UNIVERSIDAD SAN PEDRO

FACULTAD DE INGENIERÍA

PROGRAMA DE ESTUDIOS DE INGENIERÍA INFORMÁTICA Y DE SISTEMAS

Metodología Magerit y su relación con gestión de riesgos de seguridad del sistema de información en MiBanco, Huaraz 2023

Tesis para obtener el título profesional de Ingeniero en Informática y de Sistemas

Autora

Silva Medina Ketty Milagros

Asesor

Wilmer Pasión Carrasco Alvarado

Código ORCID 0000-0003-3138-9808

Huaraz – Perú

2023

ÍNDICE GENERAL

ÍNDICE DE TABLAS

PALABRAS CLAVE:

Tema	Seguridad Informática
Especialidad	Sistemas de información

KEYWORDS:

Theme	Security Policy
Specialty	Information System

LÍNEA DE INVESTIGACIÓN:

Línea	Sistema de Seguridad
Área	Ciencias Sociales
Sub Área	Economía y Negocios
Disciplina	Negocios y Management

USP UNIVERSIDAD SAN PEDRO | VICERRECTORADO DE INVESTIGACIÓN

CONSTANCIA DE ORIGINALIDAD

El que suscribe, Vicerrector de Investigación de la Universidad San Pedro:

HACE CONSTAR

Que, de la revisión del trabajo titulado **"Metodología Magerit y su relación con gestión de riesgos de seguridad del sistema de información en MiBanco, Huaraz 2023"** del (a) estudiante: **SILVA MEDINA KETTY MILAGROS**, identificado(a) con Código N° **1413100283**, se ha verificado un porcentaje de similitud del **22%**, el cual se encuentra dentro del parámetro establecido por la Universidad San Pedro mediante resolución de Consejo Universitario N° 5037-2019-USP/CUpara la obtención de grados y títulos académicos de pre y posgrado, así como proyectos de investigación anual Docente.

Se expide la presente constancia para los fines pertinentes.

Chimbote, 12 de diciembre de 2023

UNIVERSIDAD SAN PEDRO
VICERRECTORADO DE INVESTIGACIÓN
Dr. JAVIER MARTÍNEZ CARRIÓN
VICERRECTOR

NOTA: Este documento carece de valor si no tiene adjunta el reporte del Software TURNITIN.

TÍTULO

Metodología Magerit y su relación con gestión de riesgos de seguridad del sistema de información en MiBanco, Huaraz 2023

RESUMEN

La presente investigación tuvo como objetivo general fue determinar la relación entre de la aplicación de la metodología Magerit con la Gestión de riesgos de seguridad del sistema de información en MiBanco, Huaraz 2023, la hipótesis general consistió en que la aplicación de la metodología Magerit se relaciona positivamente con la Gestión de riesgos de seguridad del sistema de información. Se aplico investigación descriptiva correlación no experimental, se trabajó con 48 activos informáticos, se aplicó ficha de registro de datos como instrumento. Como resultado general se tuvo que existió correlación positiva alta y significativa de 0.706 entre la variable Aplicación de la metodología Magerit con la variable Gestión de riesgos de seguridad de los activos informáticos en MiBanco, Huaraz 2023. Existió correlación positiva moderada significativa moderada de 0.679 entre la variable Aplicación de la metodología Magerit con la dimensión Gestión de riesgos de seguridad de hardware. Existió correlación positiva moderada y significativa de 0.660 entre la variable Aplicación de la metodología Magerit con la dimensión Gestión de riesgos de seguridad de software. Existió correlación positiva alta significativa de 0.735 entre la variable Aplicación de la metodología Magerit con la dimensión Gestión de riesgos de seguridad de la información. En todos los casos el p valor o valor de significancia o error fue de 0.000, lo cual indicó que los datos no correspondieron a una curva normal.

ABSTRACT

The general objective of this research was to determine the relationship between the application of the Magerit methodology with the Security Risk Management of the information system in MiBanco, Huaraz 2023, the general hypothesis was that the application of the Magerit methodology is positively related to the Security Risk Management of the information system. Descriptive non-experimental correlation research was applied, 48 computer assets were worked with, data registration form was applied as an instrument. As a general result, there was a high and significant positive correlation of 0.706 between the variable Application of the Magerit methodology with the variable Security risk management of computer assets in MiBanco, Huaraz 2023. There was a moderate significant moderate correlation of 0.679 between the variable Application of the Magerit methodology with the dimension Hardware security risk management. There was a moderate and significant positive correlation of 0.660 between the variable Application of the Magerit methodology with the dimension Software security risk management. There was a significant high positive correlation of 0.735 between the variable Application of the Magerit methodology with the dimension Information Security Risk Management. In all cases the p value or significance or error value was 0.000, which indicated that the data did not correspond to a normal curve.

INTRODUCCIÓN

Con el propósito de conocer la relación entre la aplicación Metodología Magerit y la gestión de riesgos de seguridad del sistema de información en MiBanco, Huaraz 2023 se ha realizado un analisis de los antecedentes locales, nacionales e internacionales para que puedan ser analizados y discutidos con posterioridad en función a los resulatdos del presente estudio.

Contreras (2022) en la tesis de grado desarrollada en la Universidad Técnica de Babahoyo. Ecuador; se trazó el objetivo de elaborar el análisis comparativo entre las metodologías de Magerit y Octave. Aplicó las metodologías indicadas. Tuvo como resultado que la metodología más utilizada fue Magerit con un 37% y Octave con 16%. Encontró que Magerit cumplió desempeños bastante inetgarles enfocadas en la clase de análisis, metas de seguridad, clases de riesgos, componentes de la metodología e implantación, esto permite que esta metodología se comporte como robusta en el análisis y gestión de riesgos, por su parte, Octave no cumplió con los parámetros de importancia que puedan satisfacer el desarrollo institucional, a veces no demuestra confianza y atracción para algunas instituciones financieras que deseen implementarla para gestión de riesgos. También identificó las características, fortalezas y debilidades de las metodologías estudiadas, así como el alcance de la gestión de los riesgos. Concluyó que Magerit fue más completo que la metodología Octave en el desarrollo de los análisis relacioandos con riesgos.

Andrade (2021) en la tesis de grado desarrollada en una universidad colombiana a distancia, se planteó el objetivo de realizar aspectos analíticos conceptuales, de los elementos y técnicas enfocados en la gestión de riesgo de Pymes relacionadas a las telecomunicaciones usando MAGERIT V.3. Trabajaron estudio de tipo básico, aplicó diseño con descripción y con propuesta, población y muestra estuvieron conformados por archivos, documentos, ambos generados y procesados en la misma institución, utilizó entrevista, mientras que también aplicó a la entrevista, aplicó la metodología Magerit. Concluyó que después de la implantación de las tres iniciales etapas de la metodología Magerit existieron riesgos críticos, considerables,

estimables, también, los que estuvieron relacionados con Internet, determinaron que tuvieron que asegurar los activos informáticos con las salvaguardas sugeridas por Magerit. Encontró que los activos de información sobre Hardware se vieron afectados por diversos riesgos, se propusieron salvaguardas, que la mayoría de los riesgos requirieron control para que sean reducidos ya que estuvieron relacionados directamente con el negocio de la empresa y que estuvo ocasionando altos costos, encontraron que pocos riesgos fueron aceptados los cuales pudieron ser atendidos a costos bastante bajos. Concluyó que Magerit contribuyó positivamente en el estudio analítico y ejecución del tratamiento de riesgos dentro de institución mejorando los resulatdos.

Salazar (2020) en el artículo científico realizado en la Universidad Mayor de San Andrés, La Paz, Bolivia; se planteó el objetivo de proponer un modelo de Gestión de Riesgo en el Sistema de Seguridad Electrónica. Aplicó la norma ISO 31000: 2018, método hipotético deductivo, diseño experimental, aplicó las técnicas de encuestas, entrevistas, consultas, observación y análisis. La población muestral estuvo conformada por las entidades financieras de la ASOBAN. Tuvo como resultado final que se lograron identificar los riesgos existentes en el espacio estudiado respecto a seguridad electrónica, establecieron los juicios criteriales en los riesgos que correspondieron en la concesión de valores en el impacto y posibilidad de que ocurra en los activos de la infromación. Propuso un modelo analítico relacionados con los riesgos basado en el estándar internacional ISO 31000. Concluyó que el modelo propuesto en función a los riesgos pertinentes permitió el tratamiento de los riesgos minimizó significativamente a cada uno de los riesgos.

A nivel nacional, Gastelo y Rodríguez (2023) en la tesis de grado desarrollada en la Universidad señor de Sipán. Pimentel Perú, se plantearon el objetivo de realizar el perfeccionamiento de la gestión de riesgos cimentado en Magerit con fines de minimización de riesgos y uso de las tecnologías computacionales o informáticas. Trabajó investigación aplicada, de diseño correlacional, aplicó la metodologia

Magerit para asegurar la información, trabajó con una población de 115 empleados, como técnica aplicó análisis documental, y encuesta, como instrumento aplicó el cuestionario. Tuvo como resultado que Magerit contribuyó en la aplicación de un pertinente juicio de expertos con quienes estuvieron a cargo de los procesos del logro de gestión, permitió agilizar dichos procesos, ayudó en la identificación del factor que hacía diferencia dentro del área de las tecnologías informáticas dentro de institución, estos fueron la falta o escasez de desarrollo de software, enfoque estratégico relacionado con las tecnologías, así como también, la considerable dependencia con el Gobierno Regional y Central, también permitió el establecimiento de una guía ágil sobre el proceso. Que permitieron agilizar a la construcción del modelo de gestión, existió apoyo de las autoridades, lo cual garantizó el éxito de la implementación porque proporcionaron comprensión del proceso de manejo y adquisición de TI. Lograron inicialmente un valor promedio de riesgo, esto fue 363, mientras que con el plan de tratamiento y elección de salvaguardas se redujo a un promedio de valor de riesgo excedente de 175.49.

Linares, Balverdi y Cuellar (2022) en el artículo científico desarrollado en la. Universidad Peruana Unión, Perú, se trazaron el objetivo de realizar el diseño de un modelo de políticas de seguridad enfocados en la información cimentada en el estándar internacional ISO 27001:2013, así como también en la metodología Magerit con la finalidad de analizar los riesgos en la empresa objeto de estudio. Trabajaron investigación básica en el tipo, el diseño fue participativo y propositivo, la población y muestra fue conformada por toda la información institucional, emplearon como técnica a la entrevista y como instrumento a la guía de entrevista, utilizaron a Magerit como metodología. Tuvieron como resultados que la información que se debería de cuidar fuero los datos e información, servicios, software, equipos, comunicaciones, equipamiento auxiliar, instalaciones y personal. Tuvieron como amenazas a las de tipo natural, industrial, errores y fallos no intencionados y ataques mal intencionados. Con las políticas cimentadas en Magerit permitió el desarrollo de implantación en concordancia con las amenazas que pueden materializarse y perturbar a los activos de la empresa.

Collazos (2021) en la tesis realizada en la Universidad Nacional Pedro Ruiz Gallo, Perú; se planteó el objetivo de elaborar una metodología con el propósito de gestionar riesgos operativos de TI en el espacio estudiado. Trabajó investigación descriptivo propositivo, aplicó metodologia Magerit, enfoque combinado entre lo cualitativo y cuantitativo, mixto. Concluyó que implementó el modelo de gestión de riesgos en donde identificaron los activos de las tecnologías de la información y su respectiva priorización, también, identificó amenazas y vulnerabilidades, impacto de las amenazas, asimismo, determinó las posibilidades de que puedan ocurrir de cada una de las amenazas. La metodología permitió el establecimiento de pautas de evaluación de la magnitud de los riesgos, la identificación de los índices considerados como de importancia los cuales permitieron el control eficaz de los procesos de la gestión de riesgos con fines de controlar la seguridad de la información. También fueron tenidos en cuenta cada uno de los requisitos básicos correspondientes a la exigencia de la SBS a entidades financieras. Concluyó que implemento un dashboard para evaluar con efectividad a los componentes de caracterización y valoración de riesgos relacionados con el uso de las tecnologías de la información, así como, el cuidado de los riesgos en espacios intolerables. Los resultados demostraron que la aplicación de la metodologia Magerit fue bastante aceptable.

Fernández (2021) en la tesis de grado desarrollada en la Universidad Tecnológica del Perú. Lima Perú; se planteó el objetivo de realizar la implantación de la gestión de riesgos de las tecnologías de la información con propósitos de mejora de la seguridad de los activos de información en el objeto estudiado. Aplicó Magerit como metodología, Octave, Normas ISP 31000 y la norma ISO 27005. Trabajó investigación aplicada, de diseño correlacional de nivel no experimental, aplicó enfoque mixto, la población lo constituyeron 25 empleados y la muestra por 15 de ellos; aplicó a la encuesta como técnica y al cuestionario como instrumento. Tuvo como resultado que la aplicación de la metodología Magerit mejoró la seguridad de la información, se tuvo correlación de Pearson positiva de 0.970. Lograron

establecer a los activos correspondientes relacionados con la información y la evaluación de cada uno de ellos mediante Magerit, se obtuvo correlación de 0.982, es decir, la implantación de la gestión de riesgos de TI permitió mejorar el establecimiento de los activos de información. Los riesgos para los activos fueron valorados mediante la metodología Magerit, en este caso, la correlación de Pearson fue positiva de 0.971, lo cual permitió concluir que la aplicación gestión de riesgos de TI mejoró de manera significativa el grado de protección de información. Lograron instituir procesos de planificación con actividades y controles exigentes con el propósito de minimizar los riesgos presentes, la correlación de positiva fue de 0.683, lo cual permitió concluir que la aplicación gestión de riesgos de TI minimizó de manera significativa los riesgos de seguridad de información en el objeto estudiado.

Santa María (2020) en la tesis de grado realizada en la Universidad de Lambayeque, Chiclayo Perú; se planteó el objetivo de desarrollar una propuesta de un plan basado en Magerit como método con el propósito de menguar cada uno de los riesgos operativos que se pueden presentar durante el uso o aplicación de tecnologías de la informática y las comunicaciones. Aplicó metodología Magerit, la investigación fue descriptiva, propositivo, la población y los elementos de la muestra estuvieron conformadas por la jefatura TI, seguridad TI y unidad de riesgos; aplicó encuesta y cuestionario. Tuvo como resultado que se encontraron 55 riesgos operativos específicamente relacionados con la aplicación de las tecnologías de información, estos fueron agrupados en 10 tipos de activo: datos comunicaciones, equipos informáticos, documentos, personal, información, equipo auxiliar y servicios. Implementaron la propuesta establecida para el estudio consistente en el modelo de gestión de riesgos, estos, fueron: identificación de los activos de Tecnologías de Información, lista de activos, vulnerabilidades y amenazas, impacto en caso de amenaza y probabilidades de que ocurra la amenaza. El modelo del estudio fue diseñado en dos fases, estos fueron, procesos en donde se establecieron y evaluaron los riesgos consistentes o derivados del uso de las tecnologías de la información y el procedimiento de los riesgos ubicados fuera de los rangos de tolerancia. El plan

de reducción de riesgos tecnológicos que exponen a los activos de la información fue aceptado por los responsables conocedores de gestión de los riesgos operativos respecto a la aplicación de las Tecnologías informáticas, los responsables aceptaron la propuesta en un 93%.

Cabrejos (2020) en la tesis de grado realizada en la Universidad señor de Sipán, Pimentel Perú, se planteó el objetivo de realizar la determinación de la influencia de la Metodología Magerit V3 en los aspectos de seguridad informática. Trabajó investigación aplicada, de diseño correlacional, aplicó la metodologia Magerit para asegurar la información, trabajó con una población de 115 empleados, como técnica aplicó análisis documental, y encuesta, como instrumento aplicó el cuestionario. Tuvo como resultado que existió correlación directa positiva con 78% entre la aplicación de la Metodología Magerit V3 con la variable Seguridad de la información, se encontró influencia de 70.6% entre Magerit V3 y la Seguridad infromática institucional; asimismo encontró falta de capacitación del personal respecto a seguridad y defensa de los activos informáticos. Concluyó que la metodología aplicada en el estudio sirvió contundentemente en los procesos del análisis de cada uno de los riesgos, en la, determinación de las amenazas, personalización de las salvaguardas y contribuyó en la implementación de futuras salvaguardas relacionados con el control y mitigación de riesgos. Que fue necesario ejecutar un plan de gestión y tratamiento de riesgos con fines de minimización de riesgos y establecimiento de estrategias para reducción de vulnerabilidades y amenazas hacia los registros de información.

Los fundamentos teóricos de la metodologia Magerit son muy importantes cuando se desea gestionar los riesgos de seguridad de la información en todas las empresas de cualquier tipo a nivel Internacional Siempre están expuestos a Riesgos de diferentes tipos, con el avance de la tecnología, estos riesgos se han incrementado significativamente, para enfrentar el problema de los riesgos, muchas instituciones internacionales han creado diversas metodologías para enfrentar a los riesgos, una

de estas es la metodología Magerit, la cual se usa como un método básico para gestionar diversos tipos de riesgos informáticos, se encuentra basada en la norma ISO/CEI 27001, la misma que es bastante fácil y rápido de usar, y de aplicar, contribuye adecuadamente en la entrega de resultados positivos sobre el conocimiento del estado del riesgo, se puede tomar como un apoyo fundamental en el momento de toma de decisiones cuando se desea mejorar la seguridad del Sistema de información de una determinada compañía pública o privada (Fernández y García, 2016).

Esta metodología de gestión de riesgos, denominada Magerit, tiene en cuenta los aspectos cualitativos de los activos del Sistema de información, entre ellos, valora los aspectos de la integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad, Para esta valoración esta metodología. Utiliza la escala de valoración considerado como: muy alto., Alto, Medio, Bajo, Muy bajo y despreciable (Amutio et al, 2014; España, 2012). Esta metodología trata de comprobar el impacto que se puede establecer entre los valores de los activos y busca establecer el valor de estos activos, los valores en este caso, se obtiene mediante el valor del activo multiplicado por la amenaza que tiene que enfrentar, y este problema o afectación es tomada del propio riesgo y las amenazas (Brunner et al, 202; Amutio et al, 2012).

Magerit como herramienta de gestión de riesgos específicamente en aplicación de tecnologías de la información, contribuye o facilita la evaluación de riesgos en lo siguiente (Mirtsch et al, 2021; Motaki, 2016):

Identificación de riesgos: Magerit con la identificación de los activos informáticos, así como los tipos de relaciones que puedan existir entre ellos, también identifica la valoración de la empresa para conocer la importancia de los activos con las que se va a trabajar, ayuda en la caracterización de las amenazas, así como, en la estimación de cada uno de los riesgos a la que está expuesta cada una de las unidades que conforman la institución (Taubenberger, 2014; Costas Santos, 2014).

La metodología Magerit requiere de un conjunto de datos cualitativos o cuantitativos para determinar los activos que están siendo expuestos a amenazas, los costos que van a ser impactados, los datos cualitativos pueden ser convertidos en cuantitativos, esta metodología también calcula el nivel de riesgo que se fundamenta en parámetros muy importantes, estos son, el espacio o escenario de la amenaza, al posibilidad y consistencia de la ocurrencia del riesgo, qué tiene característica multidimensional, que pueden ser medidos mediante escalas categóricas (Hurtado, 2018; Medina, 2007).

Resumiendo, la metodología Magerit contribuye en la en el análisis, identificación y evaluación de las alternativas que se propone en función a la cantidad de reducción de amenazas o riesgos, el riesgo se cuantifica teniendo en cuenta el impacto sobre las cantidades perdidas, y que se expresan en costos en determinadas unidades monetarias. El análisis de riesgos tiene como resultado un conjunto de valores que expresan diversos componentes y cantidades que deben ser evaluados y valorados, así como también, tenidos en cuenta para la evaluación del riesgo (Motaki, 2016).

MAGERIT como metodología estudia los riesgos que suelen ocurrir de manera estocástica en los sistemas de información, reforzados inclusos por las vulnerabilidades de la misma organización, en ese sentido, Magerit define al riesgo como un valor probabilístico de ocurrencia de daños o perjuicios, para ello, establece un conjunto de guías, orientaciones y recomendaciones pertinentes que toda institución que use un sistema de información debería adoptarla con el propósito de para controlar los riesgos que se puedan presentar (España, 2012). De acuerdo con MAGERIT, las actividades o procesos de realizar los análisis, tratamientos y control de los riesgos, no necesariamente constituyen un fin institucional, sino que son muy necesarias y garantizan la sostenibilidad de la institución en términos de seguridad. La ejecución del análisis de riesgos conlleva a la determinación de sus características principales y básicas, identificar los aspectos valorativos y el nivel de protección del sistema de información (Chicano,

2014). Teniendo en cuenta los objetivos, estrategia y políticas institucionales, el tratamiento de los riesgos conllevan a la producción de un plan de seguridad para las instalaciones del sistema informático, que debe ser implementado y ejecutado, que permita el cumplimiento de los objetivos planificados y acordados en función al nivel de riesgo determinado y cuantificado por la administración (Figueira et al, 2020).

La metodología MAGERIT estima dos grandes trabajos a ejecutar, estos son el examen de los riesgos y su respectiva atención del riesgo. En el análisis, MAGERIT sostiene que se debe de establecer que elementos informáticos dispone la organización y que les podría pasar en función a la probabilidad de la ocurrencia de un riesgo. Respecto al tratamiento de los riesgos, MAGERIT afirma que se debe planificar, organizar y controlar un nivel de defensa con un determinado nivel de capacidad en la defensa para garantizar la seguridad de los activos informáticos, que el impacto sea lo más mínimo en función a costos e imagen institucional, la capacidad de hacer frente a las amenazas debe permitir sobrevivir a cualquier tipo de incidentes, y que permita a la institución garantizar la sostenibilidad de la operatividad en cantidad y calidad de operatividad; no obstante, se debe tener en cuenta que las amenazas y los riesgos no se pueden eliminar y que siempre van a estar presentes, esto significa que no hay seguridad al cien por ciento (Altamirano, 2019; Calder & Watkins, 2008).

En función a los riesgos que se puedan generar dentro de un sistema de información, MAGERIT recomienda el desarrollo de las siguientes actividades: establecer o identificar la cantidad de activos, los tipos de activos considerados como importantes institucionalmente; identificar a las amenazas a los que pudieran estar expuestos los activos identificados. Establecer la disponibilidad de salvaguardas eficientes y eficaces existentes en la institución y con la capacidad de hacer frente a los riesgos. Evaluar y cuantificar el impacto, perjuicio o daño hacia los bienes o activos informáticos provenientes de la situación de riesgos y amenazas. Cuantificar el riesgo en función a la frecuencia o tasa de ocurrencia de los riesgos o la amenaza (Figueira et al, 2020; Mercado, 2016)

Se debe entender que los activos informáticos de valor cuantificable para toda institución están expuestos a amenazas, que las amenazas causan un determinado nivel de degradación y que este nivel de degradación genera impacto, generalmente negativo en el valor del activo. La ocurrencia de las amenazas tiene una cierta probabilidad de ocurrencia, a este nivel de probabilidad de ocurrencia es lo que se conoce como riesgo, si el riesgo es alto, el riesgo es potencial (Baca, 2016; Joyanes, 2015).

Apetito y tolerancia al riesgo. Dentro de la ciencia informática, el apetito es denominado apetito de riesgo es un grado de riesgo al nivel de riesgo que una determinada institución que utiliza un sistema de información está dispuesta a aceptarla, es el nivel de riesgo con el que dicha empresa no se siente amenazado si no se siente cómoda. Este apetito de riesgo está en función de la capacidad de la empresa en enfrentar y asumir determinado nivel de riesgos informáticos, este nivel va a ser siempre aquel nivel que la institución pueda enfrentar exitosamente sin que afecte significativamente el logro de sus metas y objetivos institucionales (Morán, 2019). El apetito de riesgo también es conceptuado como la cantidad de riesgo que una institución está preparada para aceptarla en función a su capacidad de tolerancia al riesgo, que implica el límite de aceptación de riesgos; capacidad de riesgo lo cual se entiende como la capacidad de sobrellevar los riesgos, así como también, la conducta adecuada de gestión de riesgos (Crespo, 2016).

MAGERIT estudia los riesgos a los que está sujeto de ocurrencia cualquier tipo de sistema de información constituido por hardware, software, sistema de red y los usuarios denominados manware, los riesgos, en este caso, tienen la capacidad de afectar las funcionalidades del sistema y las dimensiones de los activos de información, es una metodología que guía, orienta y recomienda desarrollar diversos tipos e medidas de forma planificada, organizada, controlada, sistemática y secuencial que deben de realizarse con el propósito de desarrollar las

prevenciones, no permitir los ataques, reducir ataques, costos, demoras, etc.; así como también controlar todo tipo de riesgos informáticos (Amutio et al, 2014).

Objetivos de MAGERIT: Esta metodología tiene como objetivos hacer más fácil el desarrollo de las actividades de los usuarios de los sistemas de información, alcanza, guía y organización sobre los elementos estándar, los cuales pueden ser obtenidos en Internet, Magerit se centra específicamente en el análisis de los objetos están sujetos a riesgos dentro de un sistema de información. También tiene como objetivo desarrollar resultados homogéneos de los análisis realizados, promueve el uso de tecnologías y criterios bastante uniformes y centrados que conllevan a la comparación e integración de estudios elaborados por distintos equipos de trabajo (Hurtado, 2018; Shameli-Sendi, 2016).

Esta metodología considera dos tareas importantes a realizar en la gestión de riesgos de la seguridad de la información, estos son los análisis de riesgos, los cuales van a permitir la determinación de los problemas o el estado situacional de la institución, así como también cuantificar o pronosticar lo que podría pasar en el corto plazo. La segunda tarea consiste en el tratamiento de los riesgos, para desarrollar el tratamiento se tiene que organizar la defensa de forma razonada y prudente, para evitar impactos. Bastante fuertes y negativos, esta metodología sostiene que se tiene que estar preparado para enfrentar las emergencias y poder sobrevivir a los incidentes que pudieran ocurrir, con la finalidad de garantizar el trabajo de los usuarios en las mejores condiciones, sabiendo aún que los riesgos no se pueden eliminar en su totalidad (Hurtado, 2018; Amutio et al, 2014).

Desarrollo de la metodología Magerit, El desarrollo de esta metodología se enfoca principalmente en el análisis y en el tratamiento de los riesgos y, por lo tanto, se deben cumplir las siguientes fases (Hurtado, 2018; Amutio et al, 2014):

Fase 1. Determinación del contexto, consiste en identificar los activos que se van a analizar en función a los análisis de riesgo, este contexto puede ser por

unidades o áreas, o también por ubicación del sistema informático conformado por los clientes y servidores, siempre en cuando sean considerados como puntos estratégicos en donde se va a desarrollar el proceso de mejora de la seguridad informática. En este caso, se desarrolla la identificación de los parámetros que van a permitir el desarrollo de políticas en función a la gestión de riesgos se tiene que considerar el alcance del análisis, las relaciones entre áreas, esto indica el flujo de información que comparten áreas dentro de la institución (Rodríguez & Peralta, 2019).

Fase 2. Identifica los activos, en esta fase en Magerit sugiere que se deben establecer los activos de mayor consideración o importancia para la organización y que se deben ser separados por grupos, de tal forma que cada uno de ellos puedan ser analizados con el propósito de conocer sus debilidades en función a los riesgos y amenazas a las cuales puedan estar expuestas (Rodríguez & Peralta, 2019; España, 2012).

Fase 3. Identifica las amenazas, consiste en identificar a qué tipo de amenazas están expuestos los activos más importantes de la institución, es decir, las computadoras, impresoras, sistemas de red, activos de información en función a integridad, confidencialidad y disponibilidad, así como también, conocer los tipos de factores que puedan tener la capacidad de afectar negativamente la información hasta generar niveles de vulnerabilidad. Con la identificación de las amenazas también se puede conocer la capacidad que se dispone para enfrentar a las amenazas y riesgos (Hurtado, 2018; Amutio et al, 2014).

Fase 4. Identifica salvaguardas, con la identificación de las amenazas se está en la condición de identificar de qué salvaguardas dispone la institución y si son efectivas para enfrentar el nivel de riesgo y amenazas en la que se encuentra el sistema de información. Las salvaguardas son los sistemas de seguridad antivirus, manual de buenas prácticas de uso del sistema de información, etc. (Hurtado, 2018; Amutio et al, 2014).

Fase 5. Valoración del riesgo, esta metodología señala que en esta fase se debe valorar el impacto qué puede tener la amenaza en función a los valores de los activos, también se debe valorar la capacidad con que se ha enfrentado a los riesgos, la inyección de fortalezas y debilidades o deficiencias en los sistemas. La institución debe conocer que el riesgo puede presentarse de forma interna o intrínseca, lo cual significa que existe una probabilidad de que la amenaza se materialice o concretice. Asimismo, también se puede presentar de forma residual, es decir, después de la aplicación de los controles, o de forma efectiva cuando se ha generado un impacto negativo en el sistema que se está protegiendo. En ese sentido, valorar los riesgos puede implicar el uso una escala con niveles bajo, medio, alto y extremo, todo ello según el efecto de la amenaza (Hurtado, 2018; Amutio et al, 2014).

Fase 6. Mitigación del riesgo, en esta fase, la metodología Magerit recomienda que se evalúe el impacto que ha generado el riesgo teniendo en cuenta su probabilidad de ocurrencia hacia la parte afectada, en este caso se facilita la toma de decisiones sobre el tratamiento y reducción de los riesgos (Rodríguez & Peralta, 2019; España, 2012).

Después de la determinación del nivel de influencia y los distintos tipos de riesgos a los que se tiene que enfrentar un sistema de información de una determinada organización, la administración debe tomar un conjunto de decisiones en función a los siguientes aspectos: **La severidad del impacto.** El primer aspecto consiste en determinar la severidad del impacto. Generalmente el impacto es negativo, implica costos, demoras, pérdidas de imagen, Que en general implica obligaciones para la institución que debe cumplir si se desea tener la seguridad de la información en niveles aceptables. La determinación de la severidad consiste en establecer por cada equipo seleccionado, estos deben presentar un determinado nivel de severidad, el cual puede ser, leve, moderado y severo (Hurtado, 2018).

Indicadores de riesgos. Los indicadores de riesgo son métricas que sirven para cuantificar el nivel de probabilidad de que se materialice un riesgo, asociada o combinada a las consecuencias, y que supere el nivel de riesgo aceptable denominado apetito de riesgo, los indicadores de riesgo determinan el nivel de impacto que generalmente es negativo en la posibilidad de tener éxito frente a los riesgos por parte de la institución. Un indicador de riesgo para un sistema financiero lo constituye el número de ataques que no han podido ser advertidos, cantidad de computadoras atacadas, cantidad de documentación cuya dimensión integridad ha sido variada, etc. En este caso, el incremento del indicador de riesgo constituye un indicador de que se tiene que resolver el problema lo más antes posible (Berrio, 2016; Molina, 2015).

Las instituciones financieras como es la empresa Mibanco, debido a que manejan información bastante confidencial, muy susceptible y de alta importancia, así como de altos niveles de confidencialidad, deben establecer indicadores críticos de riesgo con la finalidad de asegurar y garantizar a que todos su activos de información y comunicación, y lo activos de información no se encuentre dentro de la zona de alto riesgo, debido a que ello podría generar pérdidas incalculables para la institución financiera, lo cual puede impedir a que se cumplas las metas y objetivos institucionales. Para el análisis, control de la seguridad, se deben crear una cantidad de indicadores de riesgo y que puedan ser medidos con bastante precisión, además de reflejar el nivel del impacto generalmente con consecuencias negativas (Llontop, 2018; Molina, 2017).

Gestión de Riesgos de seguridad. Las instituciones financieras son las empresas a nivel mundial que están más sujetas a ataques informáticos desde cualquier parte del mundo debido a que manejan gran cantidad de dinero, en ese sentido, los atacantes siempre buscan hacerse de esos dineros, y es por ello que vulneran los sistemas de seguridad de las instituciones financieras, debido a que este tipo de instituciones siempre buscan gestionar los riesgos de su sistema de información, se fundamenta en la formación de una disciplina constante en el

manejo de los peligros, riesgos y vulnerabilidades; en este caso se debe tener en cuenta que tan solo en la asignación de todos los recursos para gestionar los riesgos constituye un costo considerable a la empresa que se suma a los casos de seguridad de la información (Rodríguez & Peralta, 2019).

Elementos de riesgo. Las empresas financieras tienen como activos de información a las oficinas en donde se atienden a los clientes de créditos y a los clientes de ahorros. En ambos casos, los elementos de riesgo son los siguientes: Computadoras de escritorio, laptops, tablets, Celulares, impresoras, fotocopiadoras, escáner, servidores, sistema de huella dactilar, personal a cargo del sistema de información, entre otros recursos que también pueden considerarse como importantes son las instalaciones en donde se atiende a los diverso clientes de la institución financiera (Brunner et al, 2020; ISACA, 2009).

Amenazas: Las amenazas que se puedan dar en los activos de los sistemas financieros pueden ser causado por accidentes físicos, accidentes mecánicos, accidentes generados por el medio ambiente, accidentes generados por el hombre. La amenaza es una debilidad de un determinado activo, y como tal, puede ser aprovechado por un atacante interno o externo generando impacto negativo y pérdida de imagen a la institución. Por su parte, los peligros se clasifican en varias clases, lo cual puede ser de manera originaria, deficiencias en losa aspectos de uso o aplicación, puede ser generado por el medio ambiente, por actividades del hombre, por ataques internos y externos, etc. (Molina, 2015).

Vulnerabilidades: En todo sistema de información, y mucho más en los sistemas de una empresa dedicada a las finanzas, no deberían presentar vulnerabilidades porque se supone que, tanto el sistema como los usuarios, están bien implementados, pero en la realidad sucede que siempre existen vulnerabilidades en determinados niveles, los cuales pueden generar riesgos que se incrementan, y que el sistema puede ser atacado, generando impactos negativos significativos (Crespo, 2016). Los elementos o recursos de un sistema financiero

pueden presentar vulnerabilidades en cuanto al personal, la falta de dominio de uso adecuado de los sistemas de información constituye una vulnerabilidad preocupante, no disponer de un sistema antivirus que pueda proteger. Al sistema de diversos ataques informáticos también se tiene en cuenta como vulnerabilidad, etc.

Impacto: Los riesgos y vulnerabilidades generan un impacto generalmente negativo en los activos informática, así como también en la parte económica de la institución, cada riesgo invulnerabilidad tiene un determinado nivel de impacto, es por ello que este indicador es medido y cuantificado con la finalidad de conocer su influencia en la variable que se desee relacionarlo (Molina, 2015).

Activos informáticos. Los activos informáticos de una institución financiera son todos aquellos activos que conforman un sistema de información y que es utilizado por la institución financiera para el desarrollo operativo y administrativo de sus funciones como sistema, los elementos que contiene un sistema de información, estos son, hardware, software, y el personal qué utiliza el sistema de información, por tanto, un activo importante con referencia al usuario, es la comprensión que dispone cada uno de ellos con relación a la seguridad informática.

Dimensiones de la gestión de riesgos. Con la aplicación de Magerit, las dimensiones de gestión de riesgos son los siguientes: Análisis de riesgos y tratamiento de los riesgos. **Análisis de riesgos,** para esta dimensión se va a tener como indicadores a las tres primeras fases de la aplicación de Magerit, estos son: determinación del contexto, identificación de los activos y la identificación de las amenazas. La segunda dimensión tratamiento de los riesgos, los indicadores van a estar constituidos por la caracterización de las salvaguardas, la valoración del riesgo y la mitigación del riesgo (Hurtado, 2018).

Dimensiones de los activos informáticos. Para propósitos de la presente investigación, y teniendo en cuenta a la literatura científica que corresponde a la seguridad de la información, se ha creído por conveniente, tomar las dimensiones

de **software**, dimensión que contiene a los indicadores: Riesgos de sistema operativo, riesgos de software de aplicaciones, riesgos en software de seguridad y riesgos en software de gestión financiera. Dimensión **Hardware** que contiene a los indicadores amenazas, ataques repelidos e incidentes, y por último a la dimensión **Información,** dimensión que contiene a los riegos que afectan a las características del software relacionados con la Integridad, confidencialidad y disponibilidad (Baca, 2016).

Mibanco: Es el espacio empresarial financiero en donde se va a desarrollar la presente investigación, tienen como giro del negocio capotar masa monetaria de la población en forma de ahorros y prestar estos dineros a la misma población en forma de créditos..

La presente investigación es justificada en el plano social debido a que se hace necesario conocer la determinación de la relación entre la variable metodología Magerit con la gestión de riesgos de seguridad del Sistema de Información de la empresa financiera MiBanco de la ciudad de Huaraz, para que con este conocimiento se puedan tomar las decisiones oportunas respecto al sistema de información, con este conocimiento se van a beneficiar a los usuarios de la empresa financiera, sus trabajadores y la empresa en su conjunto.

Así mismo, esta investigación se justifica en el plano económico porque con los valores de las relaciones obtenidas entre las variables de estudio, se van a poder tomar decisiones que van a poder reducir. Los riesgos de seguridad del Sistema de información, con la cual se van a evitar costos de pérdidas de tiempo, costo de parada de las computadoras, costos de pérdidas de información, entre otros costos que son inherentes al uso de los sistemas de información.

Este estudio se justifica teóricamente debido a que se fundamenta en el plano teórico en los principios fundamentales de la seguridad de la información, en la teoría de la gestión de riesgos de seguridad de los sistemas de información, así como

también los conocimientos contextualizados del uso del sistema de información en un sistema financiero.

Este estudio también se justifica desde la perspectiva metodológica porque los usuarios del sistema de información de la empresa financiera van a conocer los métodos de la metodología MARGERIT para que puedan aplicarla en los análisis de riesgos y sus respectivos tratamientos mediante la aplicación de las seis fases establecidas por esta metodología.

La presente investigación es importante porque se propone determinar las relaciones entre las variables Metodologia Magerit con la variable gestión de riesgos de seguridad del sistema de información de la institución financiera MiBanco de la ciudad de Huaraz con la finalidad de que posteriormente las autoridades administrativas puedan tomar las decisiones pertinentes en función de los valores de la correlación de las variables.

A nivel internacional, los sistemas financieros manejan gran cantidad de información muy sensible, así como también, utilizan alta tecnología relacionado con el mundo de la informática cuyos elementos están dispuestos a amenazas y riesgos constantemente, son los sistemas bancarios los que sufren estos tipos de riesgos en todo el planeta, los sistemas financieros son los que más pierden económicamente como resultados de los problemas de la seguridad informática debido a riesgos y amenazas informáticas, el año 2022, las pérdidas que han sufrido el sistema financiero por seguridad de información supera los 15000 millones de dólares solo en Europa y Norteamérica. (Brunner et al, 2020). Como consecuencia de estos problemas, los sistemas financieros han adoptado diversas metodologías que permiten analizar y tratar adecuadamente los riesgos, así como también instituciones internacionales, han creado diversas normas y políticas para poder contribuir con la seguridad de los sistemas de información (Mirtsch et al, 2021).

A nivel nacional se tiene un conjunto de sistemas financieros clasificados como gran empresa, mediana y pequeña empresa, todos estos sistemas financieros están

actualizados con las altas tecnologías de la comunicación para desarrollar los procesos operativos y administrativos de las funciones que realiza, no obstante, no están libres de los riesgos y amenazas que conlleva el uso de estas tecnologías. Se observa en la literatura científica que estas empresas han utilizado diversos tipos de metodologías para poder analizar y tratar los riesgos, así como también, han determinado las relaciones entre las variables de la aplicación de esta metodología con los riesgos encontrados, los resultados encontrados les ha permitido tomar decisiones oportunas con resultados considerablemente positivos (Contreras, 2022).

A nivel local, la empresa MiBanco de la ciudad de Huaraz, es una empresa financiera que se encuentra entre la gran banca y las cajas municipales, es una mediana empresa que pertenece al Grupo Credicorp. Tiene como giro del negocio prestar créditos a diversos sectores de la sociedad, así como también capta dinero mediante su sistema de ahorros en diversas formas. Para el otorgamiento del servicio a la comunidad, esta empresa dispone de un sistema informático distribuido entre todas sus unidades, se observa que actualmente la empresa está aplicando la metodología Magerit con el objetivo de analizar y dar tratamiento a los riesgos y amenazas a su sistema de información. Todos estos procesos están a cargo del personal dedicado a la gestión de riesgos de la seguridad de la información. El problema fundamental que aborda el presente estudio consiste en que se desconoce las relaciones entre ambas variables, que, de no conocerse en el corto plazo, no se podrían tomar las acciones correctivas, lo cual, podría generar costos muy significativos a la institución.

Ante esta realidad problemática, se plantea determinar la correlación entre las variables aplicación de Magerit con la variable gestión de riesgos de seguridad del sistema de información de la empresa financiera MiBanco de la ciudad de Huaraz, así como también, determinar las relaciones que podrían existir en la variable Metodologia Magerit con las dimensiones de la variable gestión de riesgos de seguridad del sistema informático de la empresa financiera. La formulación del

problema consiste en ¿En qué medida se relaciona la aplicación de la metodología Magerit con la Gestión de riesgos de seguridad del sistema de información en MiBanco, Huaraz 2023?. Como problemas específicos se ha considerado: ¿En qué medida se relaciona la aplicación de la metodología Magerit con la Gestión de riesgos de seguridad de hardware en MiBanco, Huaraz 2023? ¿En qué medida se relaciona la aplicación de la metodología Magerit con la Gestión de riesgos de seguridad de software en MiBanco, Huaraz 2023? ¿En qué medida se relaciona la aplicación de la metodología Magerit con la Gestión de riesgos de seguridad de información en MiBanco, Huaraz 2023?

A fin de lograr el objetivo del estudio, es muy imporatnte ejecutar un plan estratégico de seguridad de la información en donde se definan las acciones a tomar para gestionar el riesgo a las que esta expuesto el hardware, software e información, en general, la seguridad de la información, con el propósito de evitar los riesgos de tipo informático. Teniendo en cuenta ello, se conceptualizan y operacionalizan las variables en estudio.

Metodología Magerit: Se definen como políticas, normas y estándares que se enfocan el control realizado con el propósito de asegurar la seguridad de los activos informáticos de un determinado tipo de organización, esta metodologia tienen en cuenta la seguridad de la información y se fundamenta en los princioios de seguridad inetrnacioanles y casados en experiencias de instituciones mundiales, contribuye con alcanzar un nivel de protección de todo el sistema de información o parte de ella, tales como los activos informáticos, tambien se conceptua como que asigna y garantiza protección a hardware y software frente a ataques internos y externos con la finalidad de hacer daño al sistema (CISCO, 2018).

Gestión de riesgos. Es la identificacion, analisis y la realziacion de determianads respuestas a los riesgos potenciales que puedan afectar a un sistema de información, es decir a, software, hardware y la inforamcion ques e genera con esta tecnologia y de esta manera evitar posibles ataques informáticos internos y

externos (Hurtado, 2018)**.** Los activos informáticos están constituidos por todos los elementos que contiene un sistema de información, estos son, hardware, software, y la informacion que son generados dentro de la instiución, por lo tanto, los activos informáticos demuestran considerable importancia para la empresa y el usuario.

Dimensiones de la Metodología Magerit. en el estudio se tomaron las dimensiones de **Analisis de seguridad.** dimensión que tiene como indicadores al Hardware, software y la inforemacion generada en la institucion financiera, los cuales estan sujetos a riesgos inetrnos y externos. **Tratamiento de la seguridad.** esta dimensión contiene a los siguientes indicadores: tratamiento de la seguridad de lso activos de hardware, softwaue y activosd e infroamcion del la institucion fiannciera (Amutio et al, 2014).

Dimensiones de la Riesgos de seguridad del sistema de información. Para propósitos de este estudio, se ha tomado las dimensiones: **Software**. dimensión que contiene a los activos propios de la institucion, tales como sistema operativos, bases de datos, aplicaciones financieras, los cualesfieron analziados en funcion a su integridad, confidencialidad y disponibilidad. **Hardware** que contiene a los activos informáticos, tales como servidores, computadoras clientes, sistema de red fisico, etc., en funcion los riesgos a las que estan sometidos, **Información,** que contiene a los archivos informáticos que se generan, reciben y distribuyen en la empresa financiera y que estan bajo riesgos internos y externos (Mercado, 2016).

Tabla 1
Operacionalizacion de la variable

Variable	Dimensión	Ítems
Aplicación de la Metodología Magerit	Análisis de seguridad	Calificación de la determinación del contexto en el área de ahorros con la aplicación de la metodología Magerit en MiBanco Huaraz 2023
		Consideración de la determinación del contexto en el área de créditos con la aplicación de Magerit en MiBanco Huaraz 2023
		Evaluación de la determinación del contexto en el área de plataforma con la aplicación de Magerit en MiBanco Huaraz 2023

		Valoración de la identificación de hardware con la aplicación de la metodología Magerit en MiBanco Huaraz 2023
		Califica la identificación de software con la aplicación de la metodología Magerit en MiBanco Huaraz 2023
		Consideración de la identificación de la información con la aplicación de Magerit en MiBanco Huaraz 2023
		Calificación de la identificación de amenazas al hardware con la aplicación de Magerit en MiBanco Huaraz 2023
		Consideración de la identificación de amenazas al software con la aplicación de la metodología Magerit en MiBanco Huaraz 2023
		Evaluacion de la identificación de amenazas a la información con la aplicación de Magerit en MiBanco Huaraz 2023
	Tratamiento de la seguridad	Calificación del tratamiento de la seguridad del sistema operativo en MiBanco Huaraz 2023
		Consideración el tratamiento de la seguridad del software antivirus en MiBanco Huaraz 2023
		Evaluación del tratamiento de la seguridad de software financiero en MiBanco Huaraz 2023
		Valoración del tratamiento de la seguridad de la información en MiBanco Huaraz 2023
		Calificación del tratamiento de la seguridad de las computadoras clientes en MiBanco Huaraz 2023
		Consideración del tratamiento de la seguridad del servidor en MiBanco Huaraz 2023
		Evaluación del tratamiento de la seguridad de hardware de conectividad de Internet en MiBanco Huaraz 2023
Riesgos de seguridad del sistema de información	Hardware	Calificación de la gestión de riesgo de seguridad del servidor en MiBanco Huaraz 2023
		Calificación de la gestión de riesgo de seguridad de las computadoras en MiBanco Huaraz 2023
		Calificación de la gestión de riesgo de seguridad del hardware de conectividad de Internet en MiBanco Huaraz 2023
		Calificación de la gestión de riesgo de seguridad de impresoras en MiBanco Huaraz 2023
	Software	Consideración del tratamiento de la seguridad del sistema operativo en MiBanco Huaraz 2023
		Consideración del tratamiento de la seguridad del software antivirus en MiBanco Huaraz 2023
		Consideración del tratamiento de la seguridad del software financiero en MiBanco Huaraz 2023
		Consideración del tratamiento de la seguridad del software de oficina en MiBanco Huaraz 2023
	Información	Consideración del tratamiento de la seguridad de la información financiera de importancia en el área de ahorros en MiBanco Huaraz 2023

		Consideración del tratamiento de la seguridad de la información financiera de importancia en el área de créditos en MiBanco Huaraz 2023
		Consideración del tratamiento de la seguridad de la base de datos en MiBanco Huaraz 2023
		Consideración del tratamiento de la seguridad del acceso a Internet en MiBanco Huaraz 2023
		Consideración del tratamiento de la seguridad del acceso a las redes sociales en MiBanco Huaraz 2023
		Consideración del tratamiento de la seguridad del acceso a correos electrónicos en MiBanco Huaraz 2023

En la investigación se plantea como hipótesis: La aplicación de la metodología Magerit se relaciona positivamente con la Gestión de riesgos de seguridad de hardware en MiBanco, Huaraz 2023. Como hipótesis específicas se plantean: La aplicación de la metodología Magerit se relaciona positivamente con la Gestión de riesgos de seguridad de hardware en MiBanco, Huaraz 2023. La aplicación de la metodología Magerit se relaciona positivamente con la Gestión de riesgos de seguridad de software en MiBanco, Huaraz 2023.La aplicación de la metodología Magerit se relaciona positivamente con la Gestión de riesgos de seguridad de información en MiBanco, Huaraz 2023

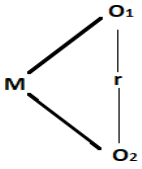
Asimismo, se formuló el objetivo general: Determinar la relación entre de la aplicación de la metodología Magerit con la Gestión de riesgos de seguridad del sistema de información en MiBanco, Huaraz 2023. Así mismo. Los objetivos específicos:

- Determinar la relación de la aplicación de la metodología Magerit con la Gestión de riesgos de seguridad de hardware en MiBanco, Huaraz 2023.
- Establecer la relación de la aplicación de la metodología Magerit con la Gestión de riesgos de seguridad de software en MiBanco, Huaraz 2023.
- Determinar la relación de la aplicación de la metodología Magerit con la Gestión de riesgos de seguridad de información en MiBanco, Huaraz 2023.

METODOLOGÍA

Para este estudio, el tipo de investigación con se trabajó fues no experimental, lo cual significó que no se tuvo que manipular a ninguna variable, ni a la metodología Magerit con el propósito de mejorar a la variable gestión de riesgos. Debido a la captación de datos, el tipo de investigación fue de corte transversal solamente se tuvo que medir a las variables por única vez durante la duración de la investigación. El enfoque aplicado fue del tipo de tipo mixto, esto significó que se trabajó con variables cuantitativa y cualitativa (Hernández, Fernández y Baptista, 2010).

El diseño del presente estudio fue de tipo descriptivo correlacional, esto significó que se tuvo que determinar la correlación entre las variables Metodologia Magerit y la variable gestión de riesgos del sistema de información y las correlaciones entre la aplicación de la metodologia Magerit y las dimensiones de la variable gestión de riesgos de seguridad del sistema de información de la empresa financiera MiBanco (Bernal, 2010; Valarino, 2010). El esquema de diseño fue:



Dónde:

M = Sistema informático de la empresa financiera MiBanco de la ciudad de Huaraz

O1 = Observación de la aplicación de la metodología Magerit

O2 = Observación de la variable Gestión de riesgos de seguridad del sistema de información de la empresa MiBanco

r = Relación entre las variables y las dimensiones de la primera con la segunda variable

Población: La población estuvo conformada por las unidades o áreas de la empresa en donde se encontraron los activos informáticos y a quienes se tuvo que determinar la relación de la metodologia Magerit con la gestión de riesgos del sistema informático, la misma que estuvo constituida por 05 unidades o áreas, la siguiente tabla muestra la cantidad de activos informáticos, en total cual sumaron 48 activos informáticos.

Tabla 2

Población de unidades de la empresa MiBanco de la ciudad de Huaraz

N°	Unidad o área	Cantidad de activos informáticos
01	Gerencia	12
02	Area de créditos	15
03	Area de ahorros	10
04	Atención al cliente	06
05	Contabilidad	05
	TOTAL	**48**

Fuente: Elaboracion propia

Muestra: Dado que la población fue pequeña, en ese sentido, la muestra estuvo estructurada por el mismo tamaño que se indica en la población, esto significa, 48 activos informáticos que formaron parte del sistema de información de la institución financiera MiBanco de la ciudad de Huaraz.

Técnica: La técnica que se aplicó para el recojo de los datos relacionados con el estado situacional de los activos informáticos que formaron parte del sistema de información y el estado de la gestión de riesgos de seguridad de la información de la empresa MiBanco fueron la observación, el análisis y la síntesis para ambas variables.

Instrumento: El instrumento para el recojo de los datos relacionados con el estado situacional de los activos informáticos que formaron parte del sistema de información y el estado de la gestión de riesgos de seguridad de la información de la empresa MiBanco fue la ficha de registro de datos para ambas variables. Para que el instrumento en mención sea aplicado, y dado que el instrumento fue creado por primera vez, inicialmente, se tuvo que establecer la confiabilidad con el método de Alfa de Cronbach para determinar la confiabilidad del instrumento cuyo valor tuvo como valor mayor a 0.80. La validez del instrumento que significa que el instrumento debe medir la variable que debe medir y no otra, se aplicó el método de Juicio de Expertos, la validación fue aceptada debido a que tuvo en promedio, las calificaciones de muy bueno o excelente.

Tabla 3

Técnicas e instrumentos de investigación

Técnicas	Instrumentos
Observacion, análisis, sintesis	Ficha de registro de datos
Análisis documental	Textos, tesis, artículos científicos, revistas cientificas e investigaciones antecedentes

Fuente: Elaboracion propia

La metodología de desarrollo consistió en aplicar la metodología MAGERIT en sus seis fases que la misma metodología establece para analizar y dar tratamientos a los riesgos a los que pueden estar expuestos los activos informáticos de la institución financiera MiBanco.

Análisis de riesgos: En esta fase se analizaron los riesgos en cada una de las unidades de la empresa MiBanco, se inició con la realización del inventario de hardware software y personal, para ello se tuvo que crear una lista de los activos en función de importancia para la empresa, se desarrolló el análisis de software, hardware, conectividad de redes, los riesgos y amenazas a los que

estuvieron expuestos todos los activos informáticos en cada una de las áreas, se tuvieron que analizar los riesgos y vulnerabilidades en función a la seguridad de la información, se analizó el riesgo existente cuando se hicieron uso de la red de redes, así como también, las redes sociales y correos electrónicos. Se tuvo que analizar la gestión de la seguridad actual que realizó la administración de la entidad financiera, lo cual significó que se tuvo que analizar cómo estuvieron identificando los riesgos y las vulnerabilidades. Se analizó el nivel se seguridad de la información, específicamente a los activos más importantes para la institución financiera.

Tratamiento de riesgos: Se desarrolló el análisis de las unidades o áreas de la institución financiera en función de la aplicación de la metodología Magerit sobre cómo estuvieron tratando a los riesgos a los que estuvieron expuestos los activos informáticos, se tuvo que analizar los medios tecnológicos que disponen para enfrentar los riesgos; cómo estuvieron utilizando los medios de control de riesgos, asimismo, se analizaron las conductas y desempeños en el uso de hardware, software, amenazas, riesgos, y seguridad de la información, etc.

RESULTADOS

Objetivo específico 1

Determinar la relación de la aplicación de la metodología Magerit con la Gestión de riesgos de seguridad de hardware en MiBanco, Huaraz 2023.

Tabla 4
Correlación entre la variable Aplicación de la Metodologia Magerit con la dimensión Gestión de riesgos de seguridad de hardware

			Aplicación de la Metodología Magerit	Hardware
Rho de Spearman	Aplicación de la Metodología Magerit	Coeficiente de correlación	1,000	,679**
		Sig. (bilateral)	.	,000
		N	48	48
	Hardware	Coeficiente de correlación	,679**	1,000
		Sig. (bilateral)	,000	.
		N	48	48

**. La correlación es significativa en el nivel 0,01 (bilateral).

La relación entre la variable Aplicación de la metodología Magerit con la dimensión Gestión de riesgos de seguridad de hardware en MiBanco, Huaraz 2023 establecida fue 0.679, esta relación fue positiva moderada significativa. El p valor o valor de significancia o error fue de 0.000, lo cual indica que es menor a 0.05, lo cual indicó que los datos no correspondieron a una curva normal.

Objetivo específico 2

Establecer la relación de la aplicación de la metodología Magerit con la Gestión de riesgos de seguridad de software en MiBanco, Huaraz 2023.

Tabla 5

Correlación entre la variable Aplicación de la Metodologia Magerit con la dimensión Gestión de riesgos de seguridad de software

			Aplicación de la Metodología Magerit	Software
Rho de Spearman	Aplicación de la Metodología Magerit	Coeficiente de correlación	1,000	,660**
		Sig. (bilateral)	.	,000
		N	48	48
	Software	Coeficiente de correlación	,660**	1,000
		Sig. (bilateral)	,000	.
		N	48	48

**. La correlación es significativa en el nivel 0,01 (bilateral).

La relación entre la variable Aplicación de la metodología Magerit con la dimensión Gestión de riesgos de seguridad de software en MiBanco, Huaraz 2023 establecida fue 0.660, esta relación fue positiva moderada significativa. El p valor o valor de significancia o error fue de 0.000, lo cual indica que es menor a 0.05, lo cual indicó que los datos no correspondieron a una curva normal.

Objetivo específico 3

Determinar la relación de la aplicación de la metodología Magerit con la Gestión de riesgos de seguridad de información en MiBanco, Huaraz 2023.

Tabla 6

Correlación entre la variable Aplicación de la Metodologia Magerit con la dimensión Gestión de riesgos de seguridad de la información

			Aplicación de la Metodología Magerit	Información
Rho de Spearman	Aplicación de la Metodología Magerit	Coeficiente de correlación	1,000	,735**
		Sig. (bilateral)	.	,000
		N	48	48

Información	Coeficiente de correlación	,735**	1,000
	Sig. (bilateral)	,000	.
	N	48	48

**. La correlación es significativa en el nivel 0,01 (bilateral).

La relación entre la variable Aplicación de la metodología Magerit con la dimensión Gestión de riesgos de seguridad de la información en MiBanco, Huaraz 2023 establecida fue 0.735, esta relación fue positiva alta significativa. El p valor o valor de significancia o error fue de 0.000, lo cual indica que es menor a 0.05, lo cual indicó que los datos no correspondieron a una curva normal.

Objetivo general

Determinar la relación del plan de seguridad de la información con la seguridad de los activos informáticos de la Municipalidad Provincial de Huari, 2022.

Tabla 7

Correlación entre la variable Aplicación de la Metodologia Magerit con la variable Gestión de riesgos de seguridad de los activos informáticos

			Aplicación de la Metodología Magerit	Gestión de Riesgos de Seguridad
Rho de Spearman	Aplicación de la Metodología Magerit	Coeficiente de correlación	1,000	,706**
		Sig. (bilateral)	.	,000
		N	48	48
	Gestión de Riesgos de Seguridad	Coeficiente de correlación	,706**	1,000
		Sig. (bilateral)	,000	.
		N	48	48

**. La correlación es significativa en el nivel 0,01 (bilateral).

La relación entre la variable Aplicación de la metodología Magerit con la variable Gestión de riesgos de seguridad de los activos informáticos en MiBanco, Huaraz 2023 establecida fue 0.706, esta relación fue positiva alta significativa. El p valor o

valor de significancia o error fue de 0.000, lo cual indica que es menor a 0.05, lo cual indicó que los datos no correspondieron a una curva normal.

ANÁLISIS Y DISCUSIÓN

En este estudio se tuvo como resultado la existencia de relación positiva alta y significativa de 0.706 entre las variables Aplicación de la metodología Magerit con la variable Gestión de riesgos de seguridad de los activos informáticos en un sistema financiero, resultado que coincide ligeramente con los resultados logrados en la investigación antecedente de Contreras (2022) debido a que también encontró que la metodología más utilizada fue Magerit con un 37% y Octave con 16%. Encontró que Magerit cumplió desempeños bastante integrales enfocadas en la clase de análisis, metas de seguridad, clases de riesgos, componentes de la metodología e implantación, esto permite que esta metodología se comporte como robusta en el análisis y gestión de riesgos, por su parte, Octave no cumplió con los parámetros de importancia que puedan satisfacer el desarrollo institucional, a veces no demuestra confianza y atracción para algunas instituciones financieras que deseen implementarla para gestión de riesgos. También identificó las características, fortalezas y debilidades de las metodologías estudiadas, así como el alcance de la gestión de los riesgos. Concluyó que Magerit fue más completo que la metodología Octave en el desarrollo de los análisis relacionados con riesgos.

Se encontró en este estudio la existencia de relación ya indicada entre las variables establecidas, resultado que coincide ligeramente con los resultados logrados en la investigación antecedente de Andrade (2021) concluyó que después de la implantación de Magerit como metodología existieron riesgos con niveles de criticidad, significativos, estimables que estuvieron relacionados con Internet, determinaron que tuvieron que asegurar los activos informáticos con las salvaguardas sugeridas por Magerit. Encontró que los activos de información sobre Hardware se vieron afectados por diversos riesgos, se propusieron salvaguardas, que la mayoría de los riesgos requirieron control para que sean reducidos ya que estuvieron relacionados directamente con el negocio de la empresa y que estuvo ocasionando altos costos, encontraron que pocos riesgos fueron aceptados los

cuales pudieron ser atendidos a costos bastante bajos. Concluyó que Magerit contribuyó positivamente en el objetivo planteado por la empresa.

Se encontró en este estudio la existencia de relación ya indicada entre las variables establecidas correspondientes a la seguridad de los activos informáticos en este estudio aplicado a un sistema financiero, resultado que coincide muy ligeramente con los resultados logrados en la investigación antecedente de Salazar (2020) dado que se encontró que lograron identificar los riesgos existentes en el espacio estudiado respecto a seguridad electrónica, establecieron juicios respecto a los riesgos con fines de asignar datos de influencia y posibilidad de ocurrencia en el espacio de estudio, coincidieron en que también desarrollaron una propuesta de modelamiento de los riesgos basado en la norma ISO 31000, coincide tambien parcialmente con las conclusuones ya que en el antecedentes e tuvo que el esquema diseñado en función a los riesgos en temas de seguridad tecnológica permitió el proceso de los riesgos minimizó significativamente dichos riesgos.

Se encontró en este estudio la existencia de relación ya indicada entre las variables establecidas respecto a los riesgos de seguridad de los activos informáticos en un sistema financiero encontrado en el presente estudio coincide ligeramente con los resultados logrados en la investigación antecedente de Gastelo y Rodríguez (2023) quienes encontraron que Magerit contribuyó en la aplicación de un pertinente juicio de expertos con quienes estuvieron a cargo de los procesos del logro de gestión, permitió agilizar dichos procesos, ayudó en la identificación del factor que hacía diferencia dentro del área de las tecnologías informáticas dentro de institución, estos fueron la falta o escasez de desarrollo de software, enfoque estratégico relacionado con las tecnologías, así como también, la considerable dependencia con el Gobierno Regional y Central, también permitió el establecimiento de una guía ágil sobre el proceso. Que permitieron agilizar a la construcción del modelo de gestión, existió apoyo de las autoridades, lo cual garantizó el éxito de la implementación porque proporcionaron comprensión del proceso de manejo y adquisición de TI. Lograron inicialmente un valor promedio de riesgo, esto fue 363,

mientras que con el plan de tratamiento y elección de salvaguardas se redujo a un promedio de valor de riesgo excedente de 175.49.

En este estudio se tuvo como resultado la existencia de relación positiva alta y significativa de 0.706 entre la variable Aplicación de Magerit con la variable Gestión de riesgos de seguridad de los activos informáticos en un sistema financiero, resultado que coincide ligeramente con los resultados logrados en la investigación antecedente de Linares, Balverdi y Cuellar (2022) en donde encontraron que la información que se debería de cuidar fuero los datos e información, servicios, software, equipos, comunicaciones, equipamiento auxiliar, instalaciones y personal. Tuvieron como amenazas a las de tipo natural, industrial, errores y fallos no intencionados y ataques mal intencionados. Con las políticas cimentadas en Magerit permitió el desarrollo de implantación en concordancia con las amenazas que pueden materializarse y perturbar a los activos de la empresa.

En la presente investigación se encontró la existencia de relación positiva alta y significativa de 0.706 entre la variable Aplicación de Magerit con la variable Gestión de riesgos de seguridad de los activos informáticos en un sistema financiero, resultado que coincide ligeramente con los resultados logrados en la investigación antecedente de Collazos (2021) dado que aplicó Magerit en el establecimiento, vulnerabilidades e impacto de las amenazas, asimismo, determinó las posibilidades de que suceda cada amenaza. La metodología permitió el establecimiento de pautas de evaluación de la magnitud de los riesgos, la identificación de los indicadores importantes para controlar con eficacia a los procesos de gestión de riesgos con fines de controlar la seguridad de la información en una empresa financiera. Las conclusiones también coinciden ligeramente debido a la efectividad en la valoración de riesgos de TI, así como, el tratamiento de los riesgos en rangos no tolerables, en ambos casos, los resultados demostraron que la aplicación de la metodologia Magerit fue bastante aceptable.

Se encontró en este estudio la existencia de relación ya indicada entre las variables establecidas respecto a los riesgos de seguridad de los activos informáticos en este estudio aplicado a un sistema financiero, resultado que coincide muy ligeramente con los resultados logrados en la investigación antecedente de Fernández (2021) debido a que también tuvo como resultado que la aplicación de Magerit mejoró la seguridad de la información, se tuvo correlación de Pearson positiva de 0.970, Lograron establecer a los activos correspondientes relacionados con la información y la evaluación de cada uno de ellos mediante Magerit, se obtuvo correlación de 0.982, es decir, la implantación de la gestión de riesgos de TI permitió mejorar el establecimiento de los activos de información. Los riesgos para los activos fueron valorados mediante la metodología Magerit, en este caso, la correlación de Pearson fue positiva de 0.971, lo cual permitió concluir que la aplicación gestión de riesgos de TI mejoró de manera significativa el grado de protección de información. Lograron instituir procesos de planificación con actividades y controles exigentes con el propósito de minimizar los riesgos presentes, la correlación de positiva fue de 0.683, lo cual permitió concluir que la aplicación gestión de riesgos de TI minimizó de manera significativa los riesgos de seguridad de información en el objeto estudiado.

En esta investigación se encontró la existencia de relación positiva alta y significativa de 0.706 entre la variable Aplicación de Magerit con la variable Gestión de riesgos de seguridad de los activos informáticos en un sistema financiero, resultado que coincide ligeramente con los resultados logrados en la investigación antecedente de Santa María (2020) dado que se encontraron 55 riesgos operativos de tecnologías de información, estos fueron agrupados en 10 tipos de activo: datos comunicaciones, equipos informáticos, documentos, personal, información, equipo auxiliar y servicios. Implementaron un modelo de gestión de riesgos de Tecnologías de Información estos, fueron: identificación de los activos de Tecnologías de Información, lista de activos, vulnerabilidades y amenazas, impacto en caso de amenaza y probabilidades de que ocurra la amenaza. El plan de reducción de riesgos fue aceptado por los responsables conocedores de gestión de

los riesgos operacionales de Tecnologías, los responsables aceptaron la propuesta en un 93%.

En la actual investigación se encontró la existencia de relación positiva alta y significativa de 0.706 entre la variable Aplicación de la metodología Magerit con la variable Gestión de riesgos de seguridad de los activos informáticos en un sistema financiero, resultado que coincide significativamente con los resultados logrados en la investigación antecedente de Cabrejos (2020) en donde también se encontró que existió correlación directa positiva con 78% entre la aplicación de la Metodología Magerit V3 con la variable Seguridad de la información, se encontró influencia de 70.6% entre Magerit V3 y la Seguridad infromática institucional; asimismo encontró falta de capacitación del personal respecto a seguridad y defensa de los activos informáticos. Concluyó que la metodología aplicada en el estudio sirvió contundentemente en los procesos del análisis de cada uno de los riesgos, en la, determinación de las amenazas, personalización de las salvaguardas y contribuyó en la implementación de futuras salvaguardas relacionados con el control y mitigación de riesgos. Que fue necesario ejecutar un plan de gestión y tratamiento de riesgos con fines de minimización de riesgos y establecimiento de estrategias para reducción de vulnerabilidades y amenazas hacia los registros de información.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Se concluyó a nivel general que existió relación positiva alta y significativa de 0.706 entre la variable Aplicación de la metodología Magerit con la variable Gestión de riesgos de seguridad de los activos informáticos en MiBanco, Huaraz 2023, el p valor fue de 0.000, esto indicó que los datos no correspondieron a una curva normal.

Existió relación positiva moderada y significativa de 0.679 entre la variable Aplicación de la metodología Magerit con la dimensión Gestión de riesgos de seguridad de hardware, el p valor fue de 0.000.

Existió relación positiva moderada significativa de 0.660 entre la variable Aplicación de la metodología Magerit con la dimensión Gestión de riesgos de seguridad de software, el p valor fue de 0.000, lo cual indicó que los datos no correspondieron a una curva normal.

Existió relación positiva alta y significativa de 0.735 entre la variable Aplicación de la metodología Magerit con la dimensión Gestión de riesgos de seguridad de la información, el p valor fue de 0.000.

RECOMENDACIONES

La Gerencia de la institución financiera MiBanco filial Huaraz conjuntamente con el jefe del Área de Informática deben tomar decisiones respecto a la Aplicación de la metodología Magerit y la Gestión de riesgos de seguridad de los activos informáticos, estas decisiones deben orientarse decididamente en la mejora de ambas variables, para ello deben lograr la participación consciente, volitiva y decidida de operarios y adminsitrativos, específicamente de los usuarios del sistema de información de la empresa financiera.

La Gerencia de la institución financiera MiBanco filial Huaraz conjuntamente con el jefe del Área de Informática deben realizar capacitaciones para todos los usuarios del sistema de información Gestión de riesgos de seguridad de hardware, para lograr estos, deben contratar especialistas de instituciones conocidas y con experiencia en seguridad d hardware en instituciones financieras, las capacitaciones deben involucrar la seguridad de los servidores, computadores, hardware del sistema de red, etc.

La Gerencia de la institución financiera MiBanco filial Huaraz conjuntamente con el jefe del Área de Informática deben realizar capacitaciones para todos los usuarios del sistema de información Gestión de riesgos de seguridad de software, especialmente en el uso del sistema operativo de red, software antivirus, protección de base de datos, protección de la información, conocimiento de los diversos ataques informáticos basados en internet y enfocados en ataques al sistema financiero.

La Gerencia de la institución financiera MiBanco filial Huaraz conjuntamente con el jefe del Área de Informática deben realizar continuar con las capacitaciones en el conocimiento relacionados con la protección de las informaciones financieras de importancia para MiBanco y sus clientes, específicamente la información de ahorros y créditos con cuentas en montos significativos e información sensible para la empresa.

AGRADECIMIENTOS

A Dios por permitirme el objetivo de ser profesional, a la empresa financiera MiBanco por el espacio, los datos e información alcanzada, a la Universidad San Pedro por todo el apoyo recibido a través sus docentes quienes supieron darme la formación y enseñanza, a todos mis compañeros quienes contribuyeron en el logro de mi objetivo, ser profesional.

Milagros

REFERENCIAS BIBLIOGRÁFICAS

Altamirano, M. (2019). *Modelo para la gestión de la seguridad de la información y los riesgos asociados a su uso*. *Avances*, *21*(2), 248-263. doi: http://www.ciget.pinar.cu/ojs/index.php/publicaciones/article/view/440/1426

Amutio Gómez, M. A., Candau, J., & Mañas, J. A. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Madrid: Ministerio de Hacienda y Administraciones Públicas. doi: http://administracionelectronica.gob.es/

Amutio, M., Candau, J. & Mañas, J. (2014). *MAGERIT- V3, methodology for information systems risk analysis and management.* Book I - The Method, Ministerio de Administraciones Públicas.

Andrade, D. L. (2021). *Análisis de los conceptos, elementos y técnicas de la gestión de riesgo orientado a las pymes del sector de las telecomunicaciones basado en Magerit V3*. [Tesis de grado]. Universidad Abierta y a Distancia. Colombia.

Baca, G. (2016). *Introducción a la Seguridad Informática*. México: Grupo Editorial Patria, S.A. de C.V.

Berrio, J. P. (2016). *Metodologia para la evaluación del desempeño de controles en sistemas de gestión de seguridad de la información sobre la norma ISO/IEC 27001* [Tesis de Maestría]. Medellín, Colombia.

Brunner, M., Sauerwein, C., Felderer, M., & Breu, R. (2020). *Risk management practices in information security*: Exploring the status quo in the DACH region. (E. Ltd., Ed.) *Computers & Security, 92*, 12. doi: https://doi.org/10.1016/j.cose.2020.101776

Cabrejos, R. (2020). *Influencia de la metodología Magerit v3 en la seguridad de información de la empresa Deco Interiors SAC.* [Tesis de grado]. Universidad señor de Sipán. Pimentel Perú.

Calder, A. & Watkins, S. (2008). *A Manager's Guide to Data Security and ISO 27001/ISO 27002.* (4ta ed.). Kogan.

Chicano, E. (2014). *Gestión de incidentes de seguridad informática*. Málaga: IC Editorial. España.

Collazos, J. R. (2021). *Aplicación de la metodología MAGERIT en la gestión de riesgos de tecnologías de la información en la agencia Metro Santa Elena del banco Scotiabank –Distrito de Chiclayo – Provincia de Chiclayo – Región Lambayeque.* [Tesis de grado]. Universidad Nacional Pedro Ruiz Gallo. Lambayeque Perú.

Contreras, G. A. (2022). *Análisis comparativo entre las metodologías de gestión de riesgos de los sistemas de gestión de seguridad de la información (SGSI): Magerit y octave.* [Tesis de grado]. Universidad Técnica de Babahoyo. Ecuador.

Costas Santos, J. (2014). *Seguridad Informática*. Madrid: RA-MA.

Crespo, P. (2016). *Metodología de seguridad de la información para la gestión del riesgo informático aplicable a Mpymes* (Tesis de Maestría). Universidad de Cuenca, Ecuador. Recuperado de: http://dspace.ucuenca.edu.ec/bitstream/123456789/26105/1/Tesis.pdf

España, G. D. (2012). *MAGERIT - Metodologia de Análisis y Gestión de Riegos de los* Sistemas de Información. España.

Fernández, A. A. (2021). *Aplicación de gestión de riesgos de TI para mejorar la seguridad de información en una empresa de agencia de viajes en la ciudad de Lima -2021*. [Tesis de grado]. Universidad Tecnológica del Perú. Lima Perú.

Fernández, A. & García, D. (2016). *Complex vs. Simple Asset Modeling Approaches for Information Security Risk Assessment*. In The Sixth International Conference on Innovative Computing Technology (INTECH 2016). Recuperado de: https://sci-hub.tw/10.1109/INTECH.2016.7845064

Figueira, T., López, C., & Rivas, J. (2020). *Improving information security risk analysis by including threat-occurrence predictive models*. Computers & Security, *88*(101609), 12. doi: https://doi.org/10.1016/j.cose.2019.101609

Gastelo, E. J. y Rodríguez, A. H. (2023). *Desarrollo de un modelo de gestión de riesgos basado en la metodología Magerit para minimizar los riesgos de adquisición y uso de TI en una municipalidad de Perú. caso de estudio: municipalidad distrital de Cuspinique – Cajamarca.* [Tesis de grado]. Universidad señor de Sipán. Pimentel Perú.

Hernández, R., Fernández, C., & Baptista, P. (2014). *Metodología de la Investigación* (Vol. Sexta Edición). México: Mc Graw Hill.

Hurtado, M. (2018). Gestión de Riesgos Metodologías Octave y Magerit. *Metodología de Análisis de Riesgo.*, 12. doi: http://polux.unipiloto.edu.co:8080/00004420.pdf

ISACA, Asociación de Auditoría y Control de Sistemas de Información. (2009). Lineamientos para la gestión de la seguridad de TI. *Manual de preparación CISA 2009*. Lima, Perú.

Joyanes, L. (2015). Sistemas de información en la empresa. Alfaomega Editorial

Linares, E.; Balverdi, L. y Cuellar, I. (2022). *Políticas de seguridad de la información y metodología Magerit en la empresa Induamerica Chiclayo S.A.C.* [Artículo Científico]. Universidad Peruana Unión. Perú. Revista Pakamuros, volumen 10, 2 DOI:

https://doi.org/10.37787/pakamuros-unj.v10i2.224

Llontop, G. C. (2018). *Gestión de riesgos de Tecnologías de Información de las empresas de Nephila Networks.* [Tesis de Maestría]. Lima.

Medina, A. (2007). *Seguridad informática*. Lima: Universidad Nacional Mayor de San Marcos.

Mercado, J. E. (2016). *Modelo de gestión de seguridad de la información para el E-Gobierno* [Tesis de Maestría]. Lima.

Mirtsch, M., Blind, K., Koch, C., & Dudek, G. (2021). *Information security management in ICT and non-ICT sector companies: A preventive innovation perspective*. (E. Ltd, Ed.) *Computers & Security, 109*(October 2021), 23. doi: https://doi.org/10.1016/j.cose.2021.102383

Molina, M. (2017). *Análisis de riesgos de centro de datos basado en la herramienta Pilar de Magerit. Espirales 1*(11). Recuperado de: http://www.revistaespirales.com/index.php/es/article/view/125/68

Molina, M. F. (2015). *Propuesta de un plan de gestión de riesgos de tecnología aplicado en la Escuela Superior Politécnica del Litoral*. [Tesis de maestría]. Universidad Politécnica de Madrid, España. Recuperado de:

https://www.dit.upm.es/~posgrado/doc/TFM/TFMs2014-2015/TFM_Maria_Fernanda_Molina_Miranda_2015.pdf

Morán, A. (2019). *Ciberseguridad: aprendizaje disruptivo en la protección de infraestructuras críticas y la seguridad nacional*. Seguridad, Ciencia & Defensa, *5*(5), 73-85. doi: https://revista.insude.mil.do/index.php/rscd/article/view/64

Motaki, K. (2016). *Risk Analysis and Risk Management in Critical Infrastructures* [Tesis de Maestría]. University of Piraeus. Recuperado de: http://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/9741/Motaki_Katerina.pdf?sequence=1&isAllowed=y

Rodríguez, J. M., & Peralta, I. (02 de 04 de 2019). *Gestión de riesgo Margerit*. Obtenido de www.tithimk.com.

Salazar, L. I. (2020). *Modelo de Gestión de Riesgo para Sistemas de Seguridad Electrónica para Entidades Financieras. Revista PGI. Investigación, Ciencia y Tecnología en Informática, N.º 7, pp. 80-82*. [Artículo científico]. Universidad Mayor de San Andrés, La Paz, Bolivia.

Santa María, W. (2020). *Plan para reducir los riesgos operativos de tecnologías de la información basada en metodologia Magerit en la caja Piura de la ciudad de Chiclayo.* [Tesis de grado]. Universidad de Lambayeque. Chiclayo Perú.

Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). *Taxonomy of Information Security Risk Assessment (ISRA)*. Computers & Security, *57*, 14–30.

http://dx.doi.org/10.1016/j.cose.2015.11.001

Taubenberger, S. (2014). *Vulnerability Identification Errors in Security Risk Assessments.* (Tesis doctoral). The Open University, Reino Unido. http://oro.open.ac.uk/39626/

ANEXOS Y APÉNDICES

Anexo 01:

Matriz de Consistencia

Metodología Magerit y su relación con gestión de riesgos de seguridad del sistema de información en MiBanco Huaraz, 2023

PROBLEMA DE INVESTIGACIÓN	OBJETIVOS	HIPÓTESIS	METODOLOGÍA
Problema General	**Objetivo General**	**Hipótesis General**	
¿En qué medida se relaciona la aplicación de la metodología Magerit con la Gestión de riesgos de seguridad del sistema de información en MiBanco, Huaraz 2023?	Determinar la relación entre de la aplicación de la metodología Magerit con la Gestión de riesgos de seguridad del sistema de información en MiBanco, Huaraz 2023.	La aplicación de la metodología Magerit se relaciona positivamente con la Gestión de riesgos de seguridad del sistema de información en MiBanco, Huaraz 2023.	Se considera que la investigación es de tipo no experimental. **Diseño de la Investigación** **Diseño:**
Problemas específicos	**Objetivos Específicos**	**Hipótesis Específicas**	Descriptivo correlacional.
¿En qué medida se relaciona la aplicación de la metodología Magerit con la Gestión de riesgos de seguridad de hardware en MiBanco, Huaraz 2023?	Determinar la relación de la aplicación de la metodología Magerit con la Gestión de riesgos de seguridad de hardware en MiBanco, Huaraz 2023.	La aplicación de la metodología Magerit se relaciona positivamente con la Gestión de riesgos de seguridad de hardware en MiBanco, Huaraz 2023.	**Enfoque:** Cuantitativo **Población y Muestra:**
¿En qué medida se relaciona la aplicación de la metodología Magerit con la Gestión de riesgos de seguridad de software en MiBanco, Huaraz 2023?	Establecer la relación de la aplicación de la metodología Magerit con la Gestión de riesgos de seguridad de software en MiBanco, Huaraz 2023.	La aplicación de la metodología Magerit se relaciona positivamente con la Gestión de riesgos de seguridad de software en MiBanco, Huaraz 2023.	Los elementos de la población reconformarán 25 trabajadores de MiBanco, usuarios del sistema de información de esta institución financiera de la ciudad de Huaraz.
¿En qué medida se relaciona la aplicación de la	Determinar la relación de la aplicación de la metodología Magerit con la Gestión de riesgos de seguridad de	La aplicación de la metodología Magerit se	

metodología Magerit con la Gestión de riesgos de seguridad de información en MiBanco, Huaraz 2023?	información en MiBanco, Huaraz 2023.	relaciona positivamente con la Gestión de riesgos de seguridad de información en MiBanco, Huaraz 2023.	**Instrumentos de investigación** Encuesta

Anexo 02

UNIVERSIDAD SAN PEDRO

ENCUESTA

Bach. Silva Medina Milagros

Estimado encuestado: Sírvase responder con absoluta sinceridad la siguiente encuesta que corresponde al estudio de la aplicación de la Metodología Magerit y su relación con gestión de riesgos de seguridad del sistema de información en MiBanco Huaraz, 2023. Sírvase responder la encuesta con responsabilidad y honestidad. Este proceso es totalmente anónimo, se reitera el pedido de absoluta honestidad en sus respuestas. Muchas Gracias por su participación.

CUESTIONARIO

N°	DIM	FICHA DE REGISTRO DE DATOS	ESCALA				
			1	2	3	4	5
APLICACIÓN DE LA METODOLOGÍA MAGERIT							
01	**Análisis de seguridad**	Calificación de la determinación del contexto en el área de ahorros con la aplicación de la metodología Magerit en MiBanco Huaraz 2023					
02		Consideración de la determinación del contexto en el área de créditos con la aplicación de la metodología Magerit en MiBanco Huaraz 2023					
03		Evaluación de la determinación del contexto en el área de plataforma con la aplicación de la metodologia Magerit en MiBanco Huaraz 2023					
04		Valoración de la identificación de hardware con la aplicación de la metodología Magerit en MiBanco Huaraz 2023					

05		Califica la identificación de software con la aplicación de la metodología Magerit en MiBanco Huaraz 2023					
06		Consideración de la identificación de la información con la aplicación de la metodología Magerit en MiBanco Huaraz 2023					
07		Calificación de la identificación de amenazas al hardware con la aplicación de la metodología Magerit en MiBanco Huaraz 2023					
08		Consideración de la identificación de amenazas al software con la aplicación de la metodología Magerit en MiBanco Huaraz 2023					
09		Evaluacion de la identificación de amenazas a la información con la aplicación de la metodología Magerit en MiBanco Huaraz 2023					
10	**Tratamiento de la seguridad**	Calificación del tratamiento de la seguridad del sistema operativo en MiBanco Huaraz 2023					
11		Consideración el tratamiento de la seguridad del software antivirus en MiBanco Huaraz 2023					
12		Evaluación del tratamiento de la seguridad de software financiero en MiBanco Huaraz 2023					
13		Valoración del tratamiento de la seguridad de la información en MiBanco Huaraz 2023					
14		Calificación del tratamiento de la seguridad de las computadoras clientes en MiBanco Huaraz 2023					
15		Consideración del tratamiento de la seguridad del servidor en MiBanco Huaraz 2023					
16		Evaluación del tratamiento de la seguridad de hardware de conectividad de Internet en MiBanco Huaraz 2023					

LEYENDA

1 Malo 2 Regular 3 Normal 4 Bueno 5 Excelente

N°	DIM	FICHA DE REGISTRO DE DATOS	ESCALA				
			1	2	3	4	5
RIESGOS DE SEGURIDAD DEL SISTEMA DE INFORMACIÓN							
01	**Hardware**	Calificación de la gestión de riesgo de seguridad del servidor en MiBanco Huaraz 2023					
02		Calificación de la gestión de riesgo de seguridad de las computadoras en MiBanco Huaraz 2023					
03		Calificación de la gestión de riesgo de seguridad del hardware de conectividad de Internet en MiBanco Huaraz 2023					
04		Calificación de la gestión de riesgo de seguridad de impresoras en MiBanco Huaraz 2023					
05	**Software**	Consideración del tratamiento de la seguridad del sistema operativo en MiBanco Huaraz 2023					
06		Consideración del tratamiento de la seguridad del software antivirus en MiBanco Huaraz 2023					
07		Consideración del tratamiento de la seguridad del software financiero en MiBanco Huaraz 2023					
08		Consideración del tratamiento de la seguridad del software de oficina en MiBanco Huaraz 2023					
09	**Información**	Consideración del tratamiento de la seguridad de la información financiera de importancia en el área de ahorros en MiBanco Huaraz 2023					
10		Consideración del tratamiento de la seguridad de la información financiera de importancia en el área de créditos en MiBanco Huaraz 2023					
11		Consideración del tratamiento de la seguridad de la base de datos en MiBanco Huaraz 2023					
12		Consideración del tratamiento de la seguridad del acceso a Internet en MiBanco Huaraz 2023					
13		Consideración del tratamiento de la seguridad del acceso a las redes sociales en MiBanco Huaraz 2023					

14		Consideración del tratamiento de la seguridad del acceso a correos electrónicos en MiBanco Huaraz 2023					

LEYENDA

1 Malo 2 Regular 3 Normal 4 Bueno 5 Excelente

Anexo 03

Alfa de Cronbach

N°	APLICACIÓN DE METODOLOGÍA MAGERIT																		
	Analisis de seguridad									TOT	Tratamiento de seguridad							TOT	TOT
	1	2	3	4	5	6	7	8	9		10	11	12	13	14	15	16		
1	2	1	1	1	1	2	1	2	1	6	1	4	1	2	1	2	1	6	12
2	2	1	3	2	1	3	1	3	1	8	2	2	1	2	2	3	1	8	16
3	4	3	4	4	4	4	3	4	4	15	5	3	4	4	5	5	3	17	32
4	1	1	1	1	2	2	1	2	2	7	4	1	2	1	1	1	1	4	11
4	2	3	2	2	1	1	2	1	1	5	1	3	1	1	3	2	2	8	13
6	2	2	1	4	3	4	2	5	2	13	1	2	1	3	2	4	2	11	24
7	2	4	2	3	2	4	2	4	3	13	5	1	4	4	5	2	5	16	29
8	1	1	2	1	3	1	1	2	1	5	1	1	1	2	1	1	2	6	11
9	4	2	3	5	1	2	1	2	2	7	2	2	1	1	3	1	1	6	13
10	3	4	2	1	3	1	4	1	1	7	2	4	3	1	4	4	3	12	19
Var										12.0								17.8	
																		Suma de varianzas parciales	29.88
																		Varianza General o total	54.20
																		Valor de Alfa	0.897

N°	GESTIÓN DE RIESGOS DE SEGURIDAD DEL SISTEMA DE INFORMACIÓN																	
	Seguridad de Hardware				TOT	Seguridad de Software				TOT	Seguridad de información						TOT	TOT
	1	2	3	4		5	6	7	8		9	10	11	12	13	14		
1	1	1	2	1	5	1	1	2	1	5	1	1	2	1	1	1	7	17
2	1	1	1	1	4	1	1	1	1	4	1	1	1	4	1	1	9	17
3	4	3	1	5	13	5	4	5	5	19	5	2	5	4	5	1	22	54
4	2	1	2	1	6	4	2	4	2	12	2	1	2	1	1	1	8	26
5	1	2	1	1	5	1	1	2	1	5	1	2	1	1	1	4	10	20
6	4	2	4	2	12	5	4	5	5	19	5	3	4	2	5	3	22	53
7	5	5	5	4	19	3	5	4	1	13	4	4	5	4	4	5	26	58
8	1	1	4	1	7	1	1	1	3	6	1	1	1	1	4	1	9	22
9	4	3	3	1	11	4	2	3	4	13	2	1	5	1	3	5	17	41
10	1	2	1	2	6	1	1	1	1	4	1	1	5	1	1	1	10	20
Var					20.8					32.2							49.8	
																	Suma de varianzas	102.74
																	Varianza General	254.96
																	Valor de Alfa	0.896

MATRIZ DE VALIDACIÓN POR JUICIO DE EXPERTO

TITULO DE LA TESIS: Metodología Magerit y su relación con gestión de riesgos de seguridad del sistema de información en MiBanco, Huaraz 2023

NOMBRE DEL INSTRUMENTO: Matriz de Validación

VARIABLES	DIMENSIONES	ITEMS	OPCIÓN DE RESPUESTA					VALORACIÓN								Observ
								A		B		C		D		
			1	2	3	4	5	SI	NO	SI	NO	SI	NO	SI	NO	
APLICACIÓN DE LA METODOLOGÍA MAGERIT	Análisis de seguridad	¿Cómo califica la determinación del contexto en el área de ahorros con la aplicación de la metodología Magerit en MiBanco Huaraz 2023?			X			X		X		X		X		
		¿Cómo considera la determinación del contexto en el área de créditos con la aplicación de la metodología Magerit en MiBanco Huaraz 2023?				X		X		X		X		X		
		¿Cómo evalúa la determinación del contexto en el área de plataforma con la aplicación de la metodología Magerit en MiBanco Huaraz 2023?				X		X		X		X		X		
		¿Cómo valora la identificación de hardware con la aplicación de la metodología Magerit en MiBanco Huaraz 2023?				X		X		X		X		X		
		¿Cómo califica la identificación de software con la aplicación de la metodología Magerit en MiBanco Huaraz 2023?				X		X		X		X		X		
		¿Cómo considera la identificación de la información con la aplicación de la metodología Magerit en MiBanco Huaraz 2023?				X		X		X		X		X		

		¿Cómo califica la identificación de amenazas al hardware con la aplicación de la metodología Magerit en MiBanco Huaraz 2023?				X		X		X		X		X			
		¿Cómo considera la identificación de amenazas al software con la aplicación de la metodología Magerit en MiBanco Huaraz 2023?				X		X		X		X		X			
		¿Cómo evalúa la identificación de amenazas a la información con la aplicación de la metodología Magerit en MiBanco Huaraz 2023?				X		X		X		X		X			
	Tratamiento de la seguridad	¿Cómo califica el tratamiento de la seguridad del sistema operativo en MiBanco Huaraz 2023?				X		X		X		X		X			
		¿Cómo considera el tratamiento de la seguridad del software antivirus en MiBanco Huaraz 2023?				X		X		X		X		X			
		¿Cómo evalúa el tratamiento de la seguridad de software financiero en MiBanco Huaraz 2023?				X		X		X		X		X			
		¿Cómo valora el tratamiento de la seguridad de la información en MiBanco Huaraz 2023?				X		X		X		X		X			
		¿Cómo califica el tratamiento de la seguridad de las computadoras clientes en MiBanco Huaraz 2023?				X		X		X		X		X			
		¿Cómo considera el tratamiento de la seguridad del servidor en MiBanco Huaraz 2023?				X		X		X		X		X			
		¿Cómo evalúa el tratamiento de la seguridad de hardware de conectividad de Internet en MiBanco Huaraz 2023?				X		X		X		X		X			
		¿Cómo califica el tratamiento de la seguridad del sistema operativo en MiBanco Huaraz 2023?				X		X		X		X		X			

RIESGOS DE SEGURIDAD DEL SISTEMA DE INFORMACIÓN	Hardware	¿Cómo califica la gestión de riesgo de seguridad del servidor en MiBanco Huaraz 2023?				X		X		X		X		X			
		¿Cómo califica la gestión de riesgo de seguridad de las computadoras en MiBanco Huaraz 2023?				X		X		X		X		X			
		¿Cómo califica la gestión de riesgo de seguridad del hardware de conectividad de Internet en MiBanco Huaraz 2023?				X		X		X		X		X			
		¿Cómo califica la gestión de riesgo de seguridad de impresoras en MiBanco Huaraz 2023?				X		X		X		X		X			
	Software	¿Cómo considera el tratamiento de la seguridad del sistema operativo en MiBanco Huaraz 2023?				X		X		X		X		X			
		¿Cómo considera el tratamiento de la seguridad del software antivirus en MiBanco Huaraz 2023?				X		X		X		X		X			
		¿Cómo considera el tratamiento de la seguridad del software financiero en MiBanco Huaraz 2023?				X		X		X		X		X			
		¿Cómo considera el tratamiento de la seguridad del software de oficina en MiBanco Huaraz 2023?				X		X		X		X		X			
	Información	¿Cómo considera el tratamiento de la seguridad de la información financiera de importancia en el área de ahorros en MiBanco Huaraz 2023?				X		X		X		X		X			
		¿Cómo considera el tratamiento de la seguridad de la información financiera de importancia en el área de créditos en MiBanco Huaraz 2023?				X		X		X		X		X			

		¿Cómo considera el tratamiento de la seguridad de la base de datos en MiBanco Huaraz 2023?				X		X		X		X		X			
		¿Cómo considera el tratamiento de la seguridad del acceso a Internet en MiBanco Huaraz 2023?				X		X		X		X		X	X		
		¿Cómo considera el tratamiento de la seguridad del acceso a las redes sociales en MiBanco Huaraz 2023?				X		X		X		X		X	X		
		¿Cómo considera el tratamiento de la seguridad del acceso a correos electrónicos en MiBanco Huaraz 2023?				X		X		X		X		X	X		

1 = Malo 2 = Regular 3 = Bueno 4 = Muy Bueno 5 = Excelente.

A = Relación entre la variable y dimensión
B = Relación entre la dimensión y el indicador
C = Relación entre el indicador y los ítems
D = Relación entre el ítem y la opción de respuesta

Firma del Experto

Nombre: Juan Julio Chavez Alvaro
Correo: julio.chavez.sistemas@gmail.com
Celular: 971628339

MATRIZ DE VALIDACIÓN POR JUICIO DE EXPERTO

TITULO DE LA TESIS: Metodología Magerit y su relación con gestión de riesgos de seguridad del sistema de información en MiBanco, Huaraz 2023

NOMBRE DEL INSTRUMENTO: Matriz de Validación

VARIABLES	DIMENSIONES	ITEMS	OPCIÓN DE RESPUESTA					VALORACIÓN								Observ
								A		B		C		D		
			1	2	3	4	5	SI	NO	SI	NO	SI	NO	SI	NO	
APLICACIÓN DE LA METODOLOGÍA MAGERIT	Análisis de seguridad	¿Cómo califica la determinación del contexto en el área de ahorros con la aplicación de la metodología Magerit en MiBanco Huaraz 2023?						X		X		X		X		
		¿Cómo considera la determinación del contexto en el área de créditos con la aplicación de la metodología Magerit en MiBanco Huaraz 2023?						X		X		X		X		
		¿Cómo evalúa la determinación del contexto en el área de plataforma con la aplicación de la metodologia Magerit en MiBanco Huaraz 2023?						X		X		X		X		
		¿Cómo valora la identificación de hardware con la aplicación de la metodología Magerit en MiBanco Huaraz 2023?						X		X		X		X		
		¿Cómo califica la identificación de software con la aplicación de la metodología Magerit en MiBanco Huaraz 2023?						X		X		X		X		
		¿Cómo considera la identificación de la información con la aplicación de la metodología Magerit en MiBanco Huaraz 2023?						X		X		X		X		

		¿Cómo califica la identificación de amenazas al hardware con la aplicación de la metodología Magerit en MiBanco Huaraz 2023?						X		X		X		X			
		¿Cómo considera la identificación de amenazas al software con la aplicación de la metodología Magerit en MiBanco Huaraz 2023?						X		X		X		X			
		¿Cómo evalúa la identificación de amenazas a la información con la aplicación de la metodología Magerit en MiBanco Huaraz 2023?						X		X		X		X			
	Tratamiento de la seguridad	¿Cómo califica el tratamiento de la seguridad del sistema operativo en MiBanco Huaraz 2023?						X		X		X		X			
		¿Cómo considera el tratamiento de la seguridad del software antivirus en MiBanco Huaraz 2023?						X		X		X		X			
		¿Cómo evalúa el tratamiento de la seguridad de software financiero en MiBanco Huaraz 2023?						X		X		X		X			
		¿Cómo valora el tratamiento de la seguridad de la información en MiBanco Huaraz 2023?						X		X		X		X			
		¿Cómo califica el tratamiento de la seguridad de las computadoras clientes en MiBanco Huaraz 2023?						X		X		X		X			
		¿Cómo considera el tratamiento de la seguridad del servidor en MiBanco Huaraz 2023?						X		X		X		X			
		¿Cómo evalúa el tratamiento de la seguridad de hardware de conectividad de Internet en MiBanco Huaraz 2023?						X		X		X		X			
		¿Cómo califica el tratamiento de la seguridad del sistema operativo en MiBanco Huaraz 2023?						X		X		X		X			

RIESGOS DE SEGURIDAD DEL SISTEMA DE INFORMACIÓN	Hardware	¿Cómo califica la gestión de riesgo de seguridad del servidor en MiBanco Huaraz 2023?						X		X		X		X			
		¿Cómo califica la gestión de riesgo de seguridad de las computadoras en MiBanco Huaraz 2023?						X		X		X		X			
		¿Cómo califica la gestión de riesgo de seguridad del hardware de conectividad de Internet en MiBanco Huaraz 2023?						X		X		X		X			
		¿Cómo califica la gestión de riesgo de seguridad de impresoras en MiBanco Huaraz 2023?						X		X		X		X			
	Software	¿Cómo considera el tratamiento de la seguridad del sistema operativo en MiBanco Huaraz 2023?						X		X		X		X			
		¿Cómo considera el tratamiento de la seguridad del software antivirus en MiBanco Huaraz 2023?						X		X		X		X			
		¿Cómo considera el tratamiento de la seguridad del software financiero en MiBanco Huaraz 2023?						X		X		X		X			
		¿Cómo considera el tratamiento de la seguridad del software de oficina en MiBanco Huaraz 2023?						X		X		X		X			
	Información	¿Cómo considera el tratamiento de la seguridad de la información financiera de importancia en el área de ahorros en MiBanco Huaraz 2023?						X		X		X		X			
		¿Cómo considera el tratamiento de la seguridad de la información financiera de importancia en el área de créditos en MiBanco Huaraz 2023?						X		X		X		X			

		¿Cómo considera el tratamiento de la seguridad de la base de datos en MiBanco Huaraz 2023?						X		X		X		X		
		¿Cómo considera el tratamiento de la seguridad del acceso a Internet en MiBanco Huaraz 2023?						X		X		X		X	X	
		¿Cómo considera el tratamiento de la seguridad del acceso a las redes sociales en MiBanco Huaraz 2023?						X		X		X		X	X	
		¿Cómo considera el tratamiento de la seguridad del acceso a correos electrónicos en MiBanco Huaraz 2023?						X		X		X		X	X	

1 = Malo 2 = Regular 3 = Bueno 4 = Muy Bueno 5 = Excelente.

A = Relación entre la variable y dimensión
B = Relación entre la dimensión y el indicador
C = Relación entre el indicador y los ítems
D = Relación entre el ítem y la opción de respuesta

Edwin Alex Sanchez Rios
ING. EN INFORMATICA Y DE SISTEMAS
Reg. Colegio de Ingenieros N° 102820
Firma del Experto

Nombre: Edwin Alex Sanchez Rios
Correo: edwinalex02@hotmail.com
Celular: 996965625

Anexo 04

Mapa de datos

N°	APLICACIÓN DE LA METODOLOGÍA MAGERIT															
	Análisis de seguridad									Tratamiento de seguridad						
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	1	2	3	2	2	2	3	3	2	3	2	2	1	2	2	1
2	4	4	5	4	5	4	5	4	5	4	5	5	4	5	5	5
3	1	2	2	1	1	1	1	2	1	1	1	1	2	1	1	1
4	3	1	2	2	3	2	2	1	2	3	1	2	2	3	1	2
5	1	2	2	2	3	2	1	2	3	2	2	3	2	2	2	3
6	2	3	3	3	2	3	3	3	3	4	3	3	2	4	2	3
7	1	2	2	3	2	3	1	2	1	3	2	3	2	3	2	2
8	2	1	2	1	1	2	1	2	2	1	1	2	1	1	1	1
9	3	4	3	2	4	1	3	1	2	4	1	2	4	5	2	5
10	3	4	2	1	2	3	3	2	1	2	1	1	2	1	2	2
11	1	2	4	1	4	3	4	3	4	3	2	4	3	3	3	2
12	2	3	1	3	2	2	3	2	1	1	1	1	2	3	2	3
13	4	5	4	4	4	5	4	4	4	5	3	4	4	3	4	4
14	1	2	3	2	1	3	2	1	2	2	2	3	2	3	2	2
15	1	1	2	1	1	2	1	1	1	1	2	1	1	1	1	1
16	2	1	2	2	2	3	1	2	1	2	1	3	2	3	2	1
17	4	2	5	5	3	4	5	4	1	4	5	5	4	4	3	5
18	3	2	1	3	2	3	3	2	1	3	1	3	2	3	1	3
19	5	5	4	5	5	4	5	4	4	4	5	4	5	5	4	5
20	1	1	1	2	2	3	2	4	2	3	2	2	2	3	3	2
21	4	4	3	2	3	4	3	3	4	3	2	3	3	3	4	3
22	2	1	1	3	1	2	1	1	1	3	1	1	1	1	1	1
23	4	2	3	2	3	2	3	2	5	3	3	4	2	3	2	3
24	2	2	1	2	1	3	4	2	5	1	1	1	2	2	2	3
25	2	1	2	1	2	1	1	1	1	2	1	1	1	1	2	1
26	1	2	1	3	1	1	2	1	1	1	1	1	1	2	1	1
27	5	4	4	4	3	3	4	5	3	4	4	3	4	2	4	5
28	1	2	2	2	1	4	2	3	2	2	2	2	2	4	1	2
29	3	4	3	3	3	2	3	3	3	4	4	3	2	3	3	3
30	3	3	4	3	2	3	4	2	4	2	3	4	3	3	2	5
31	1	1	1	2	1	1	2	2	1	3	1	1	2	1	1	1
32	3	2	2	2	4	1	2	2	1	2	1	2	3	2	2	2
33	3	2	1	1	3	1	1	1	1	2	1	1	2	1	1	1
34	4	5	3	4	4	3	4	4	4	5	5	4	4	5	4	3
35	3	2	2	3	1	1	2	3	3	2	4	2	2	1	1	2
36	3	4	3	5	4	2	3	5	4	3	4	3	5	3	4	4
37	2	3	3	2	2	2	2	2	1	3	1	1	2	3	2	2

N°	APLICACIÓN DE LA METODOLOGÍA MAGERIT															
	Análisis de seguridad									Tratamiento de seguridad						
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
38	3	2	4	3	3	4	3	3	4	5	3	4	2	4	3	3
39	1	2	3	3	2	2	1	3	1	1	2	1	2	3	2	1
40	5	4	4	4	3	4	4	4	4	4	3	4	4	4	4	4
41	4	2	2	4	1	4	4	2	2	2	2	3	2	3	1	2
42	3	4	3	3	3	4	3	4	3	5	4	4	4	3	4	4
43	2	3	4	2	2	4	2	4	4	3	4	1	4	3	4	4
44	4	3	2	3	4	2	5	4	2	3	3	2	5	3	2	3
45	3	1	2	2	1	2	1	1	2	1	1	1	1	1	2	1
46	5	5	4	4	5	5	4	5	4	5	4	5	5	5	5	4
47	2	4	3	5	3	5	3	3	4	3	4	3	4	3	2	1
48	2	2	3	2	3	1	2	2	3	1	2	1	2	2	3	2

N°	GESTIÓN DE RIESGOS DE SEGURIDAD													
	Hardware				Software				Información					
	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	1	1	2	1	1	1	2	1	1	1	2	1	1	1
2	5	5	5	4	4	4	5	5	5	4	5	4	5	5
3	2	2	2	2	1	2	1	1	2	2	1	2	2	2
4	3	2	4	2	3	2	5	2	2	3	3	2	3	4
5	3	4	3	3	3	3	3	*3*	*3*	2	4	3	3	3
6	4	3	4	4	5	4	4	5	4	5	4	4	4	3
7	2	2	2	3	1	1	2	1	3	2	2	1	2	2
8	1	2	1	1	1	1	1	2	1	1	1	2	1	1
9	4	2	4	4	4	5	4	4	4	3	3	3	3	4
10	1	2	1	1	1	1	3	1	2	1	2	1	1	1
11	5	1	2	3	1	1	1	4	1	4	1	4	1	1
12	1	2	1	2	1	1	1	2	1	1	1	2	1	1
13	2	3	4	3	4	5	4	4	4	5	2	1	3	3
14	1	2	2	3	2	2	3	1	2	1	2	3	2	1
15	1	2	2	2	2	1	2	2	3	2	2	2	2	2
16	2	3	4	1	1	4	1	2	4	1	1	4	1	3
17	5	4	4	5	5	4	5	4	4	5	4	5	5	5
18	3	2	2	2	2	2	2	2	2	1	2	2	2	2
19	4	4	4	5	5	5	5	4	4	5	5	5	5	4
20	3	4	3	2	3	3	3	2	4	3	3	2	4	3
21	4	4	4	3	4	3	5	4	4	3	4	5	4	2
22	1	2	1	1	1	2	1	2	1	1	2	1	1	2

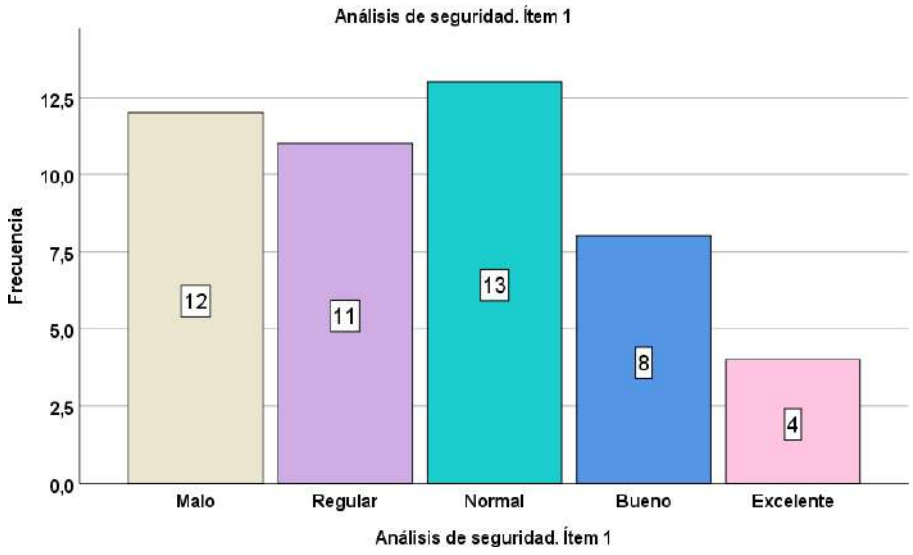
N°	GESTIÓN DE RIESGOS DE SEGURIDAD													
	Hardware				Software				Información					
	1	2	3	4	5	6	7	8	9	10	11	12	13	14
23	3	1	4	3	3	3	4	3	3	3	3	4	3	2
24	1	2	2	2	2	1	2	2	3	2	2	2	2	2
25	2	2	1	3	2	2	4	1	1	3	1	1	3	2
26	2	3	2	1	2	2	1	1	2	1	1	2	1	1
27	4	5	5	5	5	5	5	4	4	5	3	5	2	5
28	2	2	2	1	3	2	3	2	2	3	2	3	1	2
29	2	1	1	2	1	1	2	1	1	2	2	2	1	2
30	5	2	1	2	2	3	1	1	2	1	1	5	1	1
31	1	2	2	1	1	1	2	2	2	1	2	1	1	1
32	3	3	2	3	2	4	3	3	3	3	3	3	2	3
33	1	1	1	1	2	1	1	2	1	1	2	1	1	1
34	4	4	4	4	3	3	3	3	4	4	5	5	4	5
35	2	2	3	3	3	1	2	2	2	3	1	1	3	2
36	4	4	5	4	5	5	5	4	4	5	5	5	5	5
37	1	2	2	2	2	1	2	2	3	2	2	2	2	2
38	4	3	5	4	1	4	3	4	4	5	4	3	4	4
39	2	4	4	2	2	3	2	3	4	3	3	4	3	3
40	3	3	3	1	3	3	2	4	4	4	2	3	3	3
41	3	1	4	3	3	3	4	3	3	3	3	4	3	2
42	3	3	2	4	3	4	3	4	4	2	2	4	3	4
43	1	2	2	2	2	1	2	2	3	2	2	2	2	2
44	4	5	2	4	1	2	2	3	3	1	4	1	4	1
45	2	1	2	3	2	3	3	3	3	2	3	2	2	2
46	3	4	5	4	4	5	4	5	5	4	4	5	5	5
47	4	2	1	2	1	2	1	1	3	3	1	2	2	1
48	3	1	2	1	2	2	2	4	1	2	1	3	1	3

Anexo 05

Procesamiento de datos

Análisis de seguridad. Ítem 1. Calificación de la determinación del contexto en el área de ahorros con la aplicación de la metodología Magerit en MiBanco Huaraz 2023

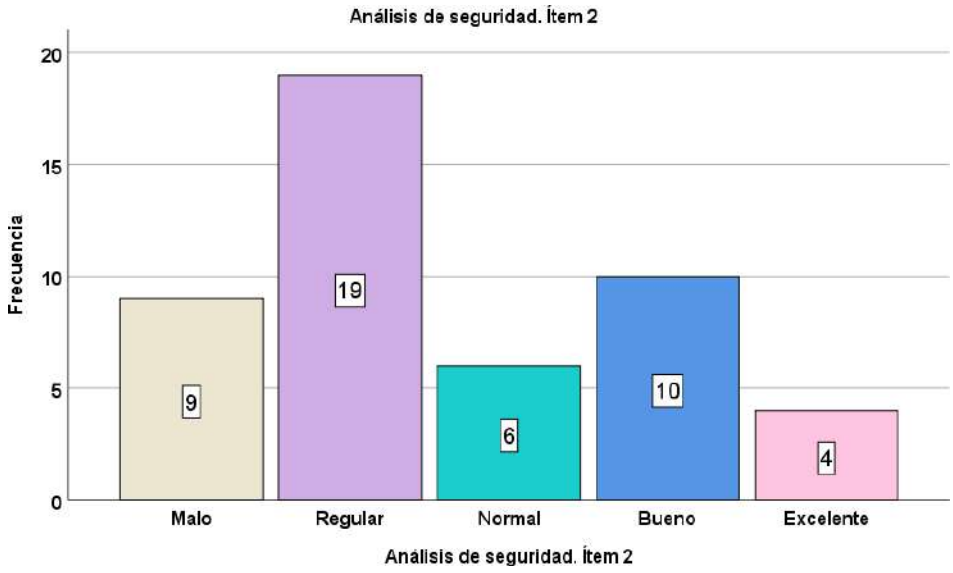
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	12	25,0	25,0	25,0
	Regular	11	22,9	22,9	47,9
	Normal	13	27,1	27,1	75,0
	Bueno	8	16,7	16,7	91,7
	Excelente	4	8,3	8,3	100,0
	Total	48	100,0	100,0	



Con referencia al ítem sobre la calificación de la determinación del contexto en el área de ahorros con la aplicación de la metodología Magerit en MiBanco Huaraz 2023 se tuvo que 12 activos informáticos (25.0%) fue calificado como malo, 11 de ellos (22.9%) se calificaron como regular, 13 activos informáticos (27.1%) sed calificaron como que fue normal, 8 de ellos (16.7%) calificaron como bueno y. 4 activos informáticos (8.3%) se calificaron como excelente.

Análisis de seguridad. Ítem 2. Consideración de la determinación del contexto en el área de créditos con la aplicación de la metodología Magerit en MiBanco Huaraz 2023

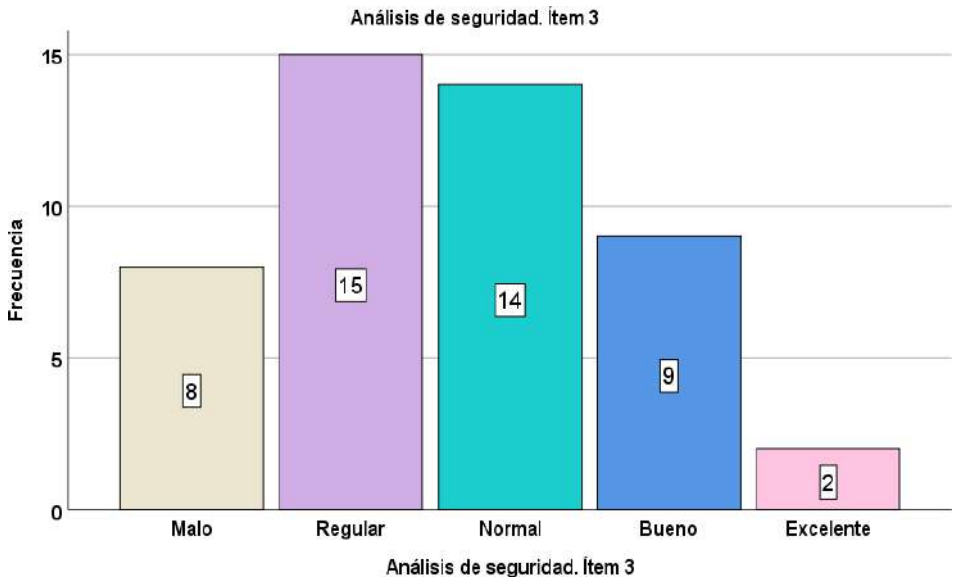
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	9	18,8	18,8	18,8
	Regular	19	39,6	39,6	58,3
	Normal	6	12,5	12,5	70,8
	Bueno	10	20,8	20,8	91,7
	Excelente	4	8,3	8,3	100,0
	Total	48	100,0	100,0	



Con referencia al ítem sobre la consideración de la determinación del contexto en el área de créditos con la aplicación de la metodología Magerit en MiBanco Huaraz 2023 se tuvo que 9 activos informáticos (18.8%) fueron considerados como malo, 19 de ellos (39.6%) se consideraron como regular, 6 activos informáticos (12.5%) consideraron como que fue normal, 10 de ellos (20.8%) se consideraron como bueno y 4 activos informáticos (8.3%) se consideraron como excelente.

Análisis de seguridad. Ítem 3. Evaluación de la determinación del contexto en el área de plataforma con la aplicación de la metodologia Magerit en MiBanco Huaraz 2023

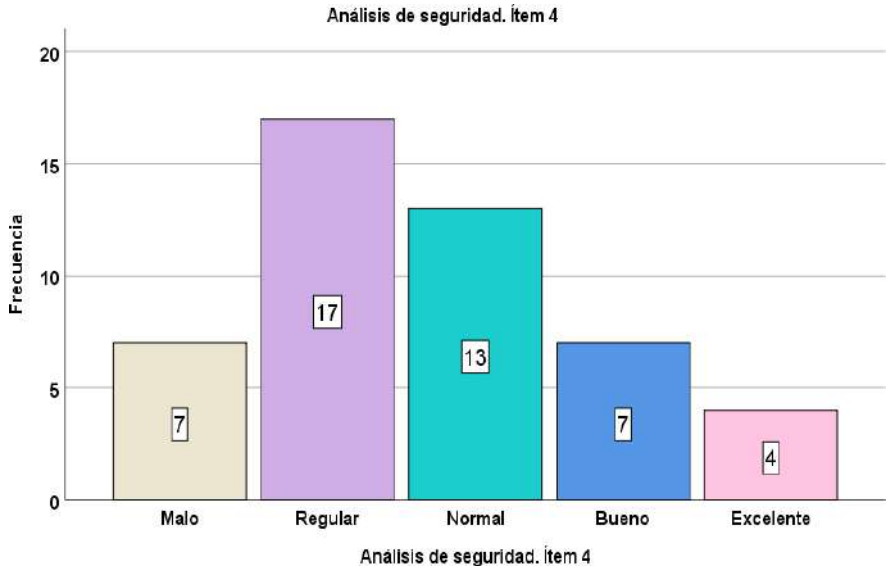
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	8	16,7	16,7	16,7
	Regular	15	31,3	31,3	47,9
	Normal	14	29,2	29,2	77,1
	Bueno	9	18,8	18,8	95,8
	Excelente	2	4,2	4,2	100,0
	Total	48	100,0	100,0	



Con referencia al ítem sobre la evaluación de la determinación del contexto en el área de plataforma con la aplicación de la metodologia Magerit en MiBanco Huaraz 2023, se tuvo que 8 activos informáticos (16.7%) fueron evaluados como malo, 15 de ellos (31.3%) se evaluaron como regular, 14 activos informáticos (29.2%) se evaluaron como que fue normal, 9 de ellos (18.8%) evaluaron como bueno y 2 activos informáticos (4.2%) se evaluaron como excelente.

Análisis de seguridad. Ítem 4. Valoración de la identificación de hardware con la aplicación de la metodología Magerit en MiBanco Huaraz 2023

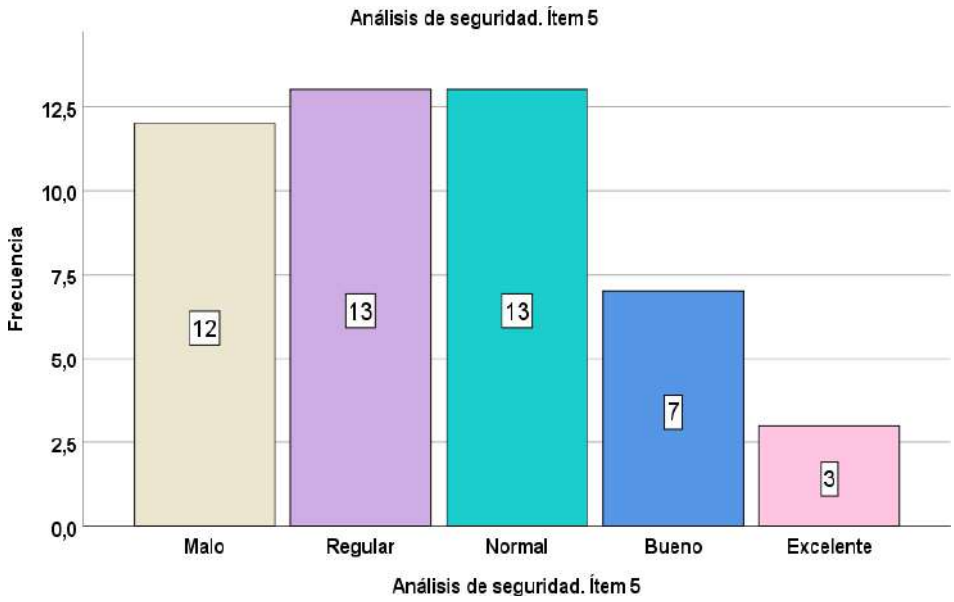
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	7	14,6	14,6	14,6
	Regular	17	35,4	35,4	50,0
	Normal	13	27,1	27,1	77,1
	Bueno	7	14,6	14,6	91,7
	Excelente	4	8,3	8,3	100,0
	Total	48	100,0	100,0	



Con referencia al ítem sobre la valoración de la identificación de hardware con la aplicación de la metodología Magerit en MiBanco Huaraz 2023, se tuvo que 7 activos informáticos (14.6%) fueron valorados como malo, 17 de ellos (35.4%) se valoraron como regular, 13 activos informáticos (27.1%) se valoraron como que fue normal, 7 de ellos (14.6%) se valoraron como bueno y 4 activos informáticos (8.3%) se valoraron como excelente.

Análisis de seguridad. Ítem 5. Calificación de la identificación de software con la aplicación de la metodología Magerit en MiBanco Huaraz 2023

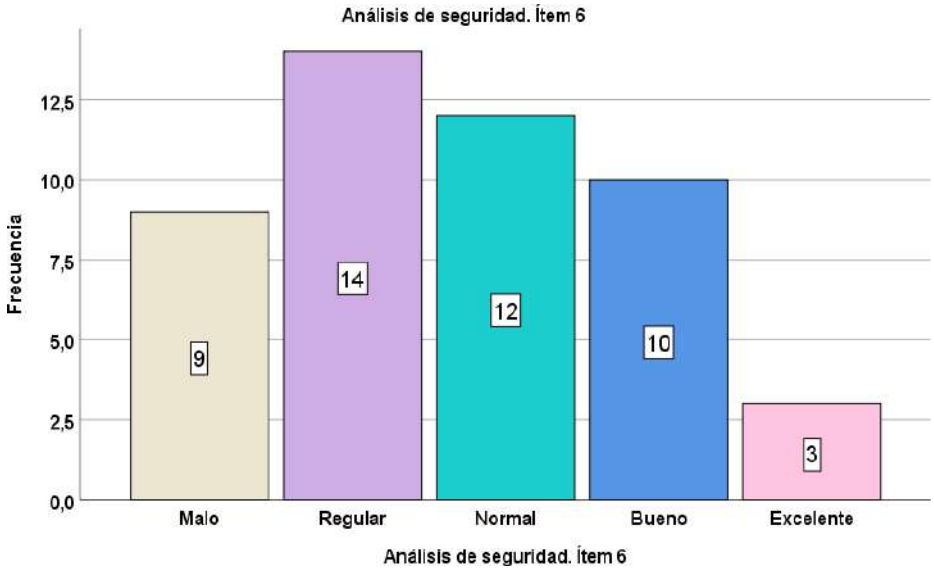
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	12	25,0	25,0	25,0
	Regular	13	27,1	27,1	52,1
	Normal	13	27,1	27,1	79,2
	Bueno	7	14,6	14,6	93,8
	Excelente	3	6,3	6,3	100,0
	Total	48	100,0	100,0	



Con referencia al ítem sobre la calificación de la identificación de software con la aplicación de la metodología Magerit en MiBanco Huaraz 2023, se tuvo que 12 activos informáticos (25.0%) fueron calificados como malo, 13 de ellos (27.1%) calificaron como regular, 13 activos informáticos (27.1%) se calificaron como que fue normal, 7 de ellos (14.6%) se calificaron como bueno y 3 activos informáticos (6.3%) se calificaron como excelente.

Análisis de seguridad. Ítem 6. Consideración de la identificación de la información con la aplicación de la metodología Magerit en MiBanco Huaraz 2023

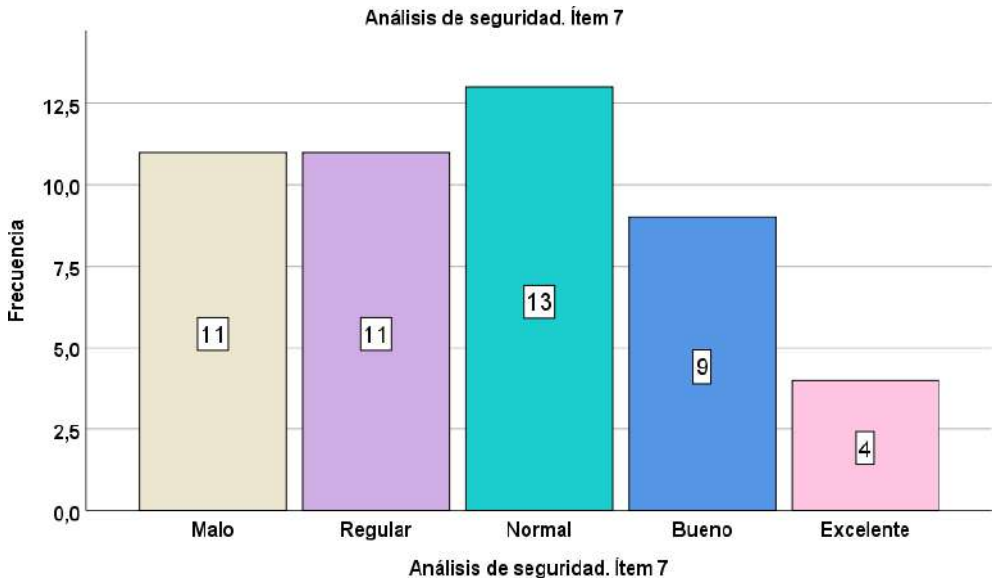
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	9	18,8	18,8	18,8
	Regular	14	29,2	29,2	47,9
	Normal	12	25,0	25,0	72,9
	Bueno	10	20,8	20,8	93,8
	Excelente	3	6,3	6,3	100,0
	Total	48	100,0	100,0	



Con referencia al ítem sobre la consideración de la identificación de la información con la aplicación de la metodología Magerit en MiBanco Huaraz 2023, se tuvo que 9 activos informáticos (18.8%) se consideraron como malo, 14 de ellos (29.2%) consideraron como regular, 12 activos informáticos (25.0%) se consideraron como que fue normal, 10 de ellos (20.8%) se consideraron como bueno y 3 activos informáticos (6.3%) se consideraron como excelente.

Análisis de seguridad. Ítem 7. Calificación de la identificación de amenazas al hardware con la aplicación de la metodología Magerit en MiBanco Huaraz 2023

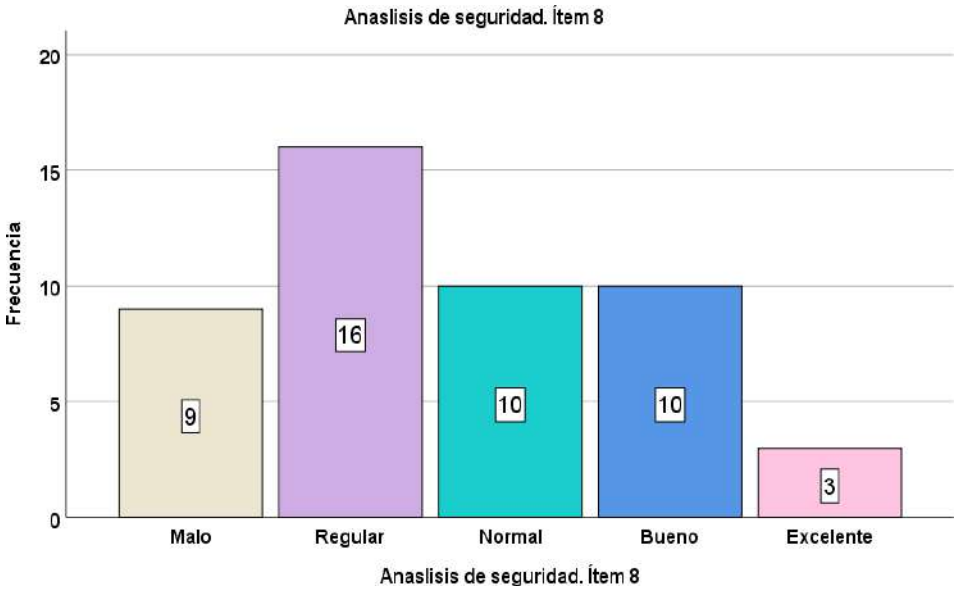
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	11	22,9	22,9	22,9
	Regular	11	22,9	22,9	45,8
	Normal	13	27,1	27,1	72,9
	Bueno	9	18,8	18,8	91,7
	Excelente	4	8,3	8,3	100,0
	Total	48	100,0	100,0	



Con referencia al ítem sobre la calificación de la identificación de amenazas al hardware con la aplicación de la metodología Magerit en MiBanco Huaraz 2023, se tuvo que 11 activos informáticos (22.9%) se calificaron como malo, 11 de ellos (22.9%) se calificaron como regular, 13 encuestados (27.1%) se calificaron como que fue normal, 9 de ellos (18.8%) se calificaron como bueno y 4 activos informáticos (8.3%) se calificaron como excelente.

Análisis de seguridad. Ítem 8. Consideración de la identificación de amenazas al software con la aplicación de la metodología Magerit en MiBanco Huaraz 2023

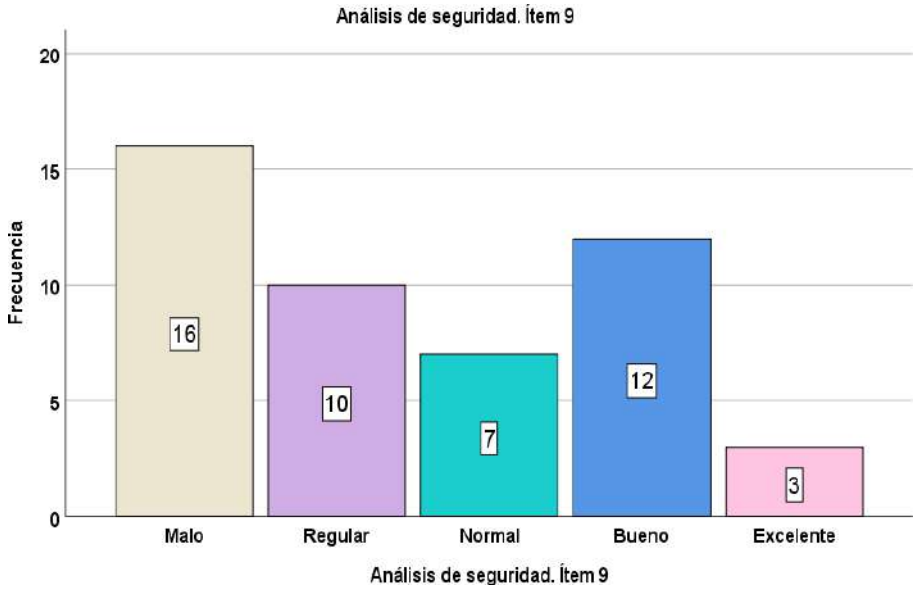
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	9	18,8	18,8	18,8
	Regular	16	33,3	33,3	52,1
	Normal	10	20,8	20,8	72,9
	Bueno	10	20,8	20,8	93,8
	Excelente	3	6,3	6,3	100,0
	Total	48	100,0	100,0	



Con referencia al ítem sobre la consideración de la identificación de amenazas al software con la aplicación de la metodología Magerit en MiBanco Huaraz 2023, se tuvo que 9 activos informáticos (18.8%) se consideraron como malo, 16 de ellos (33.3%) se consideraron como regular, 10 activos informáticos (20.8%) se consideraron como que fue normal, 10 de ellos (20.8%) se consideraron como bueno y 3 activos informáticos (6.3%) se consideraron como excelente.

Análisis de seguridad. Ítem 9. Evaluacion de la identificación de amenazas a la información con la aplicación de la metodología Magerit en MiBanco Huaraz 2023

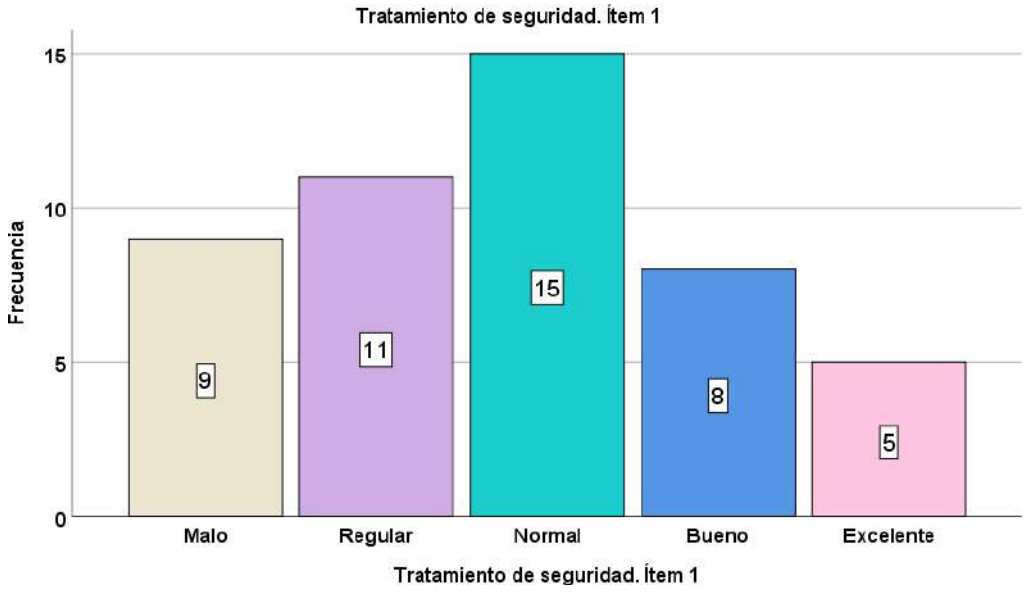
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	16	33,3	33,3	33,3
	Regular	10	20,8	20,8	54,2
	Normal	7	14,6	14,6	68,8
	Bueno	12	25,0	25,0	93,8
	Excelente	3	6,3	6,3	100,0
	Total	48	100,0	100,0	



Con referencia al ítem sobre la evaluación de la identificación de amenazas a la información con la aplicación de la metodología Magerit en MiBanco Huaraz 2023, se tuvo que 16 activos informáticos (33.3%) se evaluaron como malo, 10 de ellos (20.8%) se evaluaron como regular, 7 activos informáticos (14.6%) consideraron como que fue normal, 12 de ellos (25.0%) se evaluaron como bueno y 3 activos informáticos (6.3%) se evaluaron como excelente.

Tratamiento de seguridad. Ítem 1. Calificación del tratamiento de la seguridad del sistema operativo en MiBanco Huaraz 2023

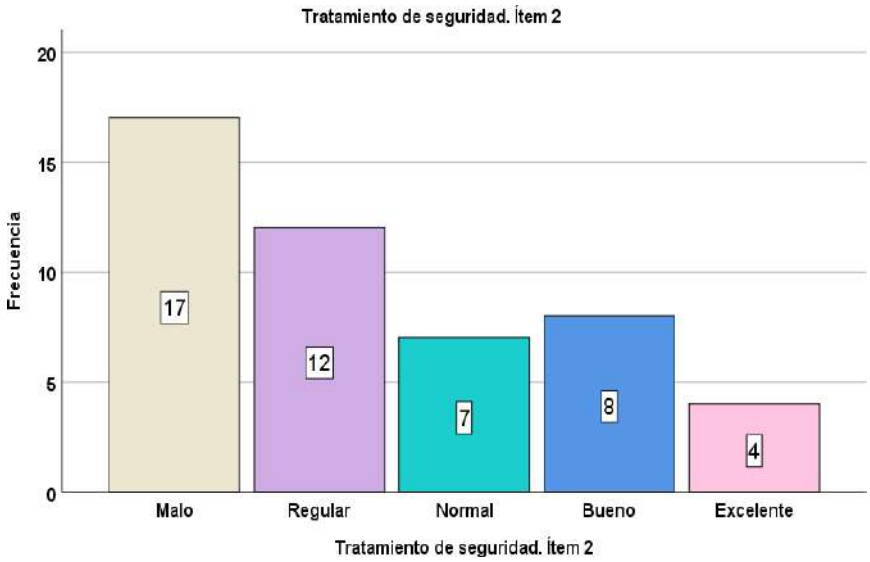
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	9	18,8	18,8	18,8
	Regular	11	22,9	22,9	41,7
	Normal	15	31,3	31,3	72,9
	Bueno	8	16,7	16,7	89,6
	Excelente	5	10,4	10,4	100,0
	Total	48	100,0	100,0	



Con referencia al ítem sobre la calificación del tratamiento de la seguridad del sistema operativo en MiBanco Huaraz 2023, se tuvo que 9 activos informáticos (18.8%) se calificaron como malo, 11 de ellos (22.9%) se calificaron como regular, 15 activos informáticos (31.3%) se calificaron como que fue normal, 8 de ellos (16.7%) se calificaron como bueno y 5 activos informáticos (10.4%) se calificaron como excelente.

Tratamiento de seguridad. Ítem 2. Consideración el tratamiento de la seguridad del software antivirus en MiBanco Huaraz 2023

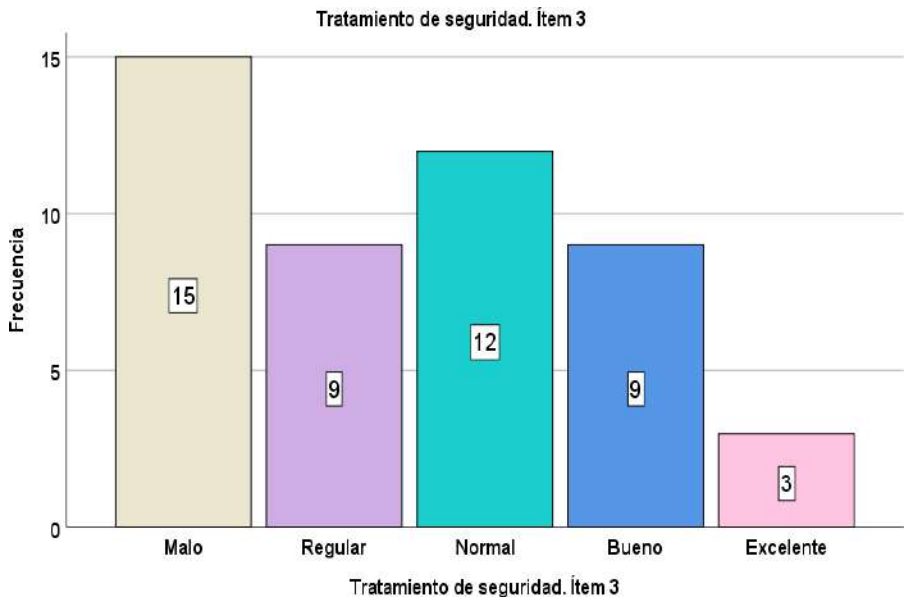
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	17	35,4	35,4	35,4
	Regular	12	25,0	25,0	60,4
	Normal	7	14,6	14,6	75,0
	Bueno	8	16,7	16,7	91,7
	Excelente	4	8,3	8,3	100,0
	Total	48	100,0	100,0	



Con referencia al ítem sobre la consideración del tratamiento de la seguridad del software antivirus en MiBanco Huaraz 2023, se tuvo que 17 activos informáticos (35.4%) se consideraron como malo, 12 de ellos (25.0%) se consideraron como regular, 7 activos informáticos (14.6%) se consideraron como que fue normal, 8 de ellos (16.7%) se consideraron como bueno y 4 activos informáticos (8.3%) se consideraron como excelente.

Tratamiento de seguridad. Ítem 3. Evaluación del tratamiento de la seguridad de software financiero en MiBanco Huaraz 2023

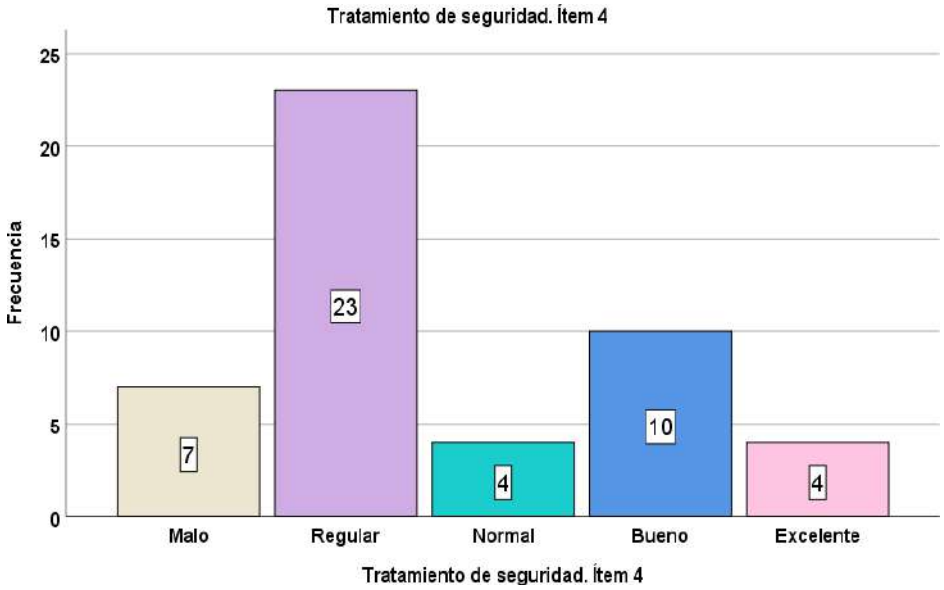
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	15	31,3	31,3	31,3
	Regular	9	18,8	18,8	50,0
	Normal	12	25,0	25,0	75,0
	Bueno	9	18,8	18,8	93,8
	Excelente	3	6,3	6,3	100,0
	Total	48	100,0	100,0	



Con referencia al ítem sobre la evaluación del tratamiento de la seguridad de software financiero en MiBanco Huaraz 2023, se tuvo que 15 activos informáticos (31.3%) se evaluaron como malo, 9 de ellos (18.8%) se evaluaron como regular, 12 activos informáticos (25.0%) se evaluaron como que fue normal, 9 de ellos (18.8%) se evaluaron como bueno y 3 activos informáticos (6.3%) se evaluaron como excelente.

Tratamiento de seguridad. Ítem 4. Valoración del tratamiento de la seguridad de la información en MiBanco Huaraz 2023

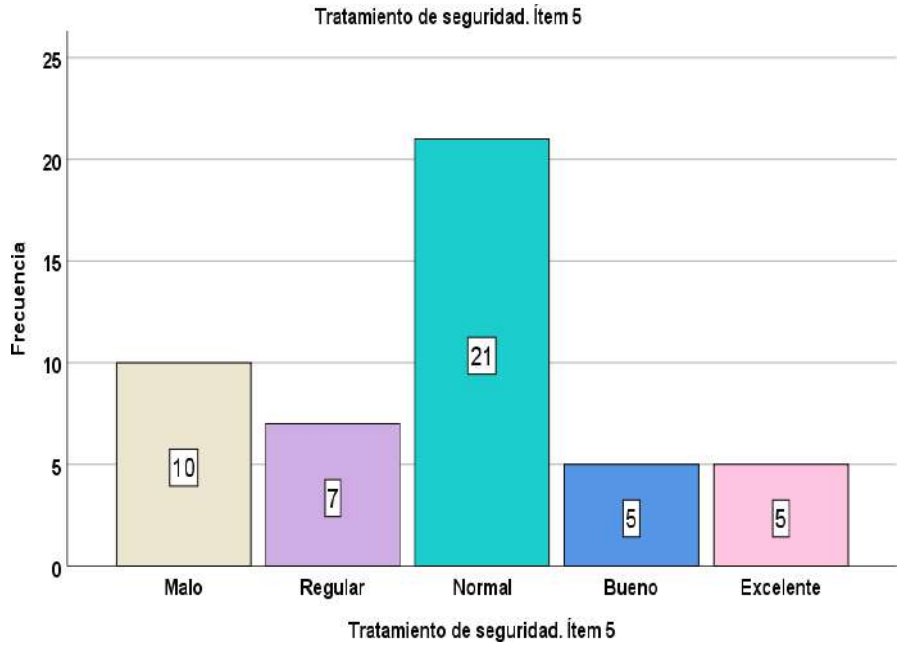
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	7	14,6	14,6	14,6
	Regular	23	47,9	47,9	62,5
	Normal	4	8,3	8,3	70,8
	Bueno	10	20,8	20,8	91,7
	Excelente	4	8,3	8,3	100,0
	Total	48	100,0	100,0	



Con referencia al ítem sobre la valoración del tratamiento de la seguridad de la información en MiBanco Huaraz 2023, se tuvo que 7 activos informáticos (14.6%) se evaluaron como malo, 23 de ellos (47.9%) se evaluaron como regular, 4 activos informáticos (8.3%) se evaluaron como que fue normal, 10 de ellos (20.8%) evaluaron como bueno y 4 activos informáticos (8.3%) se evaluaron como excelente.

Tratamiento de seguridad. Ítem 5. Calificación del tratamiento de la seguridad de las computadoras clientes en MiBanco Huaraz 2023

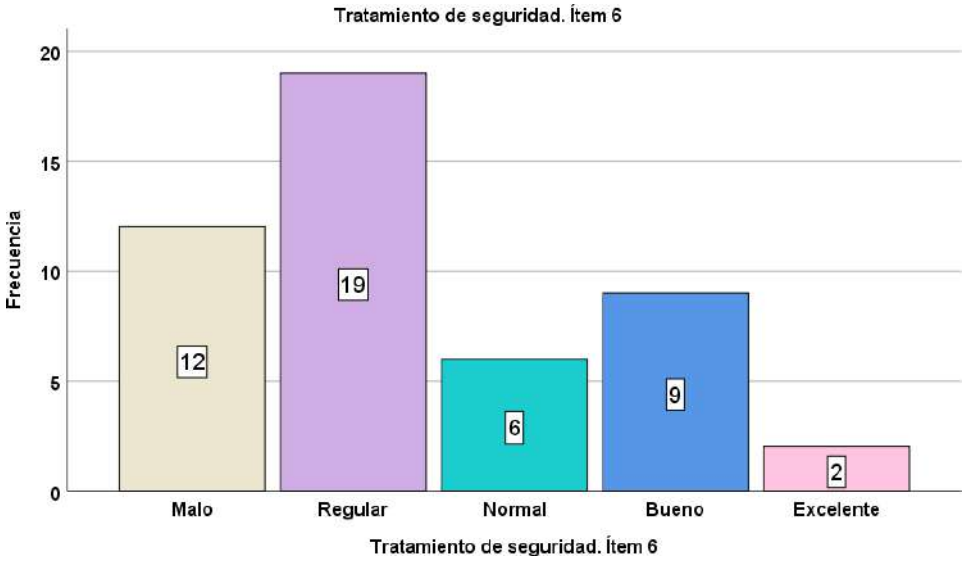
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	10	20,8	20,8	20,8
	Regular	7	14,6	14,6	35,4
	Normal	21	43,8	43,8	79,2
	Bueno	5	10,4	10,4	89,6
	Excelente	5	10,4	10,4	100,0
	Total	48	100,0	100,0	



Con referencia al ítem sobre la calificación del tratamiento de la seguridad de las computadoras clientes en MiBanco Huaraz 2023, se tuvo que 10 activos informáticos (20.8%) se calificaron como malo, 7 de ellos (14.6%) se calificaron como regular, 21 activos informáticos 43.8%) se calificaron como que fue normal, 5 de ellos (10.4%) se calificaron como bueno y 5 activos informáticos (10.4%) se calificaron como excelente.

Tratamiento de seguridad. Ítem 6. Consideración del tratamiento de la seguridad del servidor en MiBanco Huaraz 2023

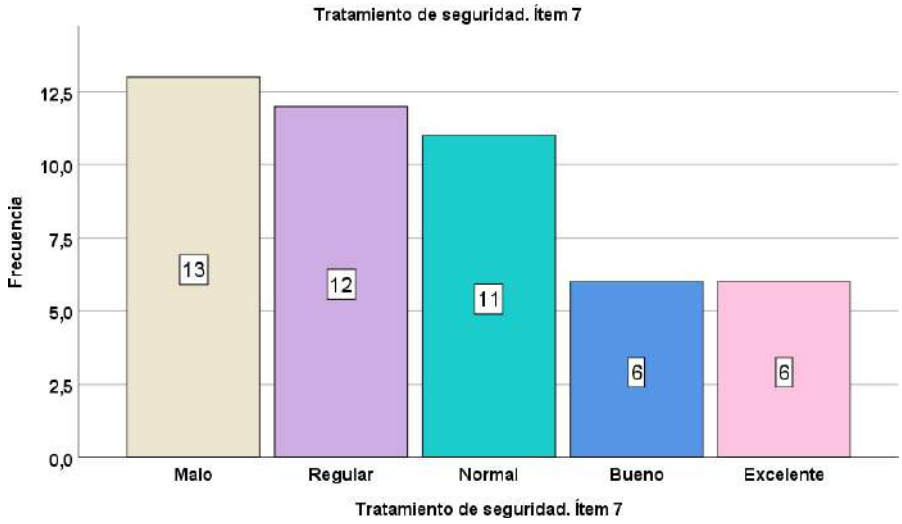
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	12	25,0	25,0	25,0
	Regular	19	39,6	39,6	64,6
	Normal	6	12,5	12,5	77,1
	Bueno	9	18,8	18,8	95,8
	Excelente	2	4,2	4,2	100,0
	Total	48	100,0	100,0	



Con referencia al ítem sobre la consideración del tratamiento de la seguridad del servidor en MiBanco Huaraz 2023, se tuvo que 12 activos informáticos (25.0%) se consideraron como malo, 19 de ellos (39.6%) se consideraron como regular, 6 activos informáticos (12.5%) se consideraron como que fue normal, 9 de ellos (18.8%) se consideraron como bueno y 2 activos informáticos (4.2%) se consideraron como excelente.

Tratamiento de seguridad. Ítem 7. Evaluación del tratamiento de la seguridad de hardware de conectividad de Internet en MiBanco Huaraz 2023

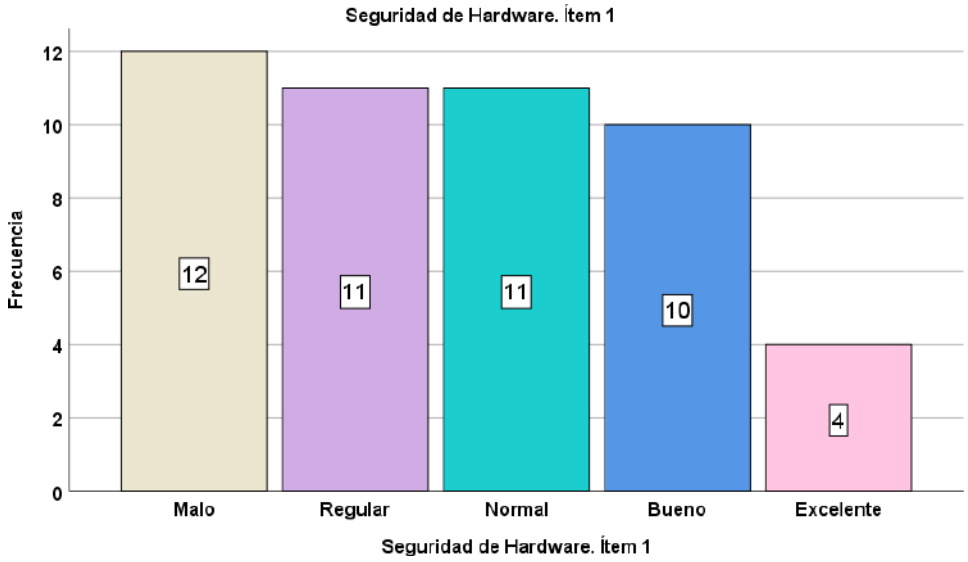
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	13	27,1	27,1	27,1
	Regular	12	25,0	25,0	52,1
	Normal	11	22,9	22,9	75,0
	Bueno	6	12,5	12,5	87,5
	Excelente	6	12,5	12,5	100,0
	Total	48	100,0	100,0	



Con referencia al ítem sobre la evaluación del tratamiento de la seguridad de hardware de conectividad de Internet en MiBanco Huaraz 2023, se tuvo que 13 activos informáticos (27.1%) se evaluaron como malo, 12 de ellos (25.0%) se evaluaron como regular, 11 activos informáticos (22.9%) se evaluaron como que fue normal, 6 de ellos (12.5%) se evaluaron como bueno y 6 activos informáticos (12.5%) se evaluaron como excelente.

Seguridad de Hardware. Ítem 1. Calificación de la gestión de riesgo de seguridad del servidor en MiBanco Huaraz 2023

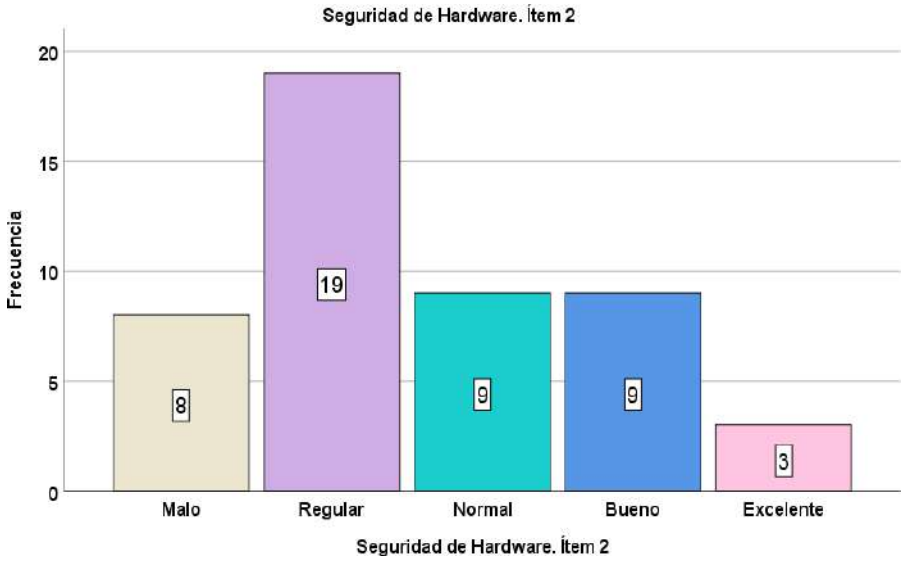
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	12	25,0	25,0	25,0
	Regular	11	22,9	22,9	47,9
	Normal	11	22,9	22,9	70,8
	Bueno	10	20,8	20,8	91,7
	Excelente	4	8,3	8,3	100,0
	Total	48	100,0	100,0	



Con referencia al ítem sobre la calificación de la gestión de riesgo de seguridad del servidor en MiBanco Huaraz 2023, se tuvo que 12 activos informáticos (25.0%) calificaron como malo, 11 de ellos (22.9%) se calificaron como regular, 11 activos informáticos (22.9%) se calificaron como que fue normal, 10 de ellos (20.8%) se calificaron como bueno y 4 activos informáticos (8.3%) se calificaron como excelente.

Seguridad de Hardware. Ítem 2. Calificación de la gestión de riesgo de seguridad de las computadoras en MiBanco Huaraz 2023

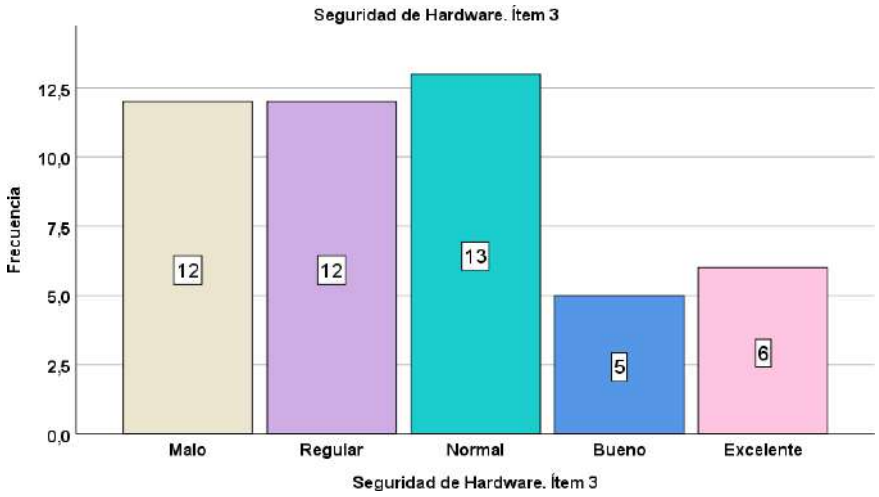
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	8	16,7	16,7	16,7
	Regular	19	39,6	39,6	56,3
	Normal	9	18,8	18,8	75,0
	Bueno	9	18,8	18,8	93,8
	Excelente	3	6,3	6,3	100,0
	Total	48	100,0	100,0	



Con referencia al ítem sobre la calificación de la gestión de riesgo de seguridad de las computadoras en MiBanco Huaraz 2023, se tuvo que 8 activos informáticos (16.7%) se calificaron como malo, 19 de ellos (39.6%) se calificaron como regular, 9 activos informáticos (18.8%) se calificaron como que fue normal, 9 de ellos (18.8%) se calificaron como bueno y 3 activos informáticos (6.3%) se calificaron como excelente.

Seguridad de Hardware. Ítem 3. Calificación de la gestión de riesgo de seguridad del hardware de conectividad de Internet en MiBanco Huaraz 2023

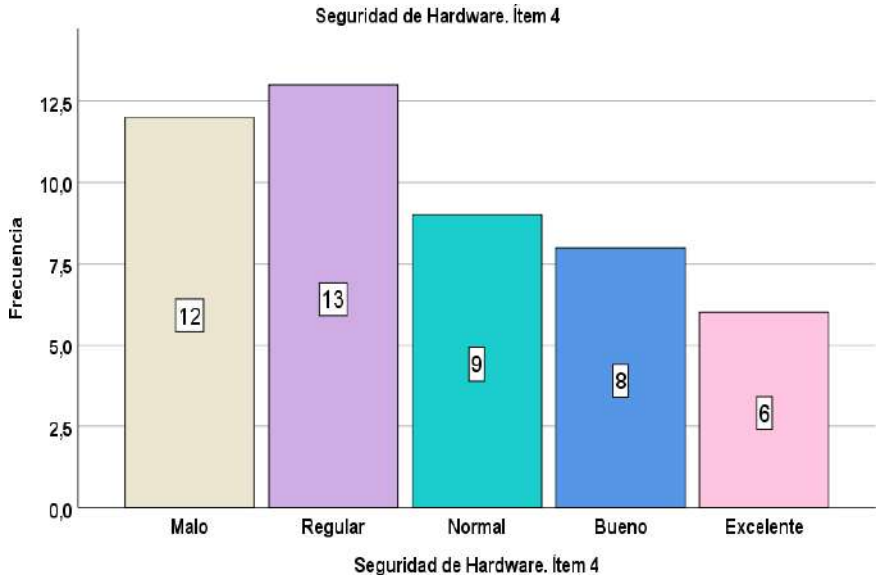
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	12	25,0	25,0	25,0
	Regular	12	25,0	25,0	50,0
	Normal	13	27,1	27,1	77,1
	Bueno	5	10,4	10,4	87,5
	Excelente	6	12,5	12,5	100,0
	Total	48	100,0	100,0	



Con referencia al ítem sobre la calificación de la gestión de riesgo de seguridad del hardware de conectividad de Internet en MiBanco Huaraz 2023, se tuvo que 12 activos informáticos (25.0%) se calificaron como malo, 12 de ellos (25.0%) se calificaron como regular, 13 activos informáticos (27.1%) se calificaron como que fue normal, 5 de ellos (10.4%) se calificaron como bueno y 6 activos informáticos (12.5%) se calificaron como excelente.

Seguridad de Hardware. Ítem 4. Calificación de la gestión de riesgo de seguridad de impresoras en MiBanco Huaraz 2023

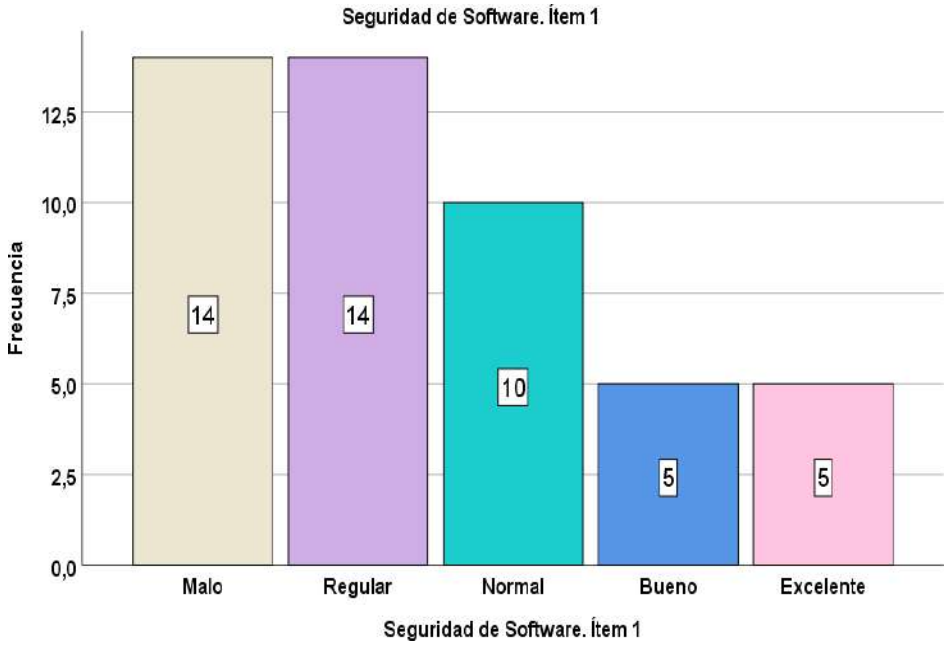
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	12	25,0	25,0	25,0
	Regular	13	27,1	27,1	52,1
	Normal	9	18,8	18,8	70,8
	Bueno	8	16,7	16,7	87,5
	Excelente	6	12,5	12,5	100,0
	Total	48	100,0	100,0	



Con referencia al ítem sobre la calificación de la gestión de riesgo de seguridad de impresoras en MiBanco Huaraz 2023, se tuvo que 12 activos informáticos (25.0%) se calificaron como malo, 13 de ellos (27.1%) se calificaron como regular, 9 activos informáticos (18.8%) se calificaron como que fue normal, 8 de ellos (16.7%) se calificaron como bueno y 6 activos informáticos (12.5%) se calificaron como excelente.

Seguridad de Software. Ítem 1. Consideración del tratamiento de la seguridad del sistema operativo en MiBanco Huaraz 2023

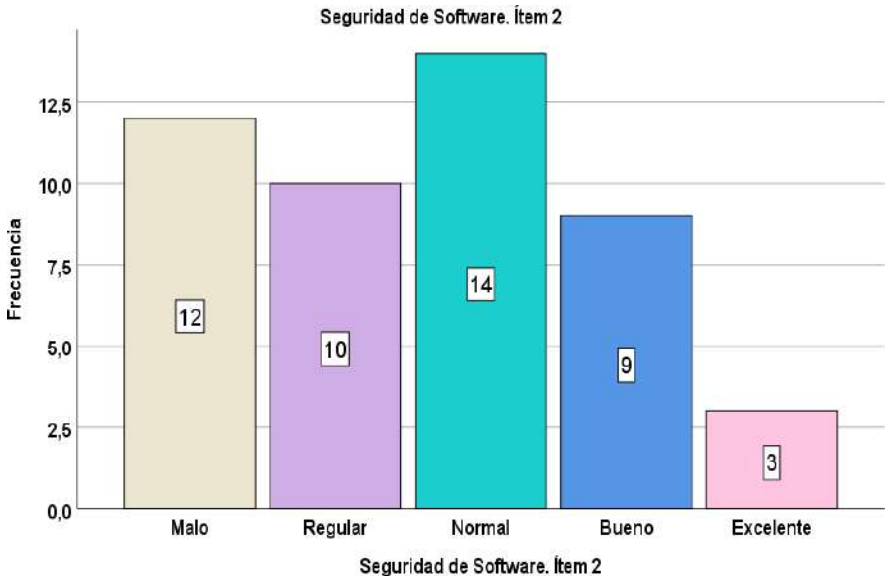
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	14	29,2	29,2	29,2
	Regular	14	29,2	29,2	58,3
	Normal	10	20,8	20,8	79,2
	Bueno	5	10,4	10,4	89,6
	Excelente	5	10,4	10,4	100,0
	Total	48	100,0	100,0	



Con referencia al ítem sobre la consideración del tratamiento de la seguridad del sistema operativo en MiBanco Huaraz 2023, se tuvo que 14 activos informáticos (29.2%) se consideraron como malo, 14 de ellos (29.2%) se consideraron como regular, 10 activos informáticos (20.8%) se consideraron como que fue normal, 5 de ellos (10.4%) se consideraron como bueno y 5 activos informáticos (10.4%) se consideraron como excelente.

Seguridad de Software. Ítem 2. Consideración del tratamiento de la seguridad del software antivirus en MiBanco Huaraz 2023

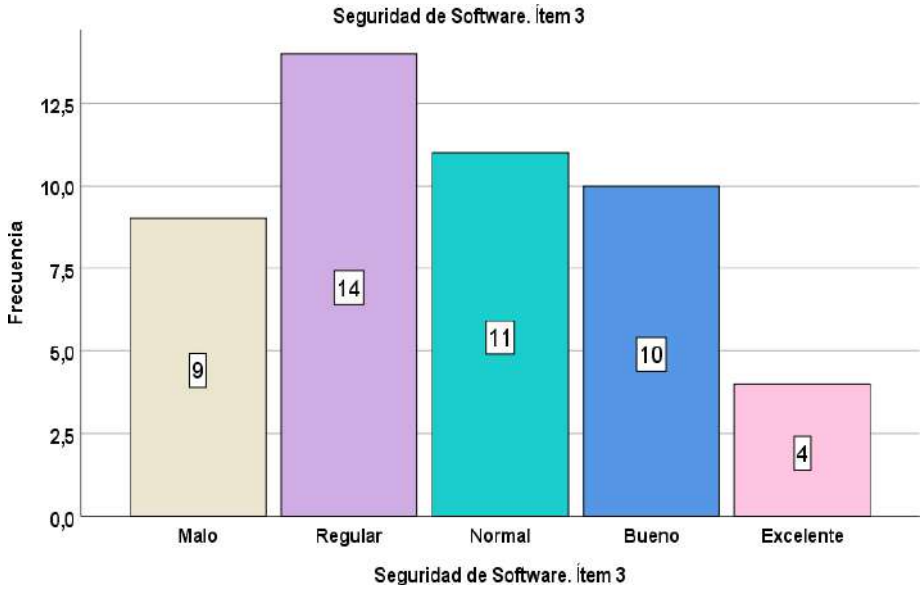
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	12	25,0	25,0	25,0
	Regular	10	20,8	20,8	45,8
	Normal	14	29,2	29,2	75,0
	Bueno	9	18,8	18,8	93,8
	Excelente	3	6,3	6,3	100,0
	Total	48	100,0	100,0	



Con referencia al ítem sobre la consideración del tratamiento de la seguridad del software antivirus en MiBanco Huaraz 2023, se tuvo que 12 activos informáticos (25.0%) se consideraron como malo, 10 de ellos (20.8%) se consideraron como regular, 14 activos informáticos (29.2%) se consideraron como que fue normal, 9 de ellos (18.8%) se consideraron como bueno y 3 activos informáticos (6.3%) se consideraron como excelente.

Seguridad de Software. Ítem 3. Consideración del tratamiento de la seguridad del software financiero en MiBanco Huaraz 2023

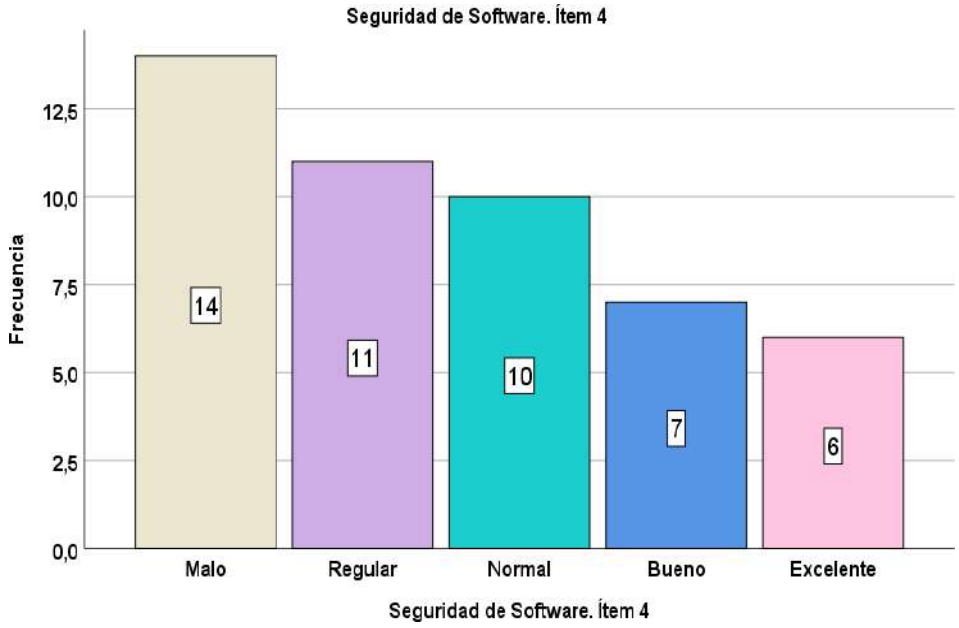
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	9	18,8	18,8	18,8
	Regular	14	29,2	29,2	47,9
	Normal	11	22,9	22,9	70,8
	Bueno	10	20,8	20,8	91,7
	Excelente	4	8,3	8,3	100,0
	Total	48	100,0	100,0	



Con referencia al ítem sobre la consideración del tratamiento de la seguridad del software financiero en MiBanco Huaraz 2023, se tuvo que 9 activos informáticos (18.8%) se consideraron como malo, 14 de ellos (29.2%) se consideraron como regular, 11 activos informáticos (22.9%) se consideraron como que fue normal, 10 de ellos (20.8%) se consideraron como bueno y 4 activos informáticos (8.3%) se consideraron como excelente.

Seguridad de Software. Ítem 4. Consideración del tratamiento de la seguridad del software de oficina en MiBanco Huaraz 2023

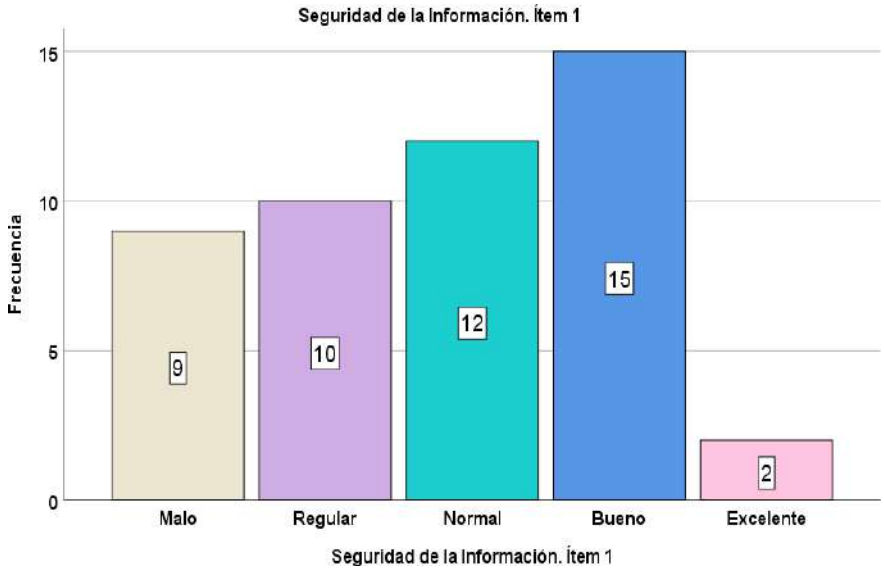
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	14	29,2	29,2	29,2
	Regular	11	22,9	22,9	52,1
	Normal	10	20,8	20,8	72,9
	Bueno	7	14,6	14,6	87,5
	Excelente	6	12,5	12,5	100,0
	Total	48	100,0	100,0	



Con referencia al ítem sobre la consideración del tratamiento de la seguridad del software de oficina en MiBanco Huaraz 2023, se tuvo que 14 activos informáticos (29.2%) se consideraron como malo, 11 de ellos (22.9%) se consideraron como regular, 10 activos informáticos (20.8%) se consideraron como que fue normal, 7 de ellos (14.6%) se consideraron como bueno y 6 activos informáticos (12.5%) se consideraron como excelente.

Seguridad de la Información. Ítem 1. Consideración del tratamiento de la seguridad de la información financiera de importancia en el área de ahorros en MiBanco Huaraz 2023

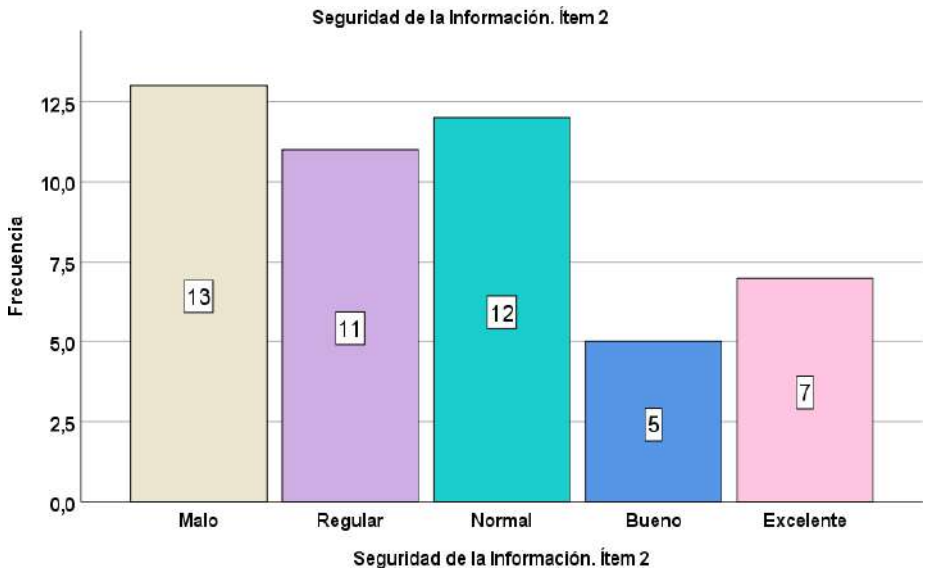
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	9	18,8	18,8	18,8
	Regular	10	20,8	20,8	39,6
	Normal	12	25,0	25,0	64,6
	Bueno	15	31,3	31,3	95,8
	Excelente	2	4,2	4,2	100,0
	Total	48	100,0	100,0	



Con referencia al ítem sobre la consideración del tratamiento de la seguridad de la información financiera de importancia en el área de ahorros en MiBanco Huaraz 2023, se tuvo que 9 activos informáticos (18.8%) se consideraron como malo, 10 de ellos (20.8%) se consideraron como regular, 12 activos informáticos (25.0%) se consideraron como que fue normal, 15 de ellos (31.3%) se consideraron como bueno y 2 activos informáticos (4.2%) se consideraron como excelente.

Seguridad de la Información. Ítem 2. Consideración del tratamiento de la seguridad de la información financiera de importancia en el área de créditos en MiBanco Huaraz 2023

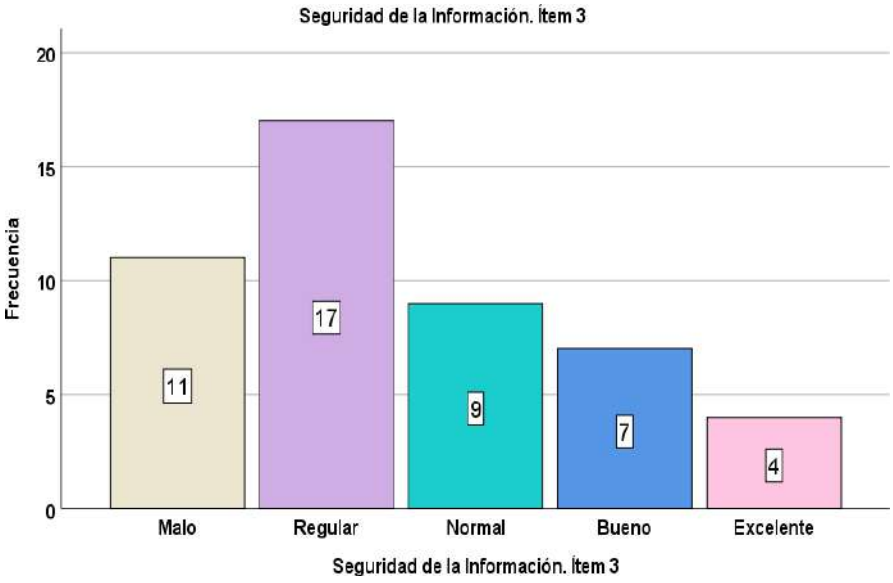
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	13	27,1	27,1	27,1
	Regular	11	22,9	22,9	50,0
	Normal	12	25,0	25,0	75,0
	Bueno	5	10,4	10,4	85,4
	Excelente	7	14,6	14,6	100,0
	Total	48	100,0	100,0	



Con referencia al ítem sobre la consideración del tratamiento de la seguridad de la información financiera de importancia en el área de créditos en MiBanco Huaraz 2023, se tuvo que 13 activos informáticos (27.1%) se consideraron como malo, 11 de ellos (22.9%) consideraron como regular, 12 activos informáticos (25.0%) se consideraron como que fue normal, 5 de ellos (10.4%) se consideraron como bueno y 7 activos informáticos (14.6%) se consideraron como excelente.

Seguridad de la Información. Ítem 3. Consideración del tratamiento de la seguridad de la base de datos en MiBanco Huaraz 2023

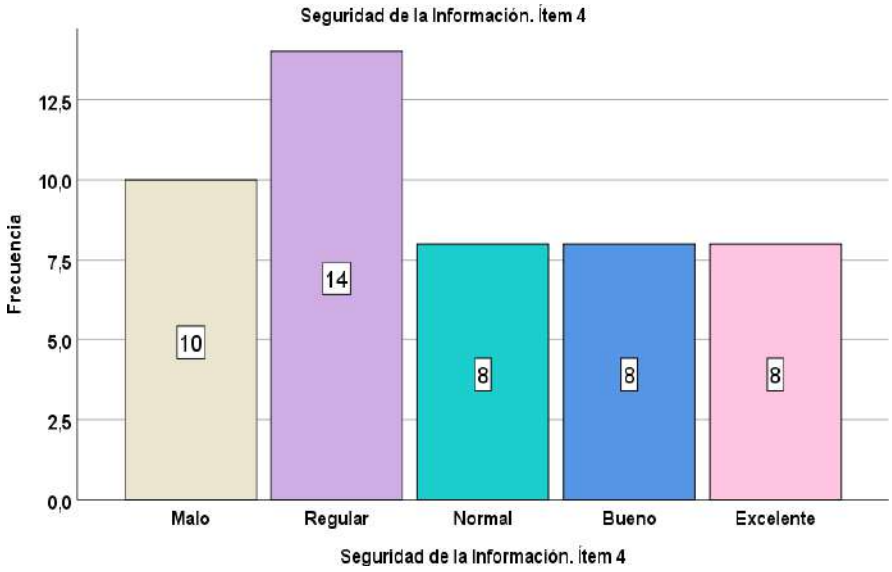
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	11	22,9	22,9	22,9
	Regular	17	35,4	35,4	58,3
	Normal	9	18,8	18,8	77,1
	Bueno	7	14,6	14,6	91,7
	Excelente	4	8,3	8,3	100,0
	Total	48	100,0	100,0	



Con referencia al ítem sobre la consideración del tratamiento de la seguridad de la base de datos en MiBanco Huaraz 2023, se tuvo que 11 activos informáticos (22.9%) se consideraron como malo, 17 de ellos (35.4%) se consideraron como regular, 9 activos informáticos (18.8%) se consideraron como que fue normal, 7 de ellos (14.6%) se consideraron como bueno y 4 activos informáticos (8.3%) se consideraron como excelente.

Seguridad de la Información. Ítem 4. Consideración del tratamiento de la seguridad del acceso a Internet en MiBanco Huaraz 2023

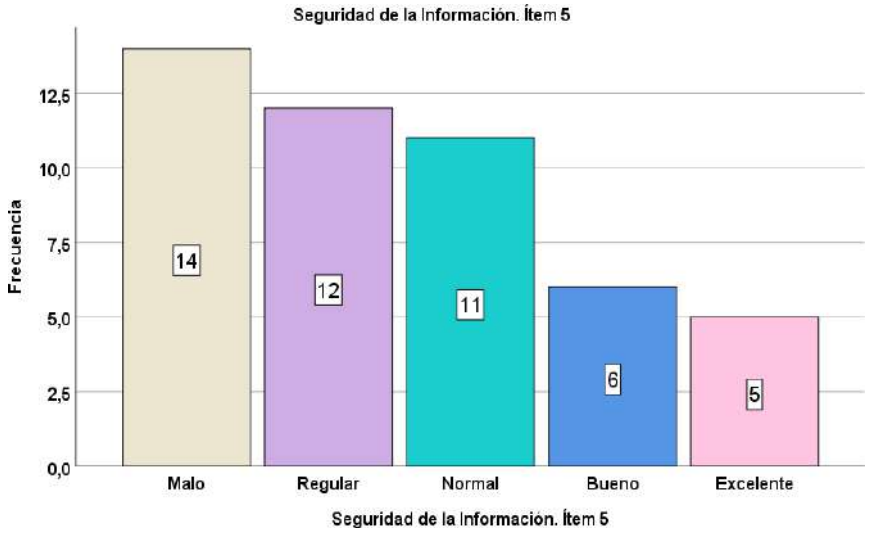
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	10	20,8	20,8	20,8
	Regular	14	29,2	29,2	50,0
	Normal	8	16,7	16,7	66,7
	Bueno	8	16,7	16,7	83,3
	Excelente	8	16,7	16,7	100,0
	Total	48	100,0	100,0	



Con referencia al ítem sobre la consideración del tratamiento de la seguridad del acceso a Internet en MiBanco Huaraz 2023, se tuvo que 10 activos informáticos (20.8%) se consideraron como malo, 14 de ellos (29.2%) se consideraron como regular, 8 activos informáticos (16.7%) se consideraron como que fue normal, 8 de ellos (16.7%) se consideraron como bueno y 8 activos informáticos (16.7%) se consideraron como excelente.

Seguridad de la Información. Ítem 5. Consideración del tratamiento de la seguridad del acceso a las redes sociales en MiBanco Huaraz 2023

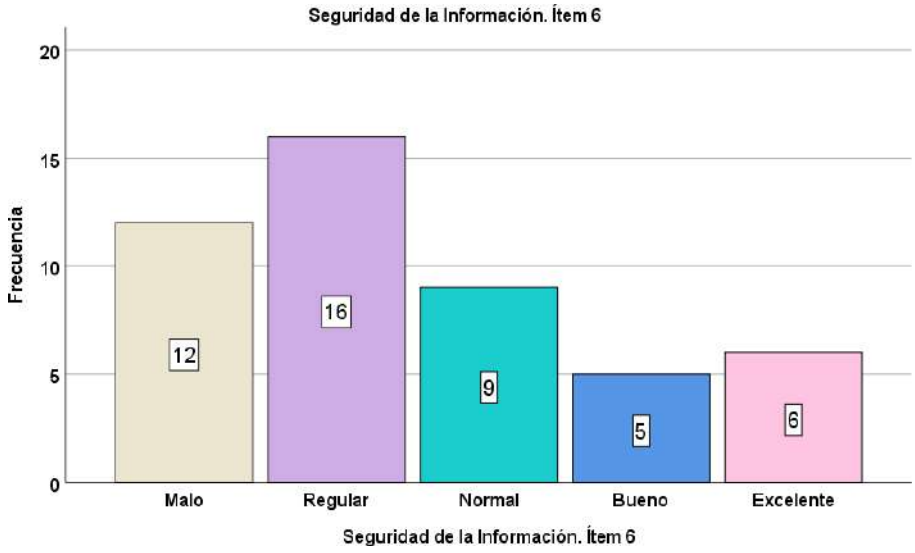
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	14	29,2	29,2	29,2
	Regular	12	25,0	25,0	54,2
	Normal	11	22,9	22,9	77,1
	Bueno	6	12,5	12,5	89,6
	Excelente	5	10,4	10,4	100,0
	Total	48	100,0	100,0	



Con referencia al ítem sobre la consideración del tratamiento de la seguridad del acceso a las redes sociales en MiBanco Huaraz 2023, se tuvo que 14 activos informáticos (29.2%) se consideraron como malo, 12 de ellos (25.0%) se consideraron como regular, 11 activos informáticos (22.9%) consideraron como que fue normal, 6 de ellos (12.5%) se consideraron como bueno y 5 activos informáticos (10.4%) se consideraron como excelente.

Seguridad de la Información. Ítem 6. Consideración del tratamiento de la seguridad del acceso a correos electrónicos en MiBanco Huaraz 2023

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	12	25,0	25,0	25,0
	Regular	16	33,3	33,3	58,3
	Normal	9	18,8	18,8	77,1
	Bueno	5	10,4	10,4	87,5
	Excelente	6	12,5	12,5	100,0
	Total	48	100,0	100,0	



Con referencia al ítem sobre la consideración del tratamiento de la seguridad del acceso a correos electrónicos en MiBanco Huaraz 2023, se tuvo que en 12 activos informáticos (25.0%) se consideraron como malo, 16 de ellos (33.3%) se consideraron como regular, 9 activos informáticos (18.8%) se consideraron como que fue normal, 5 de ellos (10.4%) consideraron como bueno y 6 activos informáticos (12.5%) se consideraron como excelente.

USP
UNIVERSIDAD SAN PEDRO

REPOSITORIO INSTITUCIONAL DIGITAL

FORMULARIO DE AUTORIZACIÓN PARA LA PUBLICACIÓN DE DOCUMENTOS DE INVESTIGACIÓN

1. Información del Autor		
SILVA MEDINA KETTY MILAGROS	76909139	silvamilagros031@gmail.com
Apellidos y Nombres	DNI	Correo Electrónico

2. Tipo de Documento de Investigación							
X	Tesis		Trabajo de Suficiencia Profesional		Trabajo Académico		Trabajo de Investigación

3. Grado Académico o Título Profesional [1]									
	Bachiller	X	Título Profesional		Título Segunda Especialidad		Maestría		Doctorado

4. Título del Documento de Investigación
Metodología Magerit y su relación con gestión de riesgos de seguridad del sistema de información en MiBanco, Huaraz 2023

5. Programa Académico
Ingeniera Informática y Sistemas

6. Tipo de Acceso al Documento			
X	Abierto o Público [3] (info:eu-repo/semantics/openAccess)		Acceso restringido [4] (info:eu-repo/semantics/restrictedAccess) (*)
(*) En caso de restringido sustentar motivo			

A. Originalidad del Archivo Digital

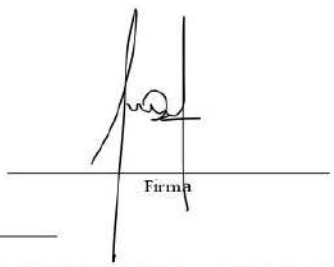
Por el presente dejo constancia que el archivo digital que entrego a la Universidad, es la versión final del trabajo de investigación sustentado y aprobado por el Jurado Evaluador y forma parte del proceso que conduce a obtener el grado académico o título profesional.

B. Otorgamiento de una licencia CREATIVE COMMONS [5]

El autor, por medio de este documento, autoriza a la Universidad, publicar su trabajo de investigación en formato digital en el Repositorio Institucional Digital, al cual se podrá acceder, preservar y difundir de forma libre y gratuita, de manera íntegra a todo el documento. [6]

Lugar	Día	Mes	Año
Chimbote	05	02	24

Huella Digital



Firma

Importante

1. Según Resolución de Consejo Directivo N° 033-2016-SUNEDU-CD, Reglamento del Registro Nacional de Trabajos de Investigación para optar Grados Académicos y Títulos Profesionales, Art. 8, inciso 8.2.
2. Ley N° 30035, Ley que regula el Repositorio Nacional Digital de Ciencia, Tecnología e Innovación de Acceso Abierto y D.S. 006-2015-PCM.
3. Si el autor eligió el tipo de acceso abierto o público, otorga a la Universidad San Pedro una licencia no exclusiva, para que se pueda hacer arreglos de forma en la obra y difundir en el Repositorio Institucional Digital. Respetando siempre los Derechos de Autor y Propiedad Intelectual de acuerdo y en el Marco de la Ley 822.
4. En caso de que el autor elija la segunda opción, únicamente se publicarán los datos del autor y resumen de la obra, de acuerdo a la directiva N° 004-2016-CONCYTEC-DEGC (Numerales 5.2 y 6.7) que norma el funcionamiento del Repositorio Nacional Digital.
5. Las licencias Creative Commons (CC) es una organización internacional sin fines de lucro que pone a disposición de los autores un conjunto de licencias flexibles y de herramientas tecnológicas que facilitan la difusión de información, recursos educativos, obras artísticas y científicas, entre otros. Estas licencias también garantizan que el autor obtenga el crédito por su obra.
6. Según el inciso 12.2, del artículo 12° del Reglamento del Registro Nacional de Trabajos de Investigación para optar grados académicos y títulos profesionales -RENATI "Las universidades, instituciones y escuelas de educación superior tienen como obligación registrar todos los trabajos de investigación y proyectos, incluyendo los metadatos en sus repositorios institucionales precisando si son de acceso abierto o restringido, los cuales serán posteriormente recolectados por el Repositorio Digital RENATI, a través del Repositorio ALICIA".

Nota - En caso de falsedad en los datos, se procederá de acuerdo a ley (Ley 27444, art. 32, núm. 32.3).

Metodología Magerit y su relación con gestión de riesgos de seguridad del sistema de información en MiBanco, Huaraz 2023

INFORME DE ORIGINALIDAD

22%	21%	5%	7%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	hdl.handle.net Fuente de Internet	6%
2	repositorio.ucv.edu.pe Fuente de Internet	3%
3	repositorio.unheval.edu.pe Fuente de Internet	2%
4	core.ac.uk Fuente de Internet	1%
5	repository.unad.edu.co Fuente de Internet	1%
6	revistas.unj.edu.pe Fuente de Internet	1%
7	repositorio.usanpedro.edu.pe Fuente de Internet	1%
8	repositorio.uss.edu.pe Fuente de Internet	<1%

9	dspace.utb.edu.ec Fuente de Internet	<1 %
10	repositorio.uladech.edu.pe Fuente de Internet	<1 %
11	www.dspace.uce.edu.ec Fuente de Internet	<1 %
12	ruidera.uclm.es Fuente de Internet	<1 %
13	repositorio.pucesa.edu.ec Fuente de Internet	<1 %
14	repositorio.udh.edu.pe Fuente de Internet	<1 %
15	1library.co Fuente de Internet	<1 %
16	Submitted to Universidad de Lima Trabajo del estudiante	<1 %
17	idoc.pub Fuente de Internet	<1 %
18	Submitted to Universidad Catolica de Manizales Trabajo del estudiante	<1 %
19	repositorio.uigv.edu.pe Fuente de Internet	<1 %
20	repositorio.utp.edu.pe	

	Fuente de Internet	<1 %
21	Submitted to Universidad Privada San Pedro Trabajo del estudiante	<1 %
22	bibliotecadigital.usb.edu.co Fuente de Internet	<1 %
23	repositorio.uct.edu.pe Fuente de Internet	<1 %
24	www.repositorio.usanpedro.edu.pe Fuente de Internet	<1 %
25	repositorio.unasam.edu.pe Fuente de Internet	<1 %
26	repositorio.uleam.edu.ec Fuente de Internet	<1 %
27	docplayer.es Fuente de Internet	<1 %
28	documentop.com Fuente de Internet	<1 %
29	repositorio.upn.edu.pe Fuente de Internet	<1 %
30	tesis.usat.edu.pe Fuente de Internet	<1 %
31	repositorio.untels.edu.pe Fuente de Internet	<1 %

32	webcache.googleusercontent.com Fuente de Internet	<1 %
33	es.scribd.com Fuente de Internet	<1 %
34	repositorio.unp.edu.pe Fuente de Internet	<1 %
35	ojs.focopublicacoes.com.br Fuente de Internet	<1 %
36	repositorio.usmp.edu.pe Fuente de Internet	<1 %
37	Submitted to UISEK Trabajo del estudiante	<1 %
38	apirepositorio.unh.edu.pe Fuente de Internet	<1 %
39	documents.mx Fuente de Internet	<1 %
40	tesis.pucp.edu.pe Fuente de Internet	<1 %
41	www.nascomponentes.com Fuente de Internet	<1 %
42	www.slideshare.net Fuente de Internet	<1 %
43	www.thefreelibrary.com Fuente de Internet	<1 %

44	Submitted to Universidad Peruana Los Andes Trabajo del estudiante	<1 %
45	hastac.hcommons.org Fuente de Internet	<1 %
46	www.inverlat.com Fuente de Internet	<1 %
47	www.pagina12.com.ar Fuente de Internet	<1 %
48	www.theibfr.com Fuente de Internet	<1 %

Excluir citas	Apagado	Excluir coincidencias	< 10 words
Excluir bibliografía	Activo		