen cuatro tipos de controles:

Controles disuasorios. Reducen la probabilidad de un ataque deliberado.

Controles preventivos. Protegen las vulnerabilidades y hacen que un ataque no tenga éxito o bien, reducen su impacto.

Controles correctores. Reducen el efecto de un ataque.

Controles de investigación. Descubren los ataques y ponen en funcionamiento controles preventivos, también llamados proactivos o correctivos, así como reactivos.

Con estos cuatro elementos, podemos obtener un indicador cualitativo del nivel de riesgo, asociado a un activo determinado dentro de la organización, visto como la probabilidad de que una amenaza se materialice sobre un activo y produzca un determinado impacto.

Enfoque cuantitativo

El enfoque cuantitativo es, con diferencia, el menos utilizado, ya que en muchos casos, implica cálculos complejos o datos difíciles de estimar. Se basa en dos parámetros fundamentales, que son la probabilidad de que se produzca un suceso y una estimación del coste o de las pérdidas, en caso de que así sea. El producto de ambos términos es lo que se denomina coste anual estimado.

Tabla 1.- Ventajas e inconvenientes de los tipos de análisis de riesgos

	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.
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.	No es fiable para eventos raros o impactos impensables. 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.

2.2.2. Seguridad de información

La seguridad de la información, según (ISO 27001, 2013), consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su

tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

• **Confidencialidad:** la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

• **Integridad:** mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

• **Disponibilidad**: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Para garantizar que la seguridad de la información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI.

2.2.3. Metodología OCTAVE

(Caralli, Stevens, Young, & Wilson, 2007) El método OCTAVE fue la primera metodología coherente, a ser introducido. El enfoque se define mediante una guía de implementación de métodos (procedimientos, orientación, Hojas de trabajo, catálogos de información) y formación. El método se realiza en una serie de talleres Conducido y facilitado por un equipo interdisciplinario de análisis de las unidades de negocio En toda la organización (por

ejemplo, la alta dirección, los gerentes de área operacional y el personal) y Miembros del departamento de TI

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

Más específicamente, fue diseñado para organizaciones que

• Tienen una jerarquía de varias capas

• Mantener su propia infraestructura informática

• Tener la capacidad de ejecutar herramientas de evaluación de vulnerabilidad

• Tienen la capacidad de interpretar los resultados de las evaluaciones de vulnerabilidad

OCTAVE-S

El desarrollo de OCTAVES fue apoyado por la Inserción, Demostración y Programa de evaluación (TIDE) en el SEI, 4 con el objetivo de llevar un enfoque basado en octava hasta Pequeñas organizaciones manufactureras. La versión más actual del enfoque OCTAVE-S, está específicamente diseñado para organizaciones de 100 personas o menos.

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

Consta de tres fases similares. Sin embargo, OCTAVE-S es realizado por un equipo de análisis que tiene un amplio conocimiento del Organización. Así, OCTAVE-S no confía en talleres formales de e licitación de conocimiento para reunir Información, ya que se supone que el equipo de análisis (típicamente compuesto por tres a cinco) tiene un conocimiento

práctico de los activos importantes relacionados con la información, los requisitos de seguridad, Amenazas y prácticas de seguridad de la organización

OCTAVE Allegro

El enfoque de OCTAVE Allegro que se introduce en este informe técnico está diseñado para permitir Una evaluación amplia del entorno de riesgo operacional de una organización con el objetivo de Resultados más robustos sin la necesidad de un amplio conocimiento de la evaluación de riesgos. Este enfoque define los enfoques anteriores de OCTAVE, centrándose principalmente en los activos de Texto de cómo se usan, donde se almacenan, transportan y procesan, y cómo están Expuestos a amenazas, vulnerabilidades e interrupciones como resultado. Al igual que los métodos anteriores, OCTAVE Allegro se puede llevar a cabo en un entorno de colaboración, y se Realza Hojas de trabajo y cuestionarios, que se incluyen en los apéndices de este documento.

Sin embargo, OCTAVE Allegro también es adecuado para el uso por personas que desean realizar Evaluación de riesgos sin una participación organizativa extensa, experiencia o insumos.

Fase de la metodología OCTAVE allegro

1. Establecer criterios de medición del riesgo.

Se establecen los controladores de la organización que evalúan los efectos de un riesgo de la misión de una organización y los objetivos de negocio. Estos conductores se reflejan en un

conjunto de criterios de medición de riesgo que se crea y se registra como parte de este primer paso.

El método OCTAVE Allegro proporciona un conjunto estándar de plantillas de hoja de trabajo para crear estos criterios en varias áreas de impacto y establecer prioridades. Las áreas de impacto que se consideran son:

- Confidencialidad, Reputación/cliente
- Financiero
- Productividad
- Salud y seguridad
- Penalidades Legales
- Definición de áreas de impacto del usuario

Se debe priorizar las áreas de impacto de la más importante a la menos importante

2. Desarrollar un perfil de Activos de Información.

La metodología OCTAVE Allegro se centra en los activos de información de la organización para lo cual se realiza el proceso de creación de un perfil de esos activos. Un perfil es una representación de una información de los activos que describe sus características únicas, cualidades, características y valor. Para desarrollar el perfil se debe tener en cuenta las siguientes actividades:

- Identificar el grupo de activos de información al cual se le va a realizar el perfil
- Enfocarse en los activos de información más críticos

- Obtener información necesaria para empezar a estructurar el proceso de análisis de riesgos del activo

3. Identificar los contenedores de los activos de la información.

Los contenedores describen los lugares en los que la información es almacenada, transportada y procesada. Los activos de información residen no sólo en los contenedores dentro de los límites de una organización, sino también a menudo en envases que no están bajo el control directo de la organización. Los diferentes tipos de contenedores se describen a continuación:

- Contenedores técnicos: Están bajo el control directo de la organización o los que son administrados fuera de la organización.
- Contenedores físicos: La información pues estar de dentro o fuera de la empresa.
- Contenedor persona: Persona interna o externa de la organización que tiene el conocimiento detallado del activo.

4. Identificar las áreas de interés

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

5. Identificar las situaciones de amenaza

En la primera mitad de la etapa 5, las áreas de interés identificadas en el paso anterior se expanden en escenarios de amenaza. Una serie de escenarios de amenaza pueden ser representados visualmente en una estructura de árbol comúnmente conocido como un árbol de amenaza.

6. Identificar los riesgos

En el anterior paso se identificaron las amenazas, y en este se identificarán las consecuencias en una organización. Una amenaza puede tener múltiples impactos potenciales sobre una organización. Por ejemplo, la interrupción de sistema de comercio electrónico de una organización puede afectar la reputación de la organización con sus clientes, así como su posición financiera.

7. Analizar los riesgos

Se calcula una medida cuantitativa en que la organización se ve afectada por una amenaza.

Esto se realiza teniendo en cuenta el escenario de amenaza y su consecuencia. Luego se determinar un valor de impacto (bajo, medio, moderado) para cada área de impacto. Por último se computa los valores de impacto de cada área para analizar el riesgo y así ayudar a la organización a determinar la mejor estrategia para manejar ese riesgo.

8. Seleccione enfoque de mitigación.

La organización determina cuál de los riesgos que han identificado requieren mitigación desarrollando una estrategia para esto.

La organización debe ordenar cada uno de los riesgos que ha identificado por su calificación ayudándole de manera ordenada a tomar decisiones sobre su estado de mitigación. A continuación se debe asignar un enfoque de mitigación para cada uno de esos riesgos y por último desarrollar la estrategia de mitigación que se decida para mitigar el riesgo.

Las hojas de trabajo han sido diseñadas para que puedan ser traducibles fácilmente a otros formatos electrónicos.

2.2.4. Metodología MAGERIT

(Consejo Superior de Administración Electrónica, 2012) De España, ha elaborado y promueve MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas) como respuesta a la percepción de que la administración (y en general toda la sociedad) depende de forma creciente de las tecnologías de la información para la consecución de sus objetivos de servicio.

La razón de ser de MAGERIT está pues directamente relacionada con la generalización del uso de los medios electrónicos, informáticos y telemáticos, que supone unos beneficios evidentes

para los ciudadanos; pero que también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que garanticen la autenticación, confidencialidad, integridad y disponibilidad de los sistemas de información y generan confianza cuando se utilicen tales medios. Una organización no alcanzará sus objetivos, metas y misión si no tiene a su alcance los elementos informáticos básicos e indispensables que le ayuden y soporten sus decisiones.

Conceptualización

MAGERIT es un método formal para investigar los riesgos que soportan los Sistemas de Información y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos.

MAGERIT permite:

- Estudiar los riesgos que soporta un sistema de información y el entorno asociado a él. MAGERIT propone la realización de un análisis de los riesgos que implica la evaluación del impacto que una violación de la seguridad tiene en la organización; señala los riesgos existentes, identificando las amenazas que acechan al sistema de información, y determina la vulnerabilidad del sistema de prevención de dichas amenazas, obteniendo unos resultados.
- Los resultados del análisis de riesgos permiten a la gestión de riesgos recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los

riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios.

Activos

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)

FASES DE MAGERIT VERSIÓN 3

- **Identificación de activos informáticos**

Se identifica los activos informáticos existentes en la organización

- **Catálogos de amenazas**

En este punto las amenazas ya vienen denotadas y estas amenazas están agrupados según el origen industrial, errores y fallos no intencionados y ataques intencionados.

- **Caracterización**

En la caracterización denotamos las amenazas que se pueden ser afectados a cada activo informático; así mismo obtenemos las probabilidades que pueden dañar estas amenazas a estos activos informáticos. Las dimensiones son valoradas por cada amenaza que contiene dichos activos.

- **Impacto**

Pasa saber el impacto por cada dimensión y por cada activo informático se realiza una operación que es obtenida de los valores de dimensiones que esto fue realizado en la identificación de activos con los valores de dimensiones que se obtuvo en la tabla de caracterización.

- **Mapa de riesgos**

Relación de las amenazas a que están expuesto los activos.

- **Salvaguardas**

En esta tarea las salvaguardas están agrupados tipos de protección

2.2.5. Diseño factorial

(kuehl, 2001) Es un tipo de Diseño Experimental, en donde cada variable independiente recibe el nombre de factor, y el numero indica los niveles de cada variables, también se definen como aquellos experimentos en los que se estudian simultáneamente dos o más factores y donde los tratamientos se forman por la combinación de los diferentes niveles de cada uno de los factores.

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** de un factor son comparaciones entre los niveles de un factor promediados para todos los niveles de otro factor.

MODELO ESTADISTICO PARA DOS FACTORES

(Porras, 2000)

MODELO DE MEDIAS DE LAS CELDAS

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

$$y_{ijk} = \mu_{ij} + e_{jk}$$
$$i=1,2,\ldots,a \quad j=1,2,\ldots,b \quad k=1,2,\ldots,r$$

Donde:
μ_{ij} = media de la combinación de los tratamientos A,B
e_{jk} =**errores experimentales aleatorios con media 0 y varianza** σ^2

ESTIMACIONES DE LAS MEDIAS DE CELDAS CON EL METODO DE MINIMOS CUADRADOS

La suma de cuadrados para el **error experimental** es

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

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

$$\widehat{\mu_{ij}} = \frac{y_{ij}}{r} = \bar{y}_{ij}$$
$$1 = 1,2,\ldots,a \quad j = 1,2,\ldots,b$$

2.3. 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 III

MATERIAL Y MÉTODOS

3.1. METODOLOGÍA UTILIZADA EN EL PROCESO DE INVESTIGACIÓN CIENTÍFICA.

se pretende alcanzar los objetivos de la investigación empleando el **método inductivo** que trabaja con el concepto de que a partir de la observación de hechos particulares obtenemos proposiciones generales es decir es aquel que establece un principio general una vez realizada el estudio y análisis de hechos y fenómenos en particular.

3.2. 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.

3.3. DISEÑO DE LA INVESTIGACIÓN.

El diseño de la investigación es experimental porque tiene como objetivo averiguar si unos determinados factores influyen en una

variable de interés y, si existe influencia de algún factor, cuantificar dicha influencia.

3.4. 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

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

Modelo estadístico

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

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

3.5. 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)

3.6. Técnicas de recojo, procesamiento y presentación de datos.

3.6.1. Técnicas para la recolección de datos

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

	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

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.

3.6.2. Técnicas para los Procesamientos de Datos;

Se utilizaron:

- **La Revisión y Consistencia de la Información**: Este paso consistió básicamente en depurar la información revisando los datos contenidos en los instrumentos de trabajo de campo, con el propósito de ajustar los llamados datos primarios (juicio de expertos).

- **Elaboración de plantillas en Excel 2013-activos:** Se elaboró una plantilla en Excel de acuerdo a los parámetros de la Metodología MARGERIT y OCTAVE, con la finalidad de poder ingresar, procesar y analizar los datos relacionados a los activos trabajando en base a las metodologías mencionadas.

- **Elaboración de plantillas en Excel 2013-diseño factorial:** Se elaboró una plantilla en Excel de acuerdo al diseño factorial con interacción, con la finalidad de poder procesar y analizar los datos obtenidos en base a la aplicación de la Metodología MARGERIT y OCTAVE en la Escuela de Pos Grado.

3.6.3. Presentación de datos.

Análisis descriptivo:

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

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.

CAPITULO IV

EXPERIMENTACIÓN

4.1. 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:

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

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

$\boldsymbol{Donde}$:

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

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

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

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

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

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

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

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:

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

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:

$$\widehat{\boldsymbol{\mu}} = \overline{\boldsymbol{y}}\ \ldots, \qquad \widehat{\boldsymbol{\alpha}_i} = \overline{\boldsymbol{y}}_{\boldsymbol{i}}\ldots - \overline{\boldsymbol{y}}\ \ldots, \qquad \widehat{\boldsymbol{\beta_j}} = \overline{\boldsymbol{y}}_{\boldsymbol{.j.}} - \overline{\boldsymbol{y}}\ \ldots$$

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

   $\boldsymbol{Donde}$:

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

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

Operando:

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

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

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

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

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

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

Operando:

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

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

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

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

Operando:

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

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

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

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

Operando:

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

Obteniendo el siguiente cuadro:

$\bar{y}_{ij.}$	VULNERABILIDAD		IMPACTO		MEDIAS MARGINALES (A) $\bar{y}_{i\cdot\cdot}$
MAGERIT	4 3	3,5	3 2	2,5	3
OCTAVE	3 5	4	5 4	4,5	4,3
MEDIAS MARGINALES (B) $\bar{y}_{\cdot j.}$	3,8		3,5		$\bar{y}\ \ldots =$ **7,3**

Tabla 1: tabla de medias de celdas y medias marginales

Se calculan los parámetros del modelo utilizando:

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

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

Operando

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

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

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

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

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

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

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

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

Obteniendo el siguiente cuadro:

$\widehat{\alpha\beta}_{ij}$	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	

Tabla 2: Parámetros del modelo

Se calculan las predicciones a partir de:

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

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:

$\hat{y}_{ij}$	VULNERABILIDAD	IMPACTO
MAGERIT	3.5	2.5
OCTAVE	4.0	4.5

Tabla 3: predicciones =medias casillas

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:

	DIMENSIONES (B)	
METODOLOGIAS (A)	VULNERABILIDAD	IMPACTO
MAGERIT	0.5	0.5
	-0.5	-0.5
OCTAVE	-1.0	0.5
	1.0	-0.5

Tabla 2: Residuos

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:

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

2. Descomposición de la variabilidad

La ecuación básica del análisis de la varianza es:

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

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

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

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

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

		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	0.8750		
scT	TOTAL	7	7.8750	1.1250		

Tabla 3: ANOVA

Coeficientes de Determinación que se obtienen son:

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

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

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

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

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

4.2. 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.

	METODOLOGIAS (B)			M (Yi)			
ACTIVOS (A)	MAGERIT	OCTAVE	A (Yj)	M	O	M*M	O*O
Equipo de Cómputo	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 Iteractiva	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	

MODELO ESTADISTICO

$$Y_{ijk} = \mu + \tau_i + \varepsilon_{ij}$$

$$i = 1, 2, \ldots, a \quad j = 1, 2, \ldots, b$$

DEFINICION DE VARIABLES DE ESTUDIOS Y DE LA HIPOTESIS A PROBAR

VARIABLE DE ESTUDIO: analisis de riesgo

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

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

El significado verbal de la hipotesis es:

H_0:	*La metodologia no influye en el analisis de riesgo o no existe diferencia significativa en el analisis de riesgo entre las metodologias de MAGERIT Y OCTAVE*	H_1:	*La metodologia influye en el analisis de riesgo o hay diferencia significativa en el analisis de riesgo entre las metodologias de MAGERIT Y OCTAVE*

DATOS

Tratamientos (Metodologias)	**a =>**	2
Numero de observaciones por Metodologia	**n=>**	22
Numero total de observaciones por Metodologia	**N =>**	44

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

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**

$$y_{2.} = \sum_{i=1}^{23} y_{ij} = \quad \textbf{394}$$

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**

$$SS_{tr} = \frac{\sum_{i=1}^{2} y_{i.}^2}{n} - \frac{y_{..}^2}{N}$$ **338,2727**

MEDIAS DE CUADRADAS

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

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

ESTADISTICA

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

TABLA ANOVA

FUENTE DE VARIACION	SUMA DE CUADRADOS	G.L	CUADRADOS MEDIOS	F	P	VALOR CRITICO PARA F
METODOLOGIAS	338,27	1	338,2727273	6,927394	0,1018	4,0762
ERROR	2050,91	42	48,83116883			
TOTAL	2389,18	43				

Utilizando un nivel de significancia del 5% ($\alpha = 0.05$), para encontrar el $F_{\alpha;0,05:3;16)}$ (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:

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

0,1018 > 0,05

Por tanto, se acepta la hipótesis nula H_0

CAPITULO V

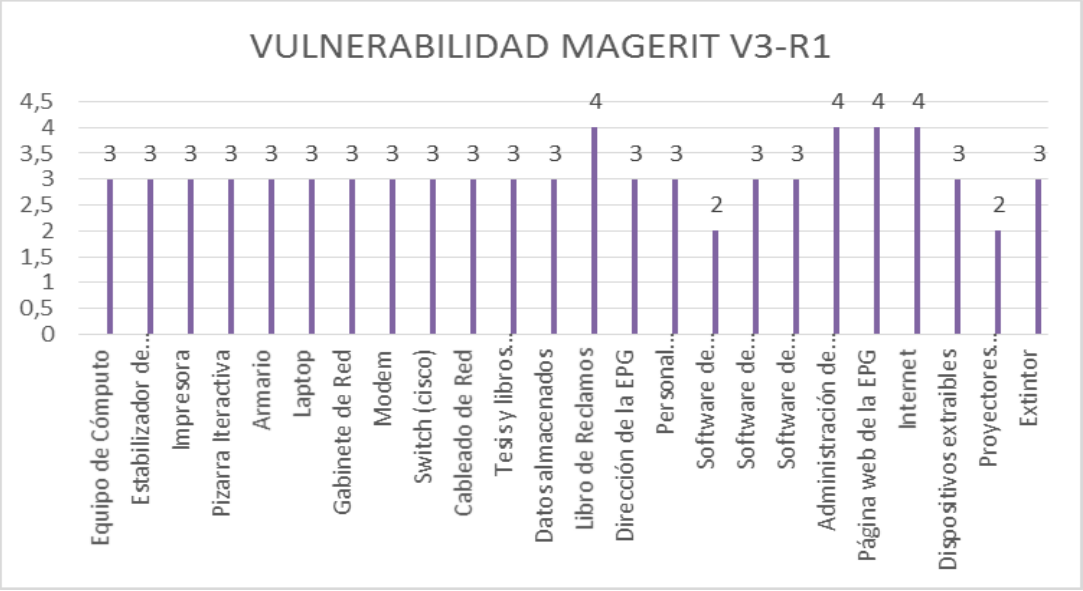
RESULTADOS

5.1. Resultado de trabajo de campo con aplicación estadística y mediante distribución de frecuencia y gráficos.

GRAFICOS DE RESULTADO DE VULNERABILIDAD E IMPACTO DE MAGERIT Y ACTAVE

Resultados de Vulnerabilidad e Impacto de la primera replica (R1), MAGERTI V3 Y OCTAVE Allegro

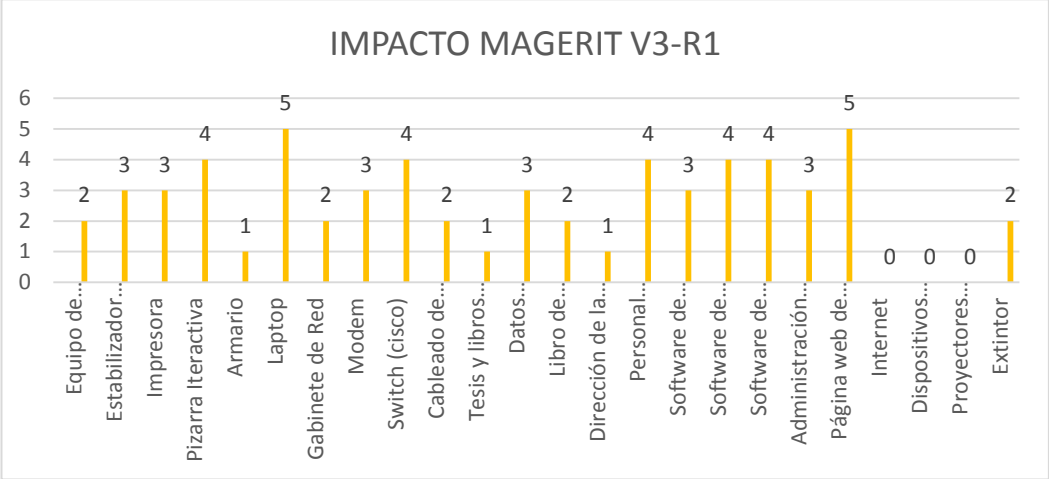
Grafico 1 Vulnerabilidades MAGERIT V3-R1



Fuente: Elaboración propia.

En el grafico 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.

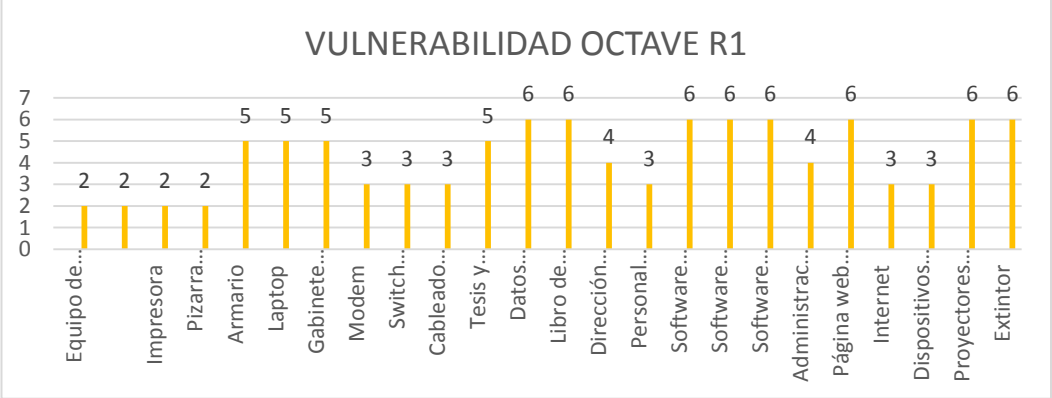
Grafico 2 Impacto MAGERIT V3-R1



Fuente: Elaboración propia.

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

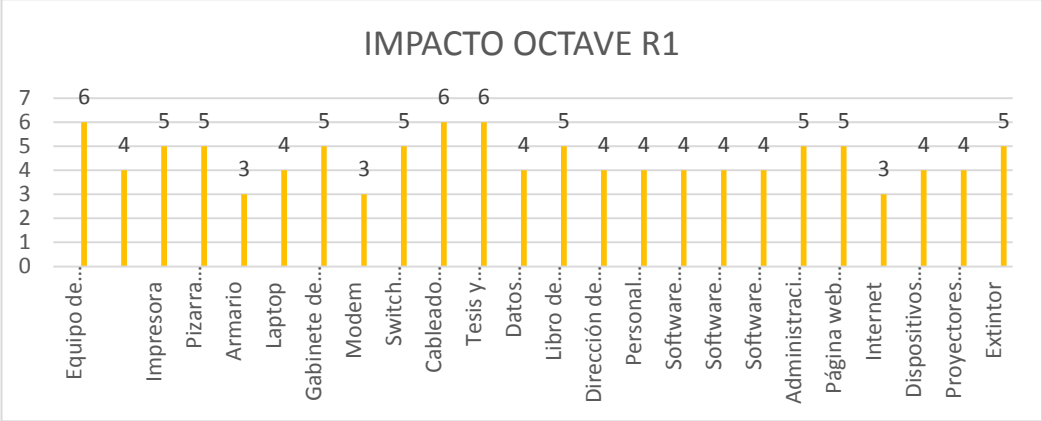
Grafico 3. Vulnerabilidades OCTAVE-R1



Fuente: Elaboración propia.

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

Grafico 4 Impacto OCTAVE -R1

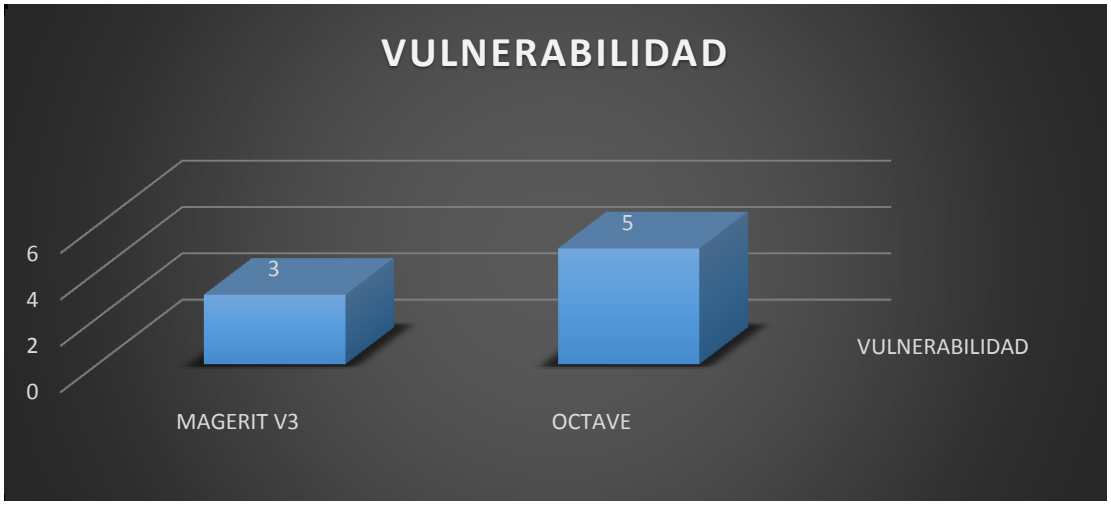


Fuente: Elaboración propia.

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

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

Grafico 5. Vulnerabilidades MAGERIT-OCTAVE.



Fuente: Elaboración propia.

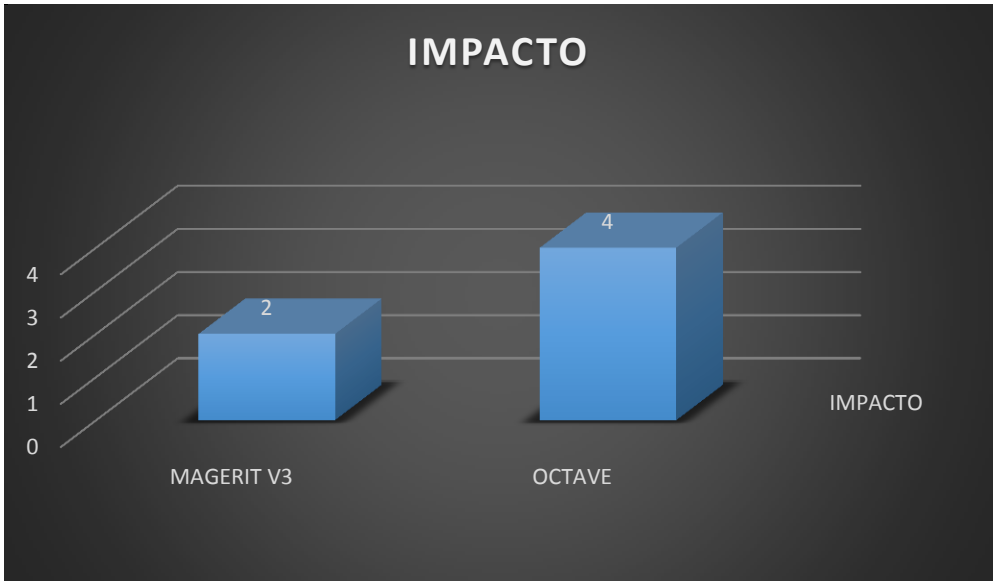
En el grafico 5 observamos el resultado de la valoración general de los activo con respecto a la vulnerabilidad de la primera replica (R1) mediante las metodologías MAGERIT V3 y OCTAVE.

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".

Resultados general del Impacto de la primera replica (R1), MAGERTI V3 Y OCTAVE.

Grafico 6.Impacto MAGERIT- OCTAVE.



Fuente : Elaboración propia.

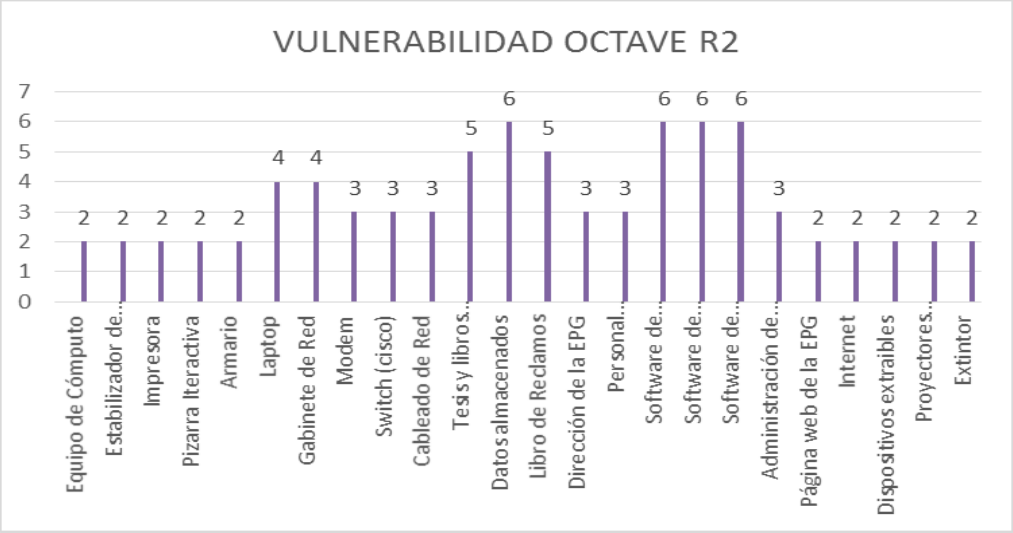
En el grafico 6 observamos el resultado de la valoración general de los activo con respecto al impacto de la primera replica (R1) mediante las metodologías MAGERIT V3 y OCTAVE.

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".

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

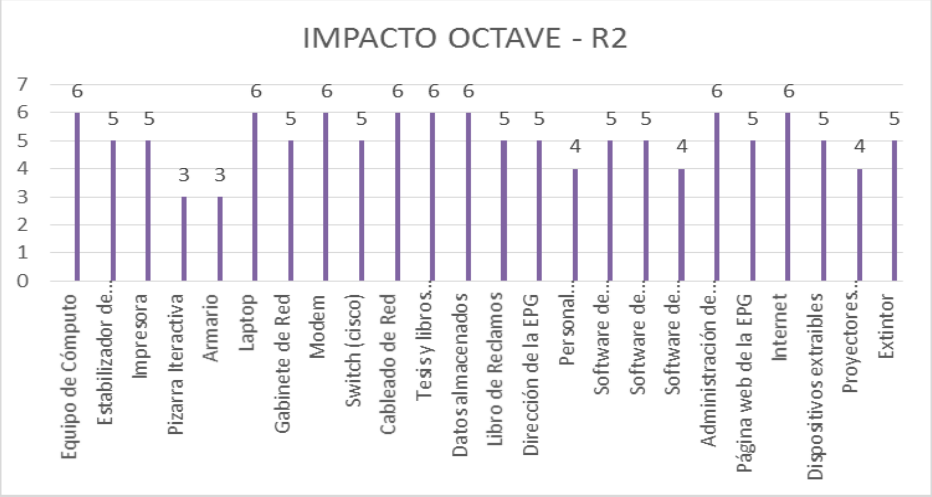
Grafico 7. Vulnerabilidades OCTAVE -R2



Fuente: Elaboración propia.

En el grafico 7 observamos el resultado de la valoración de cada activo con respecto a las vulnerabilidades de la segunda replica (R2) mediante la metodología OCTAVE.

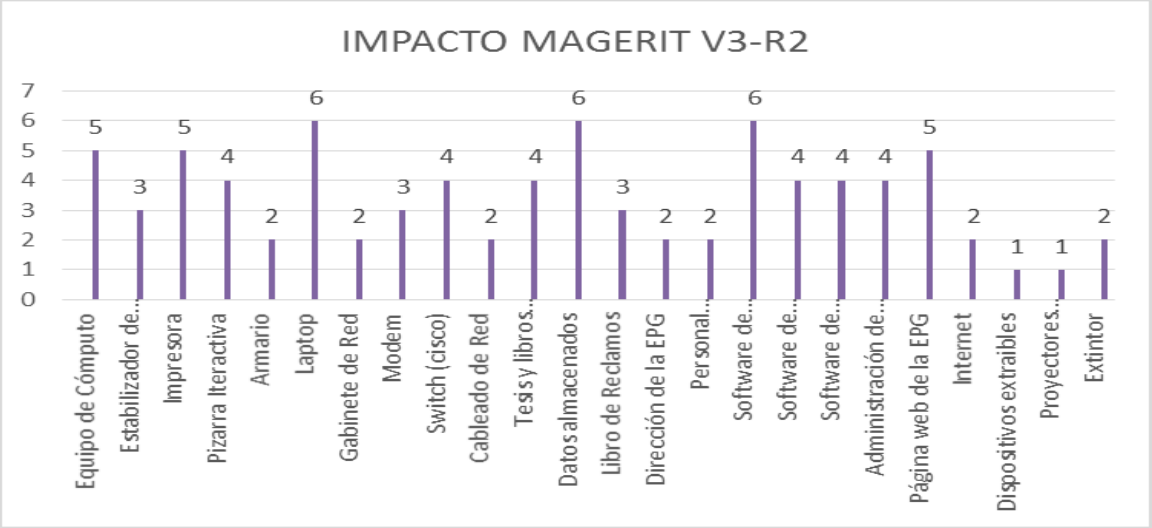
Grafico 8. Impacto OCTAVE -R2



Fuente: Elaboración propia.

En el grafico 8 observamos el resultado de la valoración de cada activo con respecto al Impacto de la segunda replica (R2) mediante la metodología OCTAVE.

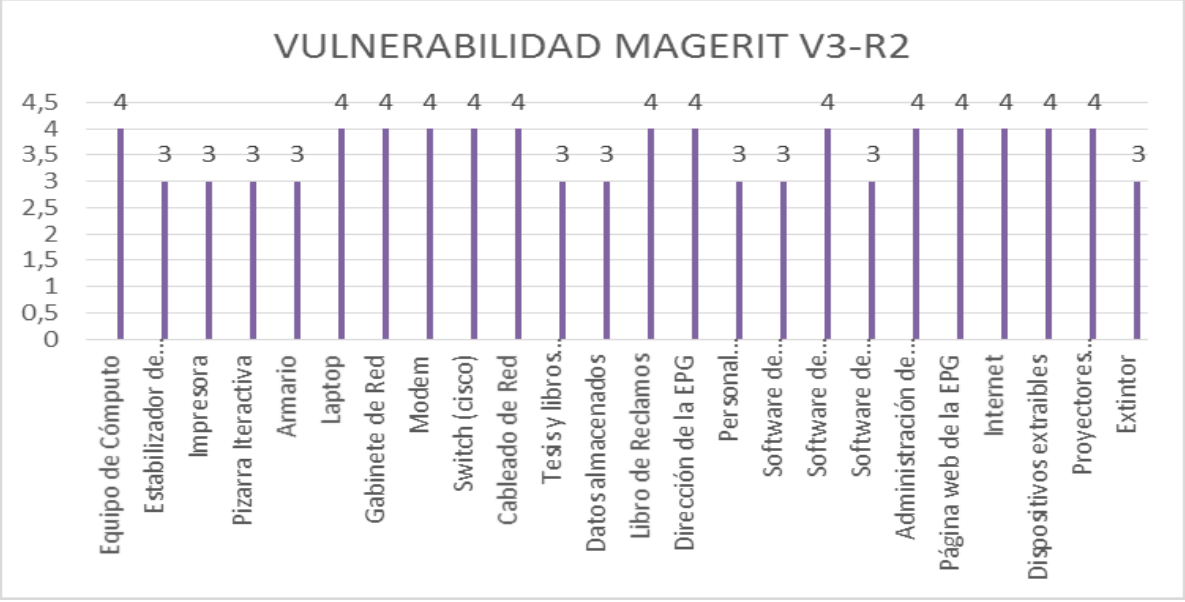
Grafico 9. Impacto MAGERIT V3 –R2



Fuente: Elaboración propia.

En el grafico 9 observamos el resultado de la valoración de cada activo con respecto al Impacto de la segunda replica (R2) mediante la metodología MAGERIT V3.

Grafico 10. Vulnerabilidades MAGERIT-R2

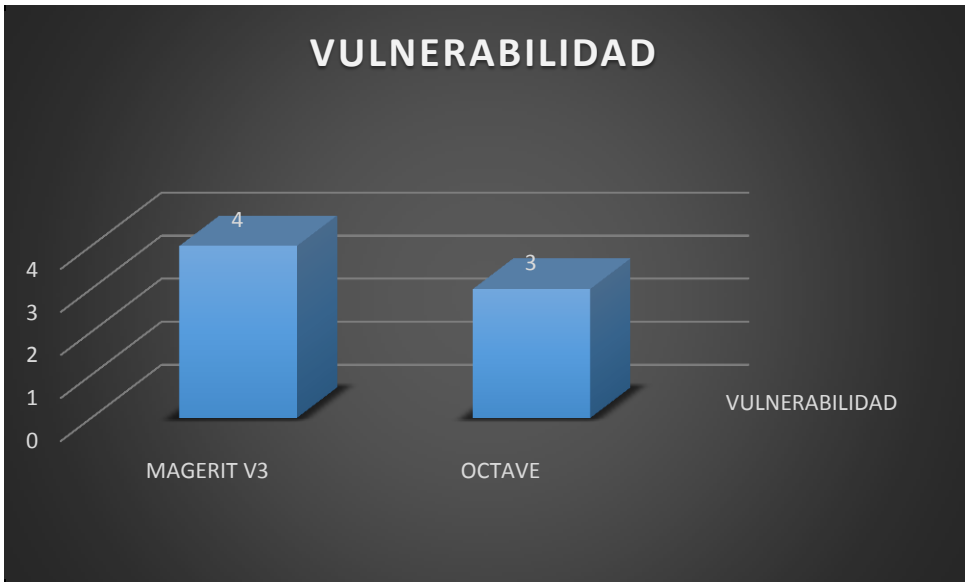


Fuente: Elaboración propia.

En el grafico 10 observamos el resultado de la valoración de cada activo con respecto a las vulnerabilidades de la segunda replica (R1) mediante la metodología OCTAVE.

Resultados general de la vulnerabilidad de la segunda replica (R2), MAGERTI V3 Y OCTAVE.

Grafico 11. Vulnerabilidades MAGERIT OCTAVE



Fuente: Elaboración propia.

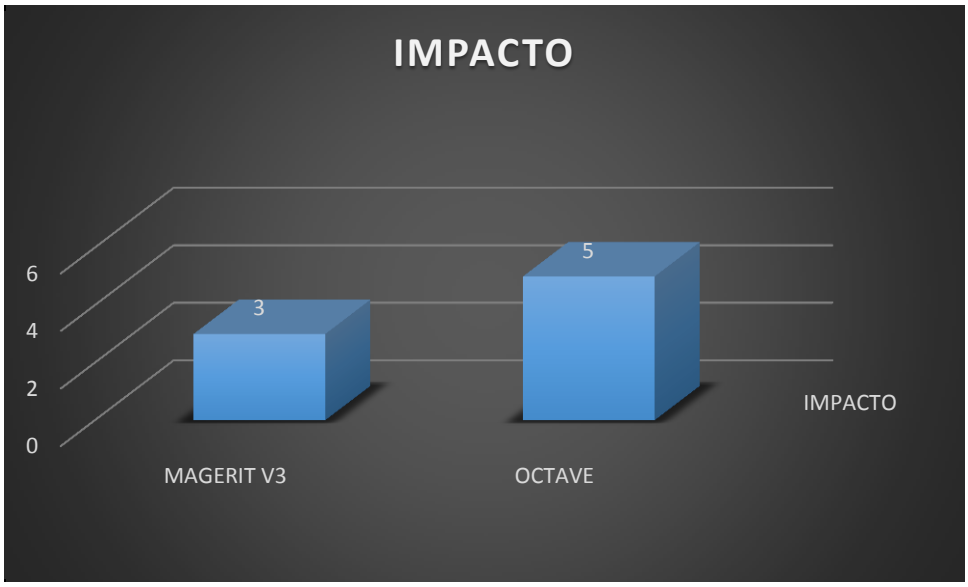
En el grafico 11 observamos el resultado de la valoración general de los activo con respecto a la vulnerabilidad de la segunda replica (R2) mediante las metodologías MAGERIT V3 y OCTAVE.

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"

Resultados general del Impacto de la segunda replica (R1), MAGERTI V3 Y OCTAVE.

Grafico 12. Impacto MAGERIT V3- OCTAVE



Fuente: Elaboración propia.

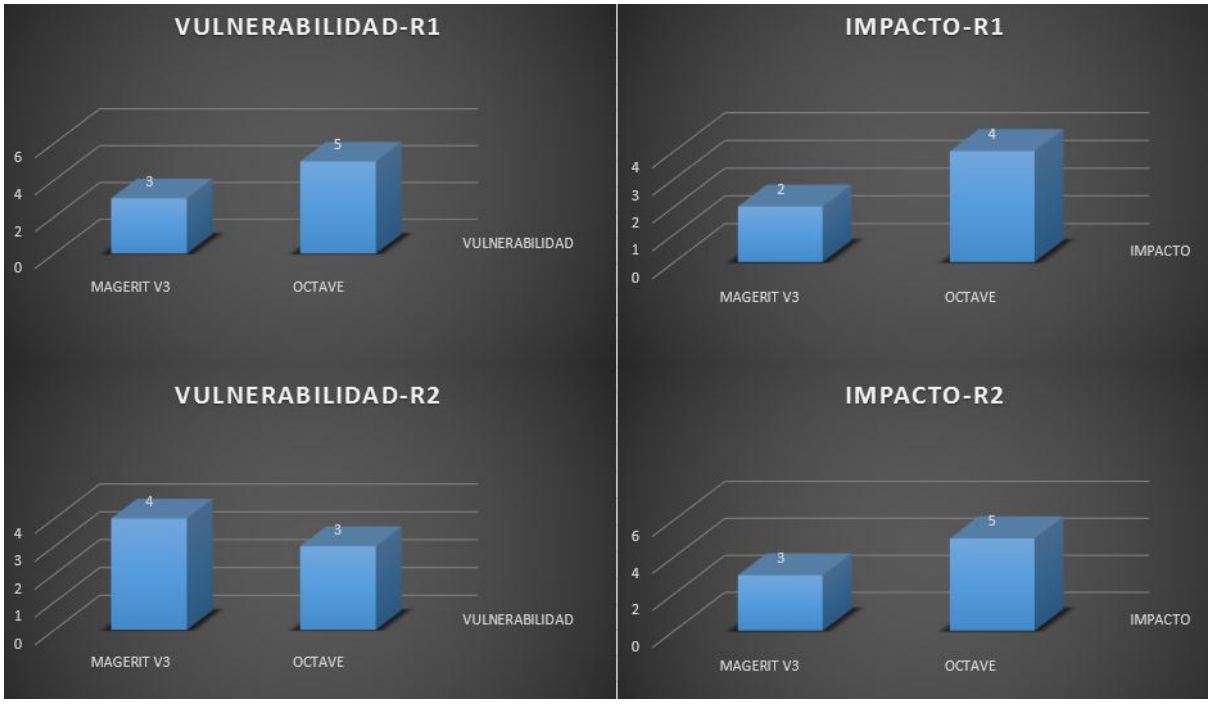
En el grafico 1 2 observamos el resultado de la valoración general de los activo con respecto al impacto de la segunda replica (R2) mediante las metodologías MAGERIT V3 y OCTAVE.

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".

Resultados final de vulnerabilidades e impacto de la primera y segunda replica, MAGERIT V3 Y OCTAVE.

Grafico 13. Resultado final de vulnerabilidad e impacto MAGERIT-OCTAVE

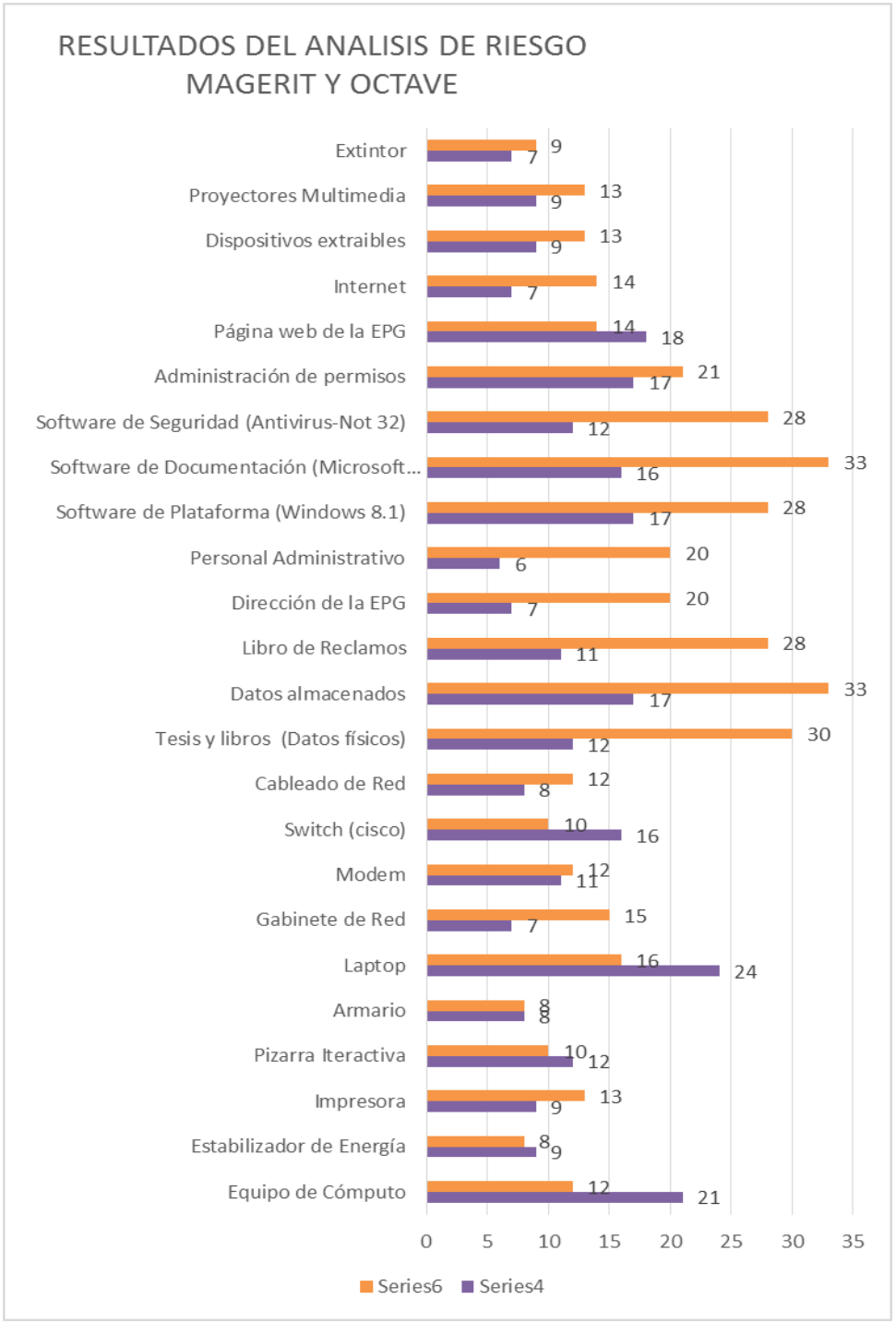


Fuente: Elaboración propia.

Mediante estos resultados del grafico 13 obtenidos de la aplicación de las metodologías MAGERIT V3 Y OCTAVE en Escuela de Pos Grado – UNHEVAL 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.

GRAFICOS DE RESULTADO DE ANALISIS DE RIESGO DE MAGERIT Y ACTAVE

Grafico 14 Resultado de análisis de riesgo MAGERIT y OCTAVE



MAGERIT COLOR LILA

OCTAVE COLOR NARANJA

En el grafico 14 observamos el resultado final del anales 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 del grafico 14 obtenidos de la aplicación de las metodologías MAGERIT V3 Y OCTAVE en Escuela de Pos Grado–UNHEVAL 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.

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

A. 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	0,8750		
scT	TOTAL	7	7,8750	1,1250		

- 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:

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

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.

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

- En la tercera hipótesis nula del diseño:

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

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.

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

5.1.1. Diseño Unifactorial

FUENTE DE VARIACION	SUMA DE CUADRADOS	G.L	CUADRADOS MEDIOS	F	P	VALOR CRITICO PARA F
METODOLOGIAS	338,27	1	338,2727273	6,927394	0,1018	4,0762
ERROR	2050,91	42	48,83116883			
TOTAL	2389,18	43				

- En la hipótesis nula del diseño:

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

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.

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

5.2. CONTRASTACIÓN DE LAS HIPÓTESIS.

Contrastes que se deducen la tabla ANOVA son los siguientes:

5.2.1. Diseño factorial de 2 x 2

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

$$H_0{}^{(1)}\text{: "El factor metodología no influye"}$$
$$A_i = 0;\ \mathrm{i} = 1{,}2$$

$$\hat{F}_A : \frac{\widehat{S^2}_A}{\widehat{S^2}_E} = \frac{3.1250}{0.8750} = 3.57 \sim F_{1,4} => p - valor = 0.132$$
$$F_{(\alpha,\, a-1,\, N-a)} = F_{(0.05,\, 0\,,7)} = 0{,}132$$
$$0.132 < 3.57$$

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

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

$$H_0{}^{(2)}\text{: "El factor dimensiones no influye"}$$
$$B_i = 0;\ \ \mathrm{j} = 1{,}2$$

$$\hat{F}_A : \frac{\widehat{S^2}_B}{\widehat{S^2}_E} = \frac{0.1250}{0.8750} = 0.14 \sim F_{1,4} => p - valor = 0.725$$
$$F_{(\alpha,\, b-1,\, N-a)} = F_{(0.05,\, 0\,,7)} = 0{,}725$$
$$0.725 > 0.14$$

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.***

$$H_0{}^{(3)}\text{: "La interacción de los dos factores no influye"}$$
$$(AB)_{ij} = 0;\ \mathrm{i,j} = 1{,}2$$

$$\hat{F}_A : \frac{\widehat{S^2}_{AB}}{\widehat{S^2}_E} = \frac{1.1250}{0.8750} = 0.14 \sim F_{1,4} => p - valor = 0.320$$
$$F_{(\alpha,\, ab-1,\, N-a)} = 0.320$$
$$0.320 < 4.0726$$

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%

5.2.2. Diseño Unifactorial

- considerando las siguientes hipótesis nula y alterna, respectivamente.

H_0: μ_1

H_1: μ_1

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:

$$F_{(0)}$$

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

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

	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		
COMUNICACIONE	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	PERSONA	[ddf]	Director de la Escuela de Posgrado	-	-	-		2	2	2	
	PSP2		[sec]	Personal Administrativo	-	-	-	3	1			

CAPITULO VI

DISCUSIÓN DE RESULTADOS

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:

  $\boldsymbol{H_c{}^{(1)}: El\ factor\ metodologías\ no\ influye\ significativamente\ en\ el\ análisis\ de\ riesgos.}$
  $\boldsymbol{H_c{}^{(2)}: El\ factor\ dimensiones\ influye\ significativamente\ en\ el\ análisis\ de\ riesgos.}$
  $\boldsymbol{H_c{}^{(3)}: la\ interaccion\ de\ los\ factores\ no\ influyen\ significativamente\ en\ el\ análisis\ de\ riesgos.}$

- **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 las 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

6.1. 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 confidencilidad.

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.

CONCLUSIONES

Después de haber analizado y desarrollado la investigación sobre el análisis de riesgo, determinamos lo siguiente:

- La metodología MAGERIT y OCTAVE identifican de forma similar las amenazas en el análisis de riesgo de los sistemas de información en la Escuela de Pos Grado de la Universidad Nacional Hermilio Valdizan, Huánuco.
- La metodología MAGERIT identifican de forma similar las vulnerabilidades en el análisis de riesgo de los sistemas de información en la Escuela de Pos Grado de la Universidad Nacional Hermilio Valdizan, Huánuco.
- La metodología OCTAVE identifican y tipifican de forma similar los impactos en el análisis de riesgo de los sistemas de información en la Escuela de Pos Grado de la Universidad Nacional Hermilio Valdizan, Huánuco.

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:

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 INFORMACION PARA UNA ENTIDAD ESTATAL DE SAUD DE ACUERDO A LA ISO/IEC 27001:2013. *Tesis*.

Caralli, R., Stevens, J., Young, L., & Wilson, W. (2007). IIntroducción 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.

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

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

ANEXOS

ANEXO 01 DISEÑO DE EXPERIMENTACIÓN

1. TABLA DE MEDIAS DE CELDAS Y MEDIAS MARGINALES

$\bar{y}_{ij\cdot}$	VULNERABILIDAD		IMPACTO		MEDIAS MARGINALES (A) $\bar{y}_{i\cdot\cdot}$
MAGERIT	4 3	3,5	3 2	2,5	3
OCTAVE	3 5	4	5 4	4,5	4,3
MEDIAS MARGINALES (B) $\bar{y}_{\cdot j\cdot}$	3,8		3,5		$\bar{y}_{\cdot\cdot\cdot} =$ **7,3**

ANEXO 02 RECOLECCIÓN DE DATOS

OCTAVE

Muy bajo	1
Bajo	2
Medio bajo	3
medio	4
Medio alto	5
Alto	6
Muy alto	7

Muy bajo	1
Bajo	2
Medio	3
Alto	4
Muy alto	5
Crítico	6

MAGERIT

	Probabilidad
Raro	1
Improbable	2
Posible	3
Probable	4
Casi seguro	5

	DIMENCIONES
D	Disponibilidad
I	Integridad de los datos
C	Confidencialidad de la información
A	Autenticidad
T	Trazabilidad

ANÁLISIS DEL RIESGO.

RIESGO = CONSECUENCIA X LA POSIBILIDAD

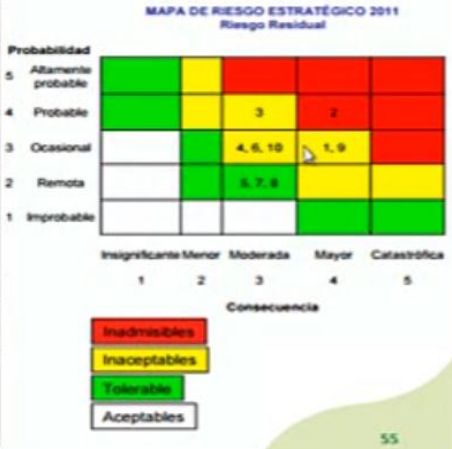
PROBABILIDAD		CONSECUENCIA				
		Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Casi certeza	Entre 81%-100% Valor : 5	A(5)	A(10)	E (15) Riesgo 10	E (20) Riesgo 7	E(25) Riego 9
Probable	Entre 61%-80% Valor : 4	M(4)	A(8)	A(12)	E(16) Riesgos 1, 2 y 12	E(20)
Posible	Entre 41%-60% Valor : 3	B(3)	M(6)	A(9) Riesgo 11	E(12) Riesgos 3, 4,5 y 6	E(15) Riesgo 8
Improbable	Entre 21%-40% Valor : 2	B(2)	B(4)	M(6)	A(8)	E(10)

MARIA DEL PILAR MURCIA C.
Especialista en Administración y Gerencia de S.G.C.

chec | Grupo epm

Mapa de riesgos estratégico 2011

No.	RIESGOS	OBJETIVO ESTRATEGICO ASOCIADO
1	Demoras en una recuperación oportuna de la operación, debido a una interrupción por falta de un plan de continuidad de negocio.	Incrementar el valor para los grupos de interés
2	Incrementos no previstos en los costos de operación del negocio.	Lograr excelencia operacional en los procesos.
3	Generar impactos negativos al medio ambiente y con ello a los diferentes grupos de interés.	Actuar con responsabilidad económica, social y ambiental en las zonas de influencia CHEC.
4	Decisiones y actuaciones de la Empresa que causan daños a su reputación.	Fortalecer las relaciones y las comunicaciones con los grupos de interés externos Fortalecer las relaciones y la comunicación efectiva de los grupos de interés internos.
5	Continuos cambios en los modelos de gestión y operación impactando negativamente la organización	Desarrollar las capacidades organizacionales.
6	Desalineación del modelo para el Gerenciamiento del Talento Humano con respecto al propósito y las estrategias.	Desarrollar las capacidades del talento humano. Fortalecer las relaciones y las comunicación efectiva con los grupos de interés internos.
7	Integración y alineación no efectiva de los diferentes sistemas de información y comunicación de la Empresa	Garantizar la disponibilidad, confiabilidad e integridad de la información para la toma de decisiones.
8	Desarrollar una estrategia comercial inadecuada en los negocios	Consolidar los negocios en el mercado nacional
9	Riesgo de gobierno	Incrementar el valor para los grupos de interés
10	Vulneración de los Derechos Humanos	Desarrollar las capacidades del talento humano /Fortalecer las relaciones y la comunicación efectiva de los grupos de interés internos. / Fortalecer las relaciones y las comunicaciones con los grupos de interés externos.



Unidad de Riesgo Procesos
Metodología aplicada

IDENTIFICACIÓN DE ESCENARIOS DE AMENAZA Y CRITERIO DE MEDICIÓN							
ACTIVO	TIPO	ARBOL DE AMENAZA	MOTIVO	CONSECUENCIA	SALVAGUARDA	POSIBILIDAD DE OCURRENCIA DE UNA AMENAZA	
						CRITERIO DE MEDICIÓN	VALOR
Equipo de Cómputo	FÍSICO	AHUMT (HURTO)	Interés por los equipos de computo.	Gravedad máxima si accede a datos privados de la organización (LPDP).	Limitación de acceso a las instalaciones de la organización.	Bajo	2
		AHUAF (ATAQUE FÍSICO)	Intención de perjudicar o retrasar las actividades planificadas.	Puede invalidar los trabajos planificados.		Bajo	2
		PT (AVERÍA)	Mal uso o infortunio.	El daño causado será asumible por el sistema.	Mantenimiento.	Medio	4
Estabilizador de Energía	FÍSICO	AHUMT (HURTO)	Interés por los equipos o dispositivo.	Gravedad máxima.	Limitación de acceso a las instalaciones de la organización.	Medio bajo	3
		AHUAF (ATAQUE FÍSICO)	Intención de perjudicar o retrasar las actividades planificadas.			Bajo	2
		PT (AVERÍA)	Mal uso o infortunio.	El daño causado será asumible por el sistema.	Mantenimiento.	Medio bajo	3
Impresora	FÍSICO	AHUMT (HURTO)	Interés por las impresoras.	Gravedad máxima.	Limitación de acceso a las instalaciones de la organización.	Medio bajo	3
		AHUAF (ATAQUE FÍSICO)	Intención de perjudicar o retrasar las actividades planificadas.			Bajo	2
		PT (AVERÍA)	Mal uso o infortunio.	El daño causado será asumible por el sistema.	Mantenimiento.	Medio	4
Proyector multimedia	FÍSICO	AHUMT (HURTO)	Interés por los proyetores multimedia.	Gravedad máxima	Limitación de acceso a las instalaciones de la organización.	Medio bajo	3
		AHUAF (ATAQUE FÍSICO)	Intención de perjudicar o retrasar las actividades planificadas.	Incremento en el tiempo de espera e incremento de gastos.		Medio bajo	3
		PT (AVERÍA)	Mal uso o infortunio.	El daño causado será asumible por el sistema.	Mantenimiento.	Medio bajo	3
Armario	FÍSICO	AHUAF (ATAQUE FÍSICO)	Intención de perjudicar o retrasar las actividades planificadas.	Gravedad máxima.	Protección del equipo en la organización	Bajo	2
		PT (AVERÍA)	Mal uso o infortunio.	El daño causado será asumible por el sistema.	Mantenimiento.	Medio bajo	3
Laptop	FÍSICO	AHUMT (HURTO)	Interés por las lap tops.	Gravedad máxima.	Limitación de acceso a las instalaciones de la organización.	Medio bajo	3
		AHUAF (ATAQUE FÍSICO)	Intención de perjudicar o retrasar las actividades planificadas.	El daño causado será asumible por el sistema.		Bajo	2
		PT (AVERÍA)	Mal uso o infortunio.		Mantenimiento.	Medio	4
Gabinete de Red	FÍSICO	AHUAF (ATAQUE FÍSICO)	Intención de perjudicar o retrasar las actividades planificadas.	Puede invalidar los trabajos planificados.	Protección del equipo en la organización	Bajo	2
		PT (AVERÍA)	Mal uso o infortunio.	El daño causado será asumible por el sistema.	Mantenimiento.	Medio bajo	3
Modem	FÍSICO	AHUMT (HURTO)	Interés por los modems.	Gravedad máxima.	Limitación de acceso a las instalaciones de la organización.	Medio bajo	3
		AHUAF (ATAQUE FÍSICO)	Intención de perjudicar o retrasar las actividades planificadas.	Puede invalidar los trabajos planificados.		Bajo	2
		PT (AVERÍA)	Mal uso o infortunio.	El daño causado será asumible por el sistema.	Mantenimiento.	Medio	3
switch (Cisco)	FÍSICO	AHUMT (HURTO)	Interés por los switchs	Gravedad máxima.	Limitación de acceso a las instalaciones de la organización.	Medio bajo	2
		AHUAF (ATAQUE FÍSICO)	Intención de perjudicar o retrasar las actividades planificadas.			Bajo	2
		PT (AVERÍA)	Mal uso o infortunio.	El daño causado será asumible por el sistema.	Mantenimiento.	Medio bajo	3
Cableado de red	FÍSICO	AHUMT (HURTO)	Interés por los cables de red.	Gravedad máxima.	Limitación de acceso a las instalaciones de la organización.	Bajo	2
		AHUAF (ATAQUE FÍSICO)	Intención de perjudicar o retrasar las actividades planificadas.	Produce retras en las actividades.		Bajo	2
		PT (AVERÍA)	Mal uso o infortunio.		Mantenimiento.	Medio bajo	3
Cuadernos y Libros (Datos físicos)	INFORMACIÓN	AHUMT (HURTO)	Interés por la información de los cuadernos y libros.	Gravedad máxima	Protección del equipo en la organización	Bajo	2
		AHUAF (DESTRUCIÓN)	Mal uso o infortunio / Intención de perjudicar o retrasar las actividades		Mantenimiento.	Bajo	2
Datos almacenados	INFORMACIÓN	AHUMT (HURTO)	Intención de acceder a información para la que no se tiene permiso.	Gravedad máxima si se accede a datos confidenciales.	Protección del equipo en la organización	Bajo	2
		AHUAF (ACCESO A DATOS PRIVADOS)			Mantenimiento.	Bajo	2
Libro de Reclamos	INFORMACIÓN	AHUMT (HURTO)	Interés por la información.	Puede invalidar los trabajos planificados.	Protección del equipo en la organización	Medio bajo	3
		AHUAF (ATAQUE FÍSICO)	Intención de perjudicar o retrasar las actividades planificadas.		Mantenimiento.	Medio bajo	3
Director de la Escuela de	PERSONAS	AHUAM (INDISPONIBILIDAD DEL DIRECTOR DE LA ESCUELA)	Inasistencia de la Decana de Postgrado.	Una mala administración de equipos produciría retraso en las actividades planificadas si no se resuelve con tiempo.	Compromiso, responsabilidad y disponibilidad	Bajo	2
Personal Responsable	PERSONAS	AHUAM (INDISPONIBILIDAD DEL PERSONAL RESPONSABLE)	Inasistencia del personal responsable.			Bajo	2
Software de Plataforma (Windows 8.1)	SOFTWARE	PT (LICENCIA)	Término y restricción del acceso al	Limita las herramientas del software.	No tiene salvaguarda	Medio bajo	3
		PT (ATAQUES DE HACKERS Y SPYWARE)	Intención de perjudicar o retrasar las actividades planificadas.	Afecta la disponibilidad		Medio bajo	3
		PT (INESTABILIDAD)	Falla desoftware de plataforma.	Paralización de actividades planificadas.		Medio bajo	3
Software de Documentación (Microfoft Office)	SOFTWARE	PT (AVERÍA)	Mal uso o infortunio.	Puede invalidar los trabajos planificados.	No tiene salvaguarda	Medio bajo	3
		PT (INESTABILIDAD)	Falla desoftware de plataforma.	Paralización de actividades planificadas.		Medio bajo	3
Software de estadística (SPSS)	SOFTWARE	PT (AVERÍA)	Mal uso o infortunio.	Puede invalidar los trabajos planificados.	No tiene salvaguarda	Medio bajo	3
		PT (INESTABILIDAD)	Falla desoftware de plataforma.	Paralización de actividades planificadas.		Medio bajo	3
Software de Información Geográfica (ArcGIS)	SOFTWARE	PT (AVERÍA)	Mal uso o infortunio.	Puede invalidar los trabajos planificados.	No tiene salvaguarda	Medio bajo	3
		PT (INESTABILIDAD)	Falla desoftware de plataforma.	Paralización de actividades planificadas.		Medio bajo	3
Software de Seguridad	SOFTWARE	PT (LICENCIA)	Falla desoftware de seguridad.	Produciría retraso en las actividades planificadas si no se resuelve a tiempo	Actualizaciones frecuentes	Medio bajo	3
Administración de permisos	INFORMACIÓN	AHUMT (SUPLANTACIÓN DE DENTIDAD)	Intención de obtener más permiso de lo as	Se produce un acceso no deseado a la información.	Administración de accesos a la información.	Bajo	2
		AHUAF (FILTRACIÓN DE INFORMACIÓN)	Intención de obtener información privada (	Puede ocasionar pérdida permanente de información y causar dañoss		Bajo	2
Página web (http://posgrado.unheval.edu.pe/)	SOFTWARE	PT (LICENCIA)	Término y restricción del acceso al softwar	Produciría retraso en las actividades planificadas si no se resuelve a tiempo	Actulizaciones, seguridad del sistema del equipo.	Bajo	2
		PT (ATAQUE CON HACKERS Y SPYWARE)	Intención de perjudicar o retrasar las actividades planificadas.	Afecta la disponibilidad		Bajo	2
		PT (INESTABILIDAD)	Falla de página web	Paralización de actividades planificadas.		Medio bajo	3
Internet	INFORMACIÓN	PT (ATAQUE A LA RED INTERNA CON RITUS INFORMATICO)	Intención de acceder a información de la o	Produciría retraso en las actividades planificadas si no se resuelve a tiempo	Actulizaciones, seguridad del sistema del equipo.	Bajo	2
		AHUMT (HURTO y/o ENVIO DE INFORMACIÓN CONFIDENCIAL)	Beneficio propio y/o de terceros.	Fuga de información interna de violación a las formas internas de		Medio bajo	3
		AHUAF (ACCESO NO PERMITIDO)	Intención de perjudicar o retrasar las actividades planificadas.	Paralización de actividades planificadas.		Bajo	2
Extintor	FÍSICO	AHUMT (HURTO)	Interés por los extintores.	Gravedad máxima	Revisión, mantenimiento continuo y llenado del contenido periódicamente.	Medio bajo	3
		AHUAF (ATAQUE FÍSICO)	Intención de perjudicar o retrasar las actividades planificadas.	La organización queda expuesta a un nivel bajo de seguridad ante cualquier incidencia		Bajo	2
		PT (CADUCIDAD)	Falla de extintores.				3
		PT (AVERÍA)	Mal uso o infortunio.			Bajo	2
Dispositivo Extraible (CD/DVD, USB)	FÍSICO	AHUMT (HURTO)	Interés por los dispositivo.	Gravedad máxima.	Limitación de acceso a las instalaciones de la organización.		3
		AHUAF (ATAQUE FÍSICO)	Intención de perjudicar o retrasar las actividades planificadas.	Puede invalidar los trabajos planificados.		Bajo	2
		PT (AVERÍA)	Mal uso o infortunio.	El daño causado será asumible por el sistema.	Mantenimiento.	Bajo	2
Servidor	FÍSICO	AHUMT (HURTO)	Interés por los servidores.	Gravedad máxima.	Limitación de acceso a las instalaciones de la organización.	Bajo	2
		AHUAF (ATAQUE FÍSICO)	Intención de perjudicar o retrasar las actividades planificadas.	Puede invalidar los trabajos planificados.		Bajo	2
		PT (AVERÍA)	Mal uso o infortunio.	El daño causado será asumible por el sistema.	Mantenimiento.	Medio bajo	3
Cámara de video	FÍSICO	AHUMT (HURTO)	Interés por las cámaras de video.	Gravedad máxima.	Limitación de acceso a las instalaciones de la organización.		3
		AHUAF (ATAQUE FÍSICO)	Intención de perjudicar o retrasar las actividades planificadas.	Puede invalidar los trabajos planificados.		Bajo	2
		PT (AVERÍA)	Mal uso o infortunio.	El daño causado será asumible por el sistema.	Mantenimiento.	Bajo	2

Muy bajo	1
Bajo	2
Medio bajo	3
medio	4
Medio alto	5
Alto	6
Muy alto	7

IDENTIFICACIÓN DE ESCENARIOS DE AMENAZA Y CRITERIO DE MEDICIÓN									
ACTIVO	NIVEL	ARBOL DE AMENAZA	SALVAGUARDA	POSIBILIDAD DE OCURRENCIA DE UNA		IMPACTO		RIESGO CALCULADO	
				CRITERIO DE MEDICIÓN	VALOR	CRITERIO DE MEDICIÓN	VALOR		
Equipo de Cómput	FÍSICO	AHUMT (HURTO)	Limitación de acceso a las instalacones de la	Bajo	2	Muy alto	5	10	24%
		AHUAF (ATAQUE FÍSICO)		Bajo	2	Alto	4	8	19%
		PT (AVERÍA)	Mantenimiento.	Medio	4	Alto	4	16	38%
Estabilizador de En	FÍSICO	AHUMT (HURTO)	Limitación de acceso a las instalacones de la	Medio bajo	3	Muy alto	5	15	36%
		AHUAF (ATAQUE FÍSICO)		Bajo	2	Medio	3	6	14%
		PT (AVERÍA)	Mantenimiento.	Medio bajo	3	Medio	3	9	21%
Impresora	FÍSICO	AHUMT (HURTO)	Limitación de acceso a las instalacones de la	Medio bajo	3	Muy alto	5	15	36%
		AHUAF (ATAQUE FÍSICO)		Bajo	2	Muy alto	5	10	24%
		PT (AVERÍA)	Mantenimiento.	Medio	4	Medio	3	12	29%
Proyector multime	FÍSICO	AHUAF (ATAQUE FÍSICO)	Protección del equipo en	Medio bajo	3	Medio	3	9	21%
		PT (AVERÍA)	Mantenimiento.	Medio bajo	3	Alto	4	12	29%
Armario	FÍSICO	AHUAF (ATAQUE FÍSICO)	Protección del equipo en	Medio bajo	3	Alto	4	12	29%
		PT (AVERÍA)	Mantenimiento.	Bajo	2	Muy alto	5	10	24%
Laptop	FÍSICO	AHUMT (HURTO)	Limitación de acceso a las instalacones de la	Medio bajo	3	Muy alto	5	15	36%
		AHUAF (ATAQUE FÍSICO)		Medio bajo	3	Muy alto	5	15	36%
		PT (AVERÍA)	Mantenimiento.	Bajo	2	Alto	4	8	19%
Gabinete de Red	FÍSICO	AHUAF (ATAQUE FÍSICO)	Protección del equipo en	Medio	4	Medio	3	12	29%
		PT (AVERÍA)	Mantenimiento.	Bajo	2	Alto	4	8	19%
Modem	FÍSICO	AHUMT (HURTO)	Limitación de acceso a las instalacones de la	Medio bajo	3	Muy alto	5	15	36%
		AHUAF (ATAQUE FÍSICO)		Medio bajo	3	Muy alto	5	15	36%
		PT (AVERÍA)	Mantenimiento.	Bajo	2	Alto	4	8	19%
switch (Cisco)	FÍSICO	AHUMT (HURTO)	Limitación de acceso a las instalacones de la	Medio	3	Muy alto	5	15	36%
		AHUAF (ATAQUE FÍSICO)		Medio bajo	2	Muy alto	5	10	24%
		PT (AVERÍA)	Mantenimiento.	Bajo	2	Alto	4	8	19%
Cableado de red	FÍSICO	AHUMT (HURTO)	Limitación de acceso a las instalacones de la	Medio bajo	3	Muy alto	5	15	36%
		AHUAF (ATAQUE FÍSICO)		Bajo	2	Muy alto	5	10	24%
		PT (AVERÍA)	Mantenimiento.	Bajo	2	Alto	4	8	19%
Cuadernos y Libros	INFORMACIÓN	AHUAF (ATAQUE FÍSICO)	Protección del equipo en	Medio bajo	3	Medio	3	9	21%
		PT (AVERÍA)	Mantenimiento.	Bajo	2	Alto	4	8	19%
Datos almacenados	INFORMACIÓN	AHUAF (ATAQUE FÍSICO)	Protección del equipo en	Bajo	2	Medio	3	6	14%
		PT (AVERÍA)	Mantenimiento.	Bajo	2	Alto	4	8	19%
Libro de Reclamos	INFORMACIÓN	AHUAF (ATAQUE FÍSICO)	Protección del equipo en	Bajo	2	Medio	3	6	14%
		PT (AVERÍA)	Mantenimiento.	Medio bajo	3	Alto	4	12	29%
Director de la Escue	PERSONAS	AHUMT (INDISPONIBILIDAD DEL	Compromiso, responsabilidad y	Medio bajo	3	Alto	4	12	29%
Personal Responsa	PERSONAS	AHUMT (INDISPONIBILIDAD DEL	Compromiso, responsabilidad y	Bajo	2	Alto	4	8	19%
Software de Plataf	SOFTWARE	PT (LICENCIA)	No tiene salvaguarda	Bajo	2	Alto	4	8	19%
		PT (ATAQUES DE HACKERS Y SPYWARE)		Medio bajo	3	Alto	4	12	29%
		PT (INESTABILIDAD)		Medio bajo	3	Muy alto	5	15	36%
Software de Documentación	SOFTWARE	PT (LICENCIA)	No tiene salvaguarda	Medio bajo	3		6	18	43%
		PT (INESTABILIDAD)		Medio bajo	3	Muy alto	5	15	36%
Software de estadística (SPSS)	SOFTWARE	PT (LICENCIA)	No tiene salvaguarda	Medio bajo	3		6	18	43%
		PT (INESTABILIDAD)		Medio bajo	3	Muy alto	5	15	36%
Software de Información	SOFTWARE	PT (LICENCIA)	No tiene salvaguarda	Medio bajo	3		6	18	43%
		PT (INESTABILIDAD)		Medio bajo	3	Muy alto	5	15	36%
Seguridad (Antivirus - ESET	SOFTWARE	PT (LICENCIA)	Actualizaciones frecuentes	Medio bajo	3	Muy alto	5	15	36%
Administración de	INFORMACIÓN	AHUMT (SUPLANTACIÓN DE DENTIDAD)	Administración de accesos a la información.	Medio bajo	3	Muy alto	5	15	36%
		AHUAF (FILTRACIÓN DE INFORMACIÓN)		Bajo	2	Muy alto	5	10	24%
Página web (http://posgrado. unheval.edu.pe/)	SOFTWARE	PT (LICENCIA)	Actualizaciones, seguridad del sistema del equipo.	Bajo	2	Alto	4	8	19%
		PT (ATAQUE CON HACKERS Y SPYWARE)		Bajo	2	Alto	4	8	19%
		PT (INESTABILIDAD)		Bajo	2	Alto	4	8	19%
Internet	INFORMACIÓN	PT (ATAQUE A LA RED INTERNA CON RITUS	Actulizaciones, seguridad del sistema del equipo.	Medio bajo	3	Muy alto	5	15	36%
		AHUMT (HURTO y/o ENVIO DE INFORMACIÓN		Bajo	2	Muy alto	5	10	24%
		AHUAF (ACCESO NO PERM		Medio bajo	3	Muy alto	5	15	36%
Extintor	FÍSICO	AHUMT (HURTO)	Revisión, mantenimiento continuo y llenado del contenido periódicamente.	Bajo	2	Muy alto	5	10	24%
		AHUAF (ATAQUE FÍSICO)		Medio bajo	3	Muy alto	5	15	36%
		PT (CADUCIDAD)		Bajo	2	Muy alto	5	10	24%
		PT (AVERÍA)		Medio bajo	3	Muy alto	5	15	36%
Dispositivo Extraib	FÍSICO	AHUMT (HURTO)	Limitación de acceso a las instalacones de la	Bajo	2	Muy alto	5	10	24%
		AHUAF (ATAQUE FÍSICO)		Medio bajo	3	Muy alto	5	15	36%
		PT (AVERÍA)	Mantenimiento.	Bajo	2	Alto	4	8	19%
Servidor	FÍSICO	AHUMT (HURTO)	Limitación de acceso a las instalaciones de la	Bajo	2	Muy alto	5	10	24%
		AHUAF (ATAQUE FÍSICO)		Bajo	2	Muy alto	5	10	24%
		PT (AVERÍA)	Mantenimiento.	Bajo	2	Alto	4	8	19%
Cámaras de video	FÍSICO	AHUMT (HURTO)	Limitación de acceso a las instalaciones de la	Medio bajo	3	Muy alto	5	15	36%
		AHUAF (ATAQUE FÍSICO)		Bajo	3	Muy alto	5	15	36%
		PT (AVERÍA)	Mantenimiento.	Bajo	2	Alto	4	8	19%

	N°	CAPA	CODIGO	ACTIVO	PROBABILIDAD	DIMENSIONES					VALOR
						[D]	[I]	[C]	[A]	[T]	[P]
ACTIVOS ESCENCIALES [esencial]	AED1	DATOS [data]	[dal]	Datos almacenados	3	18	18	15			17
	AED2	INFORMACION [info]	[cyl]	Tesis y libros(Datos fisicos)	3	15	12	9			12
	AED3		[ldr]	Libro de Reclamos	4	20		8	4		11
	AED4	SERVICIO [service]	[adp]	Administracion de permisos	4	12			20	20	17
APLICACIONES INFORMATICAS [appe]	APS1	SOFTWARE [SW]	[sdp]	Software de Plataforma(Windows 8.1)	3	12			15	24	17
	APS2		[sdd]	Software de Documentacion (Microsoft Office)	4	16		16			16
	APS3		[sps]	Software de estadística (SPSS)	4	16		16			16
	APS4		[ags]	Software de Información Geográfica (ArcGIS)	4	16		16			16
	APS5		[sds]	Software de Seguridad (Antivirus-Not)	3	9	15				12
	APS6		[web]	Página Web EPG	4	24	16	8	16	16	16
EQUIPOS INFORMATICOS [einf]	EIH1	HARDWARE [HW]	[edc]	Equipo de Computo	4	24	20	20			21
	EIH2		[imp]	Impresora	3	9					9
	EIH4		[lap]	Laptop	4	24	20	28			24
	EIH5		[mod]	Modem	4	16	8		8		11
	EIH6		[swt]	Switch(CISCO)	4	24	20	12	16	8	16
	EIH7		[svd]	Servidor	4	24	20	20			21
COMUNICACIONES [ccm]	CRC1	REDES	[int]	Internet	4	16	8	4	4		8
SOPORTES DE INFORMACIÓN	SIS1	SOPORTE	[ext]	Dispositivos Extraibles (CD/DVD,USB)	4	4	4	4		4	4
	SIS2		[pro]	Proyector Multimedia	4	4	4			4	4
	SIS3		[cmr]	Cámara de video	4	4	4			4	4
EQUIPAMIENTO AUXILIAR	EAE1	EQUIPAMIENTO	[est]	Estabilizador de Energia	3	15	9			3	9
	EAE2		[cab]	Cableado de Red	4	12		4			8
	EAE3		[ext]	Extintor	3	9	9			3	7
INSTALACIONES [ins]	INI1	INSTALACIÓN	[arm]	Armario	4		12	8	4		8
	INI2		[gab]	Gabinete de Red	3	12	6			3	7
PERSONAL [per]	PSP1	PERSONAL	[ddf]	Dirección de la EPG	4		8	8	8		8
	PSP2		[sec]	Jefe de cómputo	3	9	3				6

	N°	CÓDIGO	ACTIVO	OBABILID	DIMENSIONES				
					[D]	[I]	[C]	[A]	[T]
ACTIVOS ESENCIALES [essential]	AED1	[dal]	**Datos almacenados**	3	70%	70%	60%	10%	10%
		OI6	Avería de origen físico o lógico (I6)	4	50%	50%			
		OI11	Degradación de los soportes de almacenamiento	3	60%	40%			
		EF1	Errores de los usurios (E1)	3	60%	60%	60%		
		EF5	Deficiencia en la organización (E5)	3	50%		30%		
		EF6	Difusión de software dañino (E6)	4	70%	60%	50%		
		EF12	Errores de mantenimiento o actualizaciones de s	3	60%	60%			
		AI7	Acceso no autorizado (E7)	3		70%	60%		
		AI11	Modificación deliberada debla información (A11	4		70%			10%
		AI12	Destrucción de información (A12)	3	70%			10%	
	AED2	[cyl]	**Cuadernos y Libros (Datos físicos)**	3	70%	60%	60%	0%	10%
		OI4	Contaminación Mecánica (I4)	3	60%	30%			
		OI11	Degradación de los soportes de almancenament	3	40%				
		EF1	Errores de los usuarios (E1)	4	40%	60%	50%		
		EF2	Errores de los administrativos (E2)	4	60%	50%	40%		
		AI7	Acceso no autorizado (A7)	3		40%	50%		10%
		AI12	Destrucción de información (A12)	3	60%				
		AI16	Robo (A16)	3	70%		60%		
	AED3	[ldr]	**Libro de Reclamos**	4	60%	60%	50%	10%	10%
		OI4	Contaminación Mecánica (I4)	3	60%	30%			
		OI11	Degradación de los soportes de almancenament	3	40%				
		EF1	Errores de los usuarios (E1)	4	40%	60%	50%		
		EF2	Errores de los administrativos (E2)	4	40%	50%	40%		
		AI7	Acceso no autorizado (A7)	5		40%	50%		10%
		AI13	Divulgación de información (AI13)	4	60%			10%	
	AED4	[adp]	**Administración de permisos**	4	60%	40%	50%	50%	60%
		EF5	Deficiencia en la organización (E5)	3	60%				
		AI3	Abuso de privilegios de acceso (A3)	4	50%	40%	50%		
		AI4	Uso no previsto (A4)	3	50%	40%	50%		60%
		AI13	Divulgación de información (AI13)	4	60%			50%	
APLICACIONES INFORMÁTICAS [apps]	APS1	[sdp]	**Software de Plataforma (Windows 8.1)**	3	60%	60%	70%	60%	80%
		EF2	Error del administrador (E2)	3	60%	50%	50%		
		EF12	Errores de mantenimiento o actulización de softv	3	50%	60%			
		AI3	Abuso de privilrgios de accesos (A3)	3	50%	60%	70%		80%
		AI4	Uso no provisto (A4)	3	60%	40%	50%		
		AI7	Acceso no autorizado (A7)	3		60%	70%	60%	
	APS2	[sdd]	**Software de Documentación (Microfoft Office)**	4	60%	60%	70%	50%	10%
		EF12	Errores de mantenimiento o actulización de softv	4	60%	60%			10%
		AI1	Manipulación de la configuración (A1)	4	40%	60%	70%	50%	
	APS3	[sps]	**Software de estadística (SPSS)**	4	60%	60%	70%	50%	10%
		EF12	Errores de mantenimiento o actulización de softv	4	60%	60%			10%
		AI1	Manipulación de la configuración (A1)	4	40%	60%	70%	50%	
	APS4	[ags]	**Software de Información Geográfica (ArcGIS)**	4	60%	60%	70%	50%	10%
		EF12	Errores de mantenimiento o actulización de softv	4	60%	60%			10%
		AI1	Manipulación de la configuración (A1)	4	40%	60%	70%	50%	
	APS5	[sds]	**Software de Seguridad (Antivirus - ESET NOD32**	3	70%	70%	60%	20%	10%
		EF4	Error de configuración (E4)	3	40%	70%			
		EF6	Difusión de software dañino (E6)	4	70%	60%	60%		
		EF12	Errores de mantenimiento o actulización de softv	2	60%	70%	60%		
		AI1	Manipulación de la configuración (A1)	3		70%	60%	20%	10%
	APS6	[web]	**Página web (http://posgrado.unheval.edu.pe/)**	4	90%	60%	40%	60%	60%
		OI6	Avería de origen físico o lógico (I6)	3	60%				
		OI9	Fallo de servicios de comunicaciones (I9)	4	70%			60%	60%
		EF2	Errores de administrador (E2)	3	90%	60%	40%		
		EF12	Errores de mantenimiento o actulización de softv	4	50%	60%			
EQUIPOS INFORMÁTICOS [einf]	EIH1	[edc]	**Equipo de Cómputo**	4	80%	70%	70%	10%	10%
		OI4	Contaminación Mecánica (I4)	3	60%			10%	
		OI6	Avería de origen físico o lógico (I6)	4	70%	50%			
		EF13	Errores de mantenimiento o actulización de equi	3	80%	20%			
		AI1	Manipulación de la configuración (A1)	4	60%	70%	60%		
		AI15	Manipulación de los equipos (A15)	4	60%		60%		
		AI16	Robo (A16)	3	60%		70%		10%
	EIH2	[imp]	**Impresora**	3	60%	40%	50%	30%	0%
		OI6	Avería de origen físico o lógico (I6)	4	50%	10%			
		EF1	Errores de los usuarios (E1)	3	60%	40%	50%	30%	
		AI15	Manipulación de los equipos (A15)	3	60%		40%		
	EIH4	[lap]	**Laptop**	4	80%	70%	70%	10%	10%
		OI4	Contaminación Mecánica (I4)	3	60%			10%	
		OI6	Avería de origen físico o lógico (I6)	4	70%	50%			
		EF13	Errores de mantenimiento o actulización de equi	3	80%	20%			
		AI1	Manipulación de la configuración (A1)	4	60%	70%	60%		
		AI15	Manipulación de los equipos (A15)	4	60%		60%		
		AI16	Robo (A16)	3	60%		70%		10%
	EIH5	[mod]	**Modem**	4	60%	60%	10%	50%	50%
		OI4	Contaminación Mecánica (I4)	4	60%			10%	
		OI7	Corte del suministro eléctrico (I/)	3	50%	60%		20%	
		OI9	Fallo de servicios de comunicaciones (I9)	4	50%			30%	50%
		OI11	Degradacion de los soportes de almacenamiento	4		60%			
		EF1	Errores de los usuarios (E1)	3		60%		30%	
		EF13	Errores de mantenimiento o actulización de equi	3		20%		50%	50%
		AI6	Re-encaminamiento o alteración de mensajes (A	4		30%	10%		
	EIH6	[swt]	**Switch (Cisco)**	4	60%	50%	40%	70%	40%
		OI4	Contaminación Mecánica (I4)	3	50%				
		OI6	Avería de origen físico o lógico (I6)	3	60%	50%	40%	10%	20%
		OI7	Corte del suministro eléctrico (I/)	4	50%			20%	
		OI9	Fallo de servicios de comunicaciones (I9)	3	30%	50%	40%	70%	40%
		EF4	Errores de configuración (E4)	4	30%			30%	
		AI1	Manipulación de la configuración (A1)	4	60%				
	EIH1	[svd]	**Servidor**	4	80%	70%	70%	10%	10%
		OI4	Contaminación Mecánica (I4)	3	60%			10%	
		OI6	Avería de origen físico o lógico (I6)	4	70%	50%			
		EF13	Errores de mantenimiento o actulización de equi	3	80%	20%			
		AI1	Manipulación de la configuración (A1)	4	60%	70%	60%		
		AI15	Manipulación de los equipos (A15)	4	60%		60%		
		AI16	Robo (A16)	3	60%		70%		10%
COMUNICACIONES [com]	CRC1	[int]	**Internet**	4	60%	50%	30%	30%	40%
		OI 5	Desastres industriales (I5)	3	60%			20%	
		OI6	Avería de origen físico o lógico (I6)	4	40%	50%	30%	30%	40%
		EF10	Destrucción de información (A12)	4	20%				20%
SOPORTE DE INFORMATICO	SIS1	[ext]	**Dispositivo Extraible (CD/DVD, USB)**	4	50%	50%	50%	30%	30%
		EF1	Errores de los usuarios (E1)	3	40%	30%	40%	30%	
		EF10	Destrucción de información (A12)	4	50%	40%	50%	30%	
		AI4	Uso no previsto (A4)	5	10%	40%	20%	30%	20%
		AI17	Ataque destructivo (A17)	4	30%	50%	30%	20%	30%
	SIS2	[pro]	**Proyector multimedia**	4	40%	20%	30%	40%	30%
		OI6	Avería de origen físico o lógico (I6)	3	30%	20%	30%	20%	30%
		OI9	Fallo de servicios de comunicaciones (I9)	4	40%		20%	40%	
	SIS3	[cmr]	**Cámara de video**	4	40%	20%	30%	40%	30%
		OI6	Avería de origen físico o lógico (I6)	3	30%	20%	30%	20%	30%
		OI9	Fallo de servicios de comunicaciones (I9)	4	40%		20%	40%	
EQUIPAMIENTO AUXILIAR [eax]	EAE1	[est]	**Estabilizador de energía**	3	60%	50%	30%	20%	30%
		OI6	Avería de origen físico o lógico (I6)	2	60%	50%	30%	20%	30%
		OI9	Corte del suministro eléctrico (I/)	3	50%	20%			
	EAE2	[cab]	**Cableado de red**	4	60%	50%	30%	20%	10%
		OI3	Contaminación Electromagnética (I3)	3	40%	10%			
		OI5	Desastres industriales (I5)	4	60%	50%			
		OI9	Fallo de servicios de comunicaciones (I9)	4	50%	30%	30%	20%	10%
	EAE3	[ext]	**Extintor**	3	50%	40%	50%	30%	30%
		OI5	Desastres industriales (I5)	3	30%	10%			
		OI11	Degradación de los soportes de almacenamiento	3	50%	40%	50%	30%	30%
INSTALACIONES [ins]	INI1	[arm]	**Armario**	4	50%	60%	50%	30%	30%
		IO6	Avería de origen físico o lógico (I6)	3	50%	60%	50%	20%	30%
		AI3	Abuso de privilegios de acceso (A3)	4	40%			30%	
	INI2	[gab]	**Gabinete de Red**	3	50%	50%	60%	30%	30%
		OI4	Contaminación Mecánica (I4)	3	50%	50%	60%	20%	30%
		AI4	Uso de previsto (A4)	4		20%	20%		
		AI7	Acceso no autorizado (A7)	3		50%	60%		
		AI18	Ocupación enemiga (A18)	3	30%			30%	
PERSONAL [per]	PSP1	[ddf]	**Director de la Escuela de Posgrado**	4	20%	50%	40%	50%	60%
		AI15	Manipulación de los equipos (A15)	3		50%		50%	
		AI19	Indisponibilidad del personal (A19)	4	20%		40%		60%
	PSP2	[sec]	**Personal Responsable (Secretaria)**	3	50%	20%	50%	30%	60%
		AI2	Suplantación de la identidad del usuario (A2)	2	50%	20%	50%	20%	60%
		AI11	Modificación deliberada debla información (A11	3	50%			30%	
		AI19	Indisponibilidad del personal (A19)	4	20%		40%		60%

PROBABILIDAD	DIMENSIONES					VALOR [P]		N°	CAPA	CODIGO	ACTIVO	PROBABILIDAD	DIMENSIONES					VALOR [P]
	[D]	[I]	[C]	[A]	[T]								[D]	[I]	[C]	[A]	[T]	
3	6	6	5			6	ACTIVOS ESCENCIALES [esencial]	AED1	DATOS [data]	[dal]	Datos almacenados	3	18	18	15			17
3	5	4	3			4		AED2	INFORMACION [nfo]	[cyl]	Tesis y libros(Datos fisicos)	3	15	12	9			12
4	5		2	1		3		AED3		[ldr]	Libro de Reclamos	4	20		8	4		11
4	3			5	5	4		AED4	SERVICIO [service]	[adp]	Administracion de permisos	4	12			20	20	17
3	4			5	8	6	APLICACIONES INFORMATICAS [appe]	APS1	SOFTWARE [SW]	[sdp]	Software de Plataforma(Windows 8.1)	3	12			15	24	17
4	4		4			4		APS2		[sdd]	Software de Documentacion (Microsoft Office)	4	16		16			16
4	4		4			4		APS3		[sps]	Software de estadística (SPSS)	4	16		16			16
4	4		4			4		APS4		[ags]	Software de Información Geográfica (ArcGIS)	4	16		16			16
3	3	5				4		APS5		[sds]	Software de Seguridad (Antivirus-Not)	3	9	15				12
4	6	4	2	4	4	4		APS6		[web]	Página Web EPG	4	24	16	8	16	16	16
4	6	5	5			5	EQUIPOS INFORMATICOS [einf]	EIH1	HARDWARE [HW]	[edc]	Equipo de Computo	4	24	20	20			21
3	3					3		EIH2		[imp]	Impresora	3	9					9
4	6	5	7			6		EIH4		[lap]	Laptop	4	24	20	28			24
4	4	2		2		3		EIH5		[mod]	Modem	4	16	8		8		11
4	6	5	3	4	2	4		EIH6		[swt]	Switch(CISCO)	4	24	20	12	16	8	16
4	6	5	5			5		EIH7		[svd]	Servidor	4	24	20	20			21
4	4	2	1	1		2	COMUNICACIONES [ccm]	CRC1	REDES	[int]	Internet	4	16	8	4	4		8
4	1	1	1		1	1	SOPORTES DE INFORMACIÓN	SIS1	SOPORTE	[ext]	Dispositivos Extraibles (CD/DVD,USB)	4	4	4	4		4	4
4	1	1			1	1		SIS2		[pro]	Proyector Multimedia	4	4	4			4	4
4	1	1			1	1		SIS3		[cmr]	Cámara de video	4	4	4			4	4
3	5	3			1	3	EQUIPAMIENTO AUXILIAR	EAE1	EQUIPAMIENTO	[est]	Estabilizador de Energia	3	15	9			3	9
4	3		1			2		EAE2		[cab]	Cableado de Red	4	12		4			8
3	3	3			1	2		EAE3		[ext]	Extintor	3	9	9			3	7
4		3	2	1		2	INSTALACIONES [ins]	INI1	INSTALACIÓN	[arm]	Armario	4		12	8	4		8
3	4	2			1	2		INI2		[gab]	Gabinete de Red	3	12	6			3	7
4		2	2	2		2	PERSONAL [per]	PSP1	PERSONAL	[ddf]	Dirección de la EPG	4		8	8	8		8
3	3	1				2		PSP2		[sec]	Jefe de cómputo	3	9	3				6