UNIVERSIDAD SAN PEDRO

FACULTAD DE INGENIERÍA

PROGRAMA DE ESTUDIOS DE INGENIERÍA INFORMÁTICA Y DE SISTEMAS

Plan de seguridad de la información en la seguridad de los activos informáticos de la Municipalidad Provincial de Huari, 2022

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

Autora

Chiquian Crispín Eda Maritza

Asesor

Wilmer Carrasco Alvarado

Código ORCID 0000-0003-3138-9808

Huaraz – Perú 2023

Índice General PALABRAS CLAVE:.....**¡Error! Marcador no definido.**

CONSTANCIA DE ORIGINALIDAD.....vi

TÍTULO.....vii

RESUMEN.....viii

ABSTRACT.....ix

INTRODUCCIÓN.....1

METODOLOGÍA.....20

RESULTADOS.....25

ANÁLISIS Y DISCUSIÓN.....28

CONCLUSIONES Y RECOMENDACIONES.....32

RECOMENDACIONES.....33

AGRADECIMIENTOS.....34

REFERENCIAS BIBLIOGRÁFICAS.....35

ANEXOS Y APÉNDICES.....41

ÍNDICE DE TABLAS

Tabla 1. Técnicas e instrumentos utilizados 28

Tabla 2. Estado situacional de la confidencialidad de la información 34

Tabla 3. Estado situacional de la integridad de la información 35

Tabla 4-. Estado situacional de la disponibilidad de la información 36

Tabla 5. Promedio del estado situacional de la información 36

Tabla 6. Cantidad de documentación importante por áreas 38

Tabla 7. Cantidad de Hardware 38

Tabla 8 Elementos de hardware 39

Tabla 9. Identificación de vulnerabilidades 42

Tabla 10. Controles actuales 43

Tabla 11. Controles planificados 43

Tabla 12. Determinación de probabilidades 44

Tabla 13. Ranking de probabilidades 45

Tabla 14. Análisis de impacto 46

Tabla 15. Análisis de impacto 47

Tabla 16. recomendación de controles 48

Tabla 17. Niveles de riesgos en cantidad y porcentajes 49

Tabla 18. cantidad de usuarios autorizados 88

Tabla 19. cantidad de información confidencial accesible 89

Tabla 20. cantidad de información confidencial hackeados 90

Tabla 21. cantidad de información confidencial recuperados 91

Tabla 22. referencia grado de daño causado por el acceso a la información 92

Tabla 23. cantidad de información que debe mantenerse integro 93
Tabla 24. cantidad de información no íntegros 94
Tabla 25. referencia al nivel de integridad de fuentes de información 95
Tabla 26. cantidad de información recuperados de su integridad 96
Tabla 27. nivel de daño causado 97
Tabla 28. cantidad de información disponible 98
Tabla 29. cantidad de información no disponible 99
Tabla 30. referencia al nivel de disponibilidad 100
Tabla 31. cantidad de información no disponibles recuperados 101
Tabla 32. referencia al nivel de daño causado 102

ÍNDICE DE FIGURAS

Figura 1. Niveles de riesgos 49

Figura 2. Niveles de riesgos en porcentajes 49

Figura 3. cantidad de usuarios autorizados 88

Figura 4. cantidad de información confidencial accesible 89

Figura 5. cantidad de información confidencial hackeados 90

Figura 6. cantidad de información confidencial recuperados 91

Figura 7. referencia grado de daño causado por el acceso a la información 92

Figura 8. cantidad de información que debe mantenerse integro 93

Figura 9. cantidad de información no íntegros 94

Figura 10. referencia al nivel de integridad de fuentes de información 95

Figura 11. cantidad de información recuperados de su integridad 96

Figura 12. nivel de daño causado 97

Figura 13. cantidad de información disponible 98

Figura 14. cantidad de información no disponible 99

Figura 15. referencia al nivel de disponibilidad 100

Figura 16. cantidad de información no disponibles recuperados 101

Figura 17. referencia al nivel de daño causado 102

PALABRAS CLAVE:

Tema	Seguridad Informática
Especialidad	Sistemas de información

KEYWORDS:

Theme	Computing Security
Specialty	Information System

LÍNEA DE INVESTIGACIÓN:

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

CONSTANCIA DE ORIGINALIDAD

USP | 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 **"Plan de seguridad de la información en la seguridad de los activos informáticos de la Municipalidad Provincial de Huari, 2022"** del (a) estudiante: **CHIQUIÁN CRISPÍN EDA MARITZA**, identificado(a) con Código N° **2007125087**, se ha verificado un porcentaje de similitud del **21%**, 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, 21 de agosto 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

Plan de seguridad de la información en la seguridad de los activos informáticos de la Municipalidad Provincial de Huari, 2022

RESUMEN

El presente estudio tuvo como objetivo establecer la relación de un plan de seguridad de la información con la seguridad de los activos informáticos de la Municipalidad Provincial de Huari, 2022; la hipótesis consistió en que el plan de seguridad de la información propuesto se relaciona positivamente con la seguridad de los activos informáticos. La investigación fue de tipo no experimental propositiva, de diseño correlacional, se trabajó con una población y muestra de 24 usuarios del sistema de información edil. Se aplicó encuesta y cuestionario.

La relación entre la variable Plan de seguridad y la seguridad de los activos informáticos fue 0.788, lo cual significa que existió correlación positiva alta entre ambas variables, el p valor fue de 0.000, lo cual confirmó que los datos no correspondieron a una curva normal. Que existió relación positiva alta de 0.745 entre la variable Plan de seguridad y la dimensión Seguridad de Software. Que existió relación positiva alta de 0.763 entre la variable Plan de seguridad y la dimensión Seguridad de Hardware. Que existió relación positiva alta de 0.794, entre la variable Plan de seguridad y la dimensión Conocimientos del personal, en todos los casos el p valor fue de 0.000, por lo tanto, los datos no correspondieron a una curva normal.

ABSTRACT

The general objective of this research was to determine the relationship of the proposal of an information security plan with the security of the computer assets of the Provincial Municipality of Huari, 2022; The hypothesis was that the proposed information security plan is positively related to the security of IT assets. The research was non-experimental propositional, correlational design, we worked with a population and sample of 24 users of the building information system. A survey and questionnaire were applied.

The relationship between the variable Security Plan and the security of computer assets was 0.788, which means that there was a high positive correlation between both variables, the p value was 0.000, which confirmed that the data did not correspond to a normal curve. That there was a high positive relationship of 0.745 between the Security Plan variable and the Software Security dimension. That there was a high positive relationship of 0.763 between the Security Plan variable and the Hardware Security dimension. That there was a high positive relationship of 0.794, between the variable Security Plan and the dimension Knowledge of personnel, in all cases the p value was 0.000, therefore, the data did not correspond to a normal curve.

INTRODUCCIÓN

Con la finalidad de conocer el estado actual de la seguridad de la informacion se ha hecho un analisis de los antecedentes locales, nacionales e internacionales para que puedan ser discutidos posteriormente con los resulatdos de la presnte investigación.

Huacón (2022) en la tesis de grado denominada "Vulnerabilidades de la seguridad de la información y su incidencia en el departamento de sistemas del Municipio de Babahoyo "desarrollada en la universidad estatal península de Santa Elena, La Libertad, Ecuador, se planteó como objetivo general realizar un análisis a la plataforma de información y su incidencia en el departamento de sistemas. Trabajó con investigación no experimental de diseño descriptivo, de enfoque cualitativo. Concluyó que las empresas conforme fueron creciendo en volumen de datos e información se volvió más frágil y con tendencia a presentar mayores vulnerabilidaes, riesgos y ser atacados desde adentro y afuera de la empresa, los ataques mas usados fueron extorción, robo de información, etc., se evidenció que en aspectos de seguridad de la informacion, la empresa, tuvo mayores deficiencias y constituyó su prioridad despues de los ataques recibidos. Que las tecnologías de pretesting se seleccionaron de acuerdo a las necesidades de seguridad informatica y de obtención de información, para ello, se cumpleiron los parámetros sugeridos para su administración. Que los reportes generados por Kali Linux, mostraron conductas bastante vulnerables que estaban poniendo en alto riesgos a la institucion, con los datos reportados por el sistema operativo se pudo realziar un analisis profundo y riguroso sobre el desarrollo de las posibles soluciones a los problemas de seguridad informática.

Ramírez (2020) en la tesis de grado denominada "Análisis proactivo de amenazas de la seguridad informática y de la información para la infraestructura de servidores y red de la dirección de tic de un GAD municipal", desarrollada en la universidad estatal península de Santa Elena, la libertad, en Ecuador. Se plantearon como objetivo realziar la deteccion de las vulnerabilidades de servidores y red en de la institucion edil, con aplicación de software libre de código abierto, con el propósito de perfeccionar la seguridad del sistema de informacion edil. Trabajó estudio no experimental, descriptivo, de enfoque cualitativo.

Concluyeron que las empresas conforme crecen, también crecen los datos e información, y a lavez se vuelven más vulnerables y los riesgos se incrementan, los atacantes ven estas vulnerabilidades y atacan con la finalidad de apoderarse de los activos informáticos, también se encontró que la seguridad informática era muy baja, no se le daba mucha importancia por la empresa. Se encontró que las herramientas de prueba informático fueron escogidas teniendo en cuenta los requerimientos de obtención de información. Que los reportes generados por Kali Linux, mostraron conductas bastante vulnerables que estaban poniendo en alto riesgos a la institucion, con los datos reportados por el sistema operativo se pudo realziar un analisis profundo y riguroso sobre el desarrollo de las posibles soluciones a los problemas de seguridad informática.

Poicon y Ramírez (2020) en la tesis de grado denominada "Propuesta de un sistema de gestión de seguridad de la información para la Municipalidad Distrital de Marcavelica, mediante la NTP- ISO/IEC 27001:2014" realizada en la Universidad César Vallejo. Piura. Perú, se trazó el objetivo general de elaborar una propuesta de un Sistema de Gestión de Seguridad informática en el objeto de estudio. Aplicó como método a Magerit 3.0 y análisis de riesgos, trabajó un estudio de tipo aplicada, de diseño descriptivo y no experimental. Concluyeron que se encontraron tres tipos de activos de información, software y hardware; de la clase de equipo de proceso de datos tuvo 50.44% de los activos, de los cuales el 85.84% fue hardware, el nivel de amenaza fue alto con 57.50%, ataques con mayor probabilidad de ocurrencia debido a deficiencias de operatividad de equipos. Que los valores de criticidad de datos e información estuvieron en nivel bajo y medio; respecto a los riesgos se encontró nivel de 30%, sobre riesgo dañino se tuvo 15%, respecto al riesgo de nivel serio se encontró 4%, en este nivel de porcentaje se recomendó realziar control con fines de evitar la concreción de las amenazas. Que se operó 114 controles, 63 de estos no se cumplieron alguna evidencia, la cual no se encontró sistematizada debido a las directivas que no fueron aprobadas, la institucion edil no se registró indicador alguno sobre diagnóstico previo de la seguridad de la información. Que se alcanzaron políticas y normas para realizar monitoreos y control de seguridad de los activos de información edil.

Zapata (2020) en la tesis de grado denominada "sistema de gestión de seguridad de la información basado en las normas ISO/IEC 27001", realizada en la universidad Técnica

de Ambato de la ciudad de Ambato, Ecuador. Se plantearon como objetivo realizar la implementación del Sistema de Gestión de Seguridad de Información en concordancia con ISO/IEC 27001. Trabajó con investigación de tipo no experimental, descriptivo respecto al diseño, de enfoque cualitativo. Concluyeron que no se contó con políticas y procesos que ayuden el la salvaguarda de la seguridad informática, las actividades desarrolladas no se basaron en las normas o políticas previamente acordadas, por el contrario, emplearon normas que no contribuyeron en dar la garantía parcial o total de la disponibilidad, confodencialidad e integridad de los activos informáticos. Qué existieorn falencias en los procesos de gestión de la seguridad, en cpomputadoras, servidores y software, ello permitió que los archivos de información muy importante de la institución estuvieron vulnerables y propuestos ariesgos y amenazas.

Vargas (2019) en la tesis de maestría se trazó como objetivo realizar el diseño de un Plan de Gestión de la Seguridad de la Información con la finalidad de dar cumplimiento de la estrategia de gobierno. La investigación fue no experimental, descriptivo resepcto al diseño, de enfoque cuantitativo. Concluyeron que existió un nivel de la efectividad aceptable cuando se implementaron los controles en concordancia con la norma ISO 27001:2013 debido a que como resulatdos se tuvo una calificación de 30, debido a ello, los procesos y los controles siguieron un patrón regular, las actividades fueron desarrolladas de tal manera que diferentes procesos fueron realziados por diferentes personas, no hubo capacitación ni comunicación formal relacionados con los procesos y estándares, se evidenció un nivel considerable de confianza relacioandos con los dominios de conocimientos de los usuarios del sistema de información, existió probabilidad de fallas. No existió política de seguridad, tampoco privacidad de la información, el nivel logrado fue cero debido a la evaluación de la efectividad del control, ello condujo a que se tenga que desarrollarla, aprobarla y firmarla, tambien se tuvo que revisar y actualizar con cierta frecuencia.

A nivel nacional, Camapaza (2019) en la tesis de grado denominada “Diseño del plan de seguridad informática basado en la NTP ISO/IEC 27001:2014 para la municipalidad del centro poblado de Salcedo – Puno” realizada en la Universidad Andina de Cusco. Perú; se planteó como objetivo general en realizar el diseño de un plan de seguridad

informática cimentada en la norma indicada con el propósito de reducir los niveles de riesgo de seguridad informática en el objeto de estudio. Como metodología aplicó Margerit V.3, tratamiento de riesgos, la norma NTP-ISO/IEC 27001:2014, la investigación fue de tipo en donde se manipuló la variable independiente, de diseño pre experimental, de enfoque positivista. Encontró que el 100% indicaron que se divulgó información bastante importante y sensible, para el 75% nunca se realizó evaluación de riesgos, el 50% no realiza copia de seguridad, el 75% señala que su oficina no está protegida contra ataques informáticos. Concluyó que MARGERIT v.3 como metodología contribuyó en el dimensionamiento de la posibilidad de que ocurra cierto nivel de riesgo, ayudó en la confección de la lista de controles de seguridad con el proposito de reducir los riesgos de niveles altos y medios.

Monteza (2019) en la tesis de grado titulada "Diseño de un Sistema de Gestión de Seguridad de la Información basado en ISO/IEC 27001:2013 en la Municipalidad Distrital de El Agustino. Realizada en la UPC. Lima, Perú; se trazó como objetivo general desarrollar el diseño de un Sistema de Gestión de Seguridad de la Información con fines de protección de los activos de información con referencia a actividades de tributación. Aplicó metodología COBIT, OISM3, Magerit, método MEHARI y OCTAVE ALLEGRO. Como resultado encontró que el 92% de las instituciones que usan sistemas de información se preocupan por la seguridad de sus sistemas de datos; el 34% de los empleados son descuidados o inconscientes, el 26% indicaron que los controles de seguridad estuvieron obsoletos, para el 13% pueden ingresar al sistema sin autorización. Concluyó que se encontraron 72% de activos de información con nivel de criticidad alta, que existieron 44% de activos de información con alto riesgo alto y medio con un 44%. Que el Plan de Tratamiento de Riesgos propuesto puede minimiziar cuantitativamente los riesgos que afectan al sistema de información con grado de aceptabilidad de la organización.

Vásquez y Rengifo (2019) en la tesis denominada "Propuesta de plan de seguridad informática para la sub gerencia de tecnología de la información de la municipalidad provincial de requena, en el año 2019" realizada en la Universidad Científica del Perú, se trazaron el objetivo de proponer un plan de seguridad informática en el espacio de estudio.

Como metodología aplicaron la norma NTP ISO/IEC 27001:2014, políticas de seguridad y evaluación integral. Concluyeron que se plantearon políticas de seguridad aplicando análisis de riesgo mediante al determinación de elementos computacionales más importantes para ques ean protegidos en funcion o de acuerdo a los riesgos y vulnerabilidades que presenten con la finalidad de garantizar sus resepctivas protecciones y adminsitración de la información, cuidando siempre las dimensiones de la información edil. Que se desarrolló un plan de acción y emergencia de procedimientos para ser puestos en prácticas en caso de que suceda un ataque a la seguridad de la infraestructura del objeto de estudio. Que la investigación fue satisfactorio porque contribuyó en el conocimeinto de las deficiencias ediles, en base a la cual se logró alcanzar propuestas de mejora con el propósito de contrarrestar dicha problemática.

Armas y Pérez (2018) en la tesis de grado denominada "Desarrollo de un sistema de gestión de seguridad de la información para minimizar riesgos en los activos de información en la Municipalidad Distrital de Independencia 2016" realizada en la UNASAM, Huaraz Perú; se trazó como objetivo general aplicar el desarrollo de un sistema de gestión de seguridad de la información, con el propósito de reducir los riesgos en los activos de información de la Sub Gerencia de Informática y Telecomunicaciones en el objeto de estudio. Aplicó metodología de análisis y observación de los datos. Concluyeron que la metodología MAGERIT permitió identificar los puntos importantes en las actividades de analziar y gestionar los riesgos, logró resultados del estado de riesgo del espacio de estudio, que se tuvo un documento de seguridad que permitirá desarrolar leyes y normas relacionados con la seguridad de los sistemas de información y para el personal del espacio de estudio.

Pacheco (2018) en la tesis de maestría denominada "Políticas de seguridad de la información de aprovechamiento estudiantil en la educación general básica basado en la norma ISO 27002" desarrollada en la Universidad Espíritu Santo en Ecuador se plantearon como objetivo general hacer el diseño y aplicación de las Políticas de Seguridad de la Información mediante la aplicación de la metodología MAGERIT e ISO 27002 para manejar los riesgos y cumplir con el aseguramiento de los requisitos del sistema de información. Trabajó con investigación de tipo no experimental de diseño

descriptivo, de enfoque cuantitativo Concluyeron que se encontró que la implementación de Políticas de Seguridad de la Información cimentada en ISO 27002, así como en los procesos de control los cuales fueron creados por el personal técnico que laboran en el área de las Tecnologías de la Información y tambien participaron autoridades institucionales, fue una alternativa de solución en la protección y adminsitración eficiente de las actividades de control de gestión, así como también, se trató de dar protección proteger, prevención y minimziación de los incidentes generados por amenazas a los activos de información.

La información es sin duda uno de los activos más importantes y valiosos de cualquier organización, ya que contiene datos importantes y sensibles sobre sus estrategias comerciales, procesos, clientes, proveedores y muchos otros datos que deben protegerse y mantenerse confidenciales, independientemente de su tamaño, integridad y disponibilidad. siempre debe estar garantizado. En ese sentido, se fundamenta científicamente en bases teóricas.

Seguridad Informática. Se entiende a la seguridad informática como las medidas y controles que las autoridades de una organización establecen con el propósito de dar seguridad a los sistemas de información evitando que cualquier atacante interno o externo ejecuten ataques o procesos no autorizados en el hardware y software del sistema; de acuerdo con Corletti (2016), el establecimiento de una adecuada protección de los elementos del sistema de información con el propósito de evitar cualquier configuración de problemas de seguridad, el software aplicativo tiene que ser descargado de fuentes bastante confiables y además tienen que ser actualizadas con significativa frecuencia. Para que los activos de la información se mantengan protegidos con frecuencia se hace necesario desarrollar copias de seguridad, revisar el cifrado de datos, almacenamiento redundante de datos, así como también, deshabilitar o desconectar ciertos elementos de entrada y de salida de información que no ha sido debidamente autorizada. Con el propósito de evitar robos, se tiene que descifrar la información altamente confidencial y crítica, evitar conexiones de equipos internos y externos no autorizados, así como también llevar un control de los mantenimientos preventivos de los elementos de la información.

Seguridad de la información. también es entendida cómo es el nivel de protección con el que se cuenta en un determinado tiempo en la red, para tener la capacidad de dar proteción a la información, archivos, software, hardware en general, frente a cualquier tipo de atacante informático que traten de llevar a cabo procesos de espionaje, modificación de archivos, intercepción y eliminación de infromación, asimismo, como disponer de normas, políticas, métodos, procesos de recuperación de información en casos de ataques al sistema de infromación (CISCO, 2016).

Política de seguridad. Debido a que la seguridad informática, siempre ha sido un problema para cualquier institución pública o privada, internacionalmente se han establecido políticas de seguridad con la finalidad de documentar normas y procesos de cómo las instituciones deben de actuar en casos de ataques informáticos. (Stallings, 2004). La política de seguridad, por lo tanto, es un documento elaborado con la participación principales integrantes de la organización, en este documento se indican los términos generales, objetivos, metas, así como también, las líneas principales de acción qué los usuarios del sistema deban realizar para dar protección a los activos informáticos. En términos de seguridad, la política relacionada a esta misma variable, en primer lugar, debe contener todos los lineamientos implican dar seguridad a todo el sistema de información, específicamente al software, hardware y sin descuidar el nivel de conocimientos que debe tener el personal te gusta el sistema de información con referencia a la seguridad de la información, en los dominios de tipos de ataques, conocimiento de software antivirus, importancia de la seguridad de la información, conocimiento de hardware involucrado en la seguridad informática, etc. (Garre, Tortajada. y Cruz, 2018; Miguel, 2015).

La política de seguridad se conceptúa como un conjunto de directivas, procedimientos, guías y estándares que Norman ciertas actividades y procesos en el uso del sistema de información, así como también se establecen responsabilidades, métodos y técnicas, buenas prácticas y consideraciones que debe tener quienes usen el sistema de información. la política de seguridad aborda los temas de uso de software y hardware, y recomienda que el personal debe estar altamente capacitado, sobre todo en el caso de los ataques informáticos cuando el sistema hace uso de la red de redes (Peltier, Peltier, & Blackley, 2005).

La política de seguridad cumple un rol al interior de la institución, esto significa que, las políticas van dirigidas a su comprensión y aplicación por parte de los elementos o Recursos Humanos que utilizan el sistema de información dentro de la institución, la política hace referencia a cómo ellos deben utilizar los sistemas en función de la seguridad en el cumplimiento de sus funciones operativas o administrativas (Stair & Reynold, 2017; Santana, 2012).

La política de seguridad también cumple un rol externo, esto sucede cuando la institución demuestra al entorno de cómo se está trabajando con el sistema de información dentro de la organización, cómo se está concientizando al recurso humano en los requerimientos de protección de los activos informáticos, así como también de los clientes y proveedores, que, de alguna manera u otra, se concatenan o conectan al sistema de información institucional (Yañez, 2017; Peltier, Peltier & Blackley, 2005).

Principios básicos de la seguridad de la información. Un activo fundamental y de mucho valor para las organizaciones son los activos de información, estos pueden ser los archivos generados dentro de la institución, archivos generados fuera de ella, software, hardware, o cualquier otro elemento digital. específicamente la información generada como consecuencia del desarrollo de las actividades operativas o administrativas presentan tres atributos fundamentales, estos son, la confidencialidad, la integridad y la accesibilidad o también conocida como disponibilidad. La confidencialidad se refiere a que un archivo o documento es confidencial cuando solo su contenido puede ser conocido por uno o más personas debidamente autorizadas, este activo informático, adquiere el atributo de confidencialidad cuando representa un alto valor para la organización (Vega et al, 2020). El atributo integridad hace referencia a que el archivo o documento debe mantenerse completo, sin variación, sin que le falte ninguna parte en toda su extensión. por último, el atributo accesibilidad o disponibilidad significa que el archivo digital o físico debe ser accesible a las personas autorizadas en el espacio y tiempo especificado. Cuando un activo informático no ha sido variado en estos tres atributos, se puede decir que el sistema presenta un nivel de seguridad aceptable o adecuado (Harold & Tipton, 2008; Fitzgerald, 2007).

Riesgo. Los activos informáticos en cualquier tipo de institución se encuentran expuestos a distintos niveles o grados qué riesgos, el riesgo es definido como un suceso de ocurrencia de un determinado evento que pueda causar daño o efectos negativos, o que podría amenazar a los activos y objetivos de la organización. La posibilidad de que pueda ocurrir un riesgo obedece a una función probabilística (Mujica & Álvarez, 2009; Halvorson, 2008).

Dentro de cualquier sistema de información pueden ocurrir tres tipos de riesgos, riesgos estratégicos, los cuales hacen referencia explícitamente a la seguridad de la información en su conjunto, el cuidado adecuado de este capital repercute en la imagen de seguridad institucional, esto se explica porque la institución está tomando decisiones estratégicas decididas y que están haciendo frente a los ataques informáticos internos y externos; los riesgos tácticos se refiere a los riesgos ubicados en los sistemas de control y de fiscalización que puedan estar afectarlo a los datos e información institucional, estos riesgos dañan principalmente a estos activos; mientras que los riesgos operacionales se relacionan con los riesgos que se encuentran en los activos con los que se busca lograr los objetivos institucionales, estos pueden ser hardware, software, sistema de red, cronogramas, presupuestos, etc. (MARGERIT. (2012; Cocho & Romo, 2012).

El riesgo también es definido como una cuantificación estimada del nivel de exposición o grado en que una amenaza pueda materializarse en cualquier parte del sistema de información y que tiene una potencialidad de causar perjuicio a este activo institucional, siempre en cuando no se tomen los controles decisiones para garantizar la seguridad de dichos activos. Los encargados de la seguridad de la información institucional deben saber priorizar la seguridad en función de la importancia y el valor de los activos en función de los objetivos de la organización, Y en función a ellos, elaborar una estrategia de seguridad de los activos informáticos para poder protegerlos con éxito, y en la misma medida garantizar la sostenibilidad de la organización en el tiempo (MARGERIT, 2012; Endler, 2007).

Análisis y evaluación de riesgos. Analizar y evaluar los riesgos de un sistema de información conlleva al desarrollo de actividades y procesos sistemáticos con el propósito de cuantificar la magnitud o tamaño de los riesgos a la que se expone dicho sistema, el

análisis consiste en estudiar por separado cada uno de los elementos del activo informático y determinar cuantitativamente el grado de exposición a los riesgos y en función a ello tomar las decisiones correspondientes sobre seguridad informática (Abril, Pulido & Bohada, 2013). La evaluación consiste en medir el nivel de riesgo, identificar las causas y las vulnerabilidades que dispone frente a la materialización de un determinado riesgo (MARGERIT, 2012; Areitio, 2008).

Amenaza. Se define a las amenazas, que puedan ocurrir en un sistema de información, a las causas potenciales de un evento probabilístico no deseado y que tiene la potencia o capacidad de causar daños a dicho sistema. las amenazas se clasifican por su naturaleza, en este caso, las amenazas provienen por acción de los fenómenos naturales, tales como, sismos, inundaciones, calor excesivo, etc. las amenazas humanas, son aquellos tipos de amenazas generados por usuarios de computadora que tienen la capacidad de poder atacar un determinado sistema de información, lo realizan de manera intencional con intereses propios, la tercera clasificación consiste en amenaza tecnológica, esto se manifiesta en los virus informáticos con los cuales puede causar daños al sistema de información (Rodríguez & Peralta, 2013; Sotelo, Torres & Rivera, 2012).

Vulnerabilidades. La vulnerabilidad hace referencia a una debilidad manifiesta en el sistema de información la cual va a permitir según ataque informático se pueda realizar con facilidad, las vulnerabilidades son aprovechadas por los atacantes con la finalidad de hacer daño al sistema de información, principalmente robar la información para después concretar los objetivos que generaron el ataque. se considera vulnerabilidad al escaso conocimiento que puede tener un usuario de computadora frente a los ataques internos y externos a los elementos de la seguridad informática. Se hace necesario que una organización busque eliminar sus posibilidades porque de esta manera estaría asegurando un cierto nivel de seguridad informática (CISCO, 2018).

Control. El control de la seguridad de la información se refiere a los medios que permiten manipular y manejar el riesgo, estos medios son las normas nacionales e internacionales sobre seguridad informática, las políticas establecidas por la organización en función a la seguridad del sistema de información, los procedimientos, directivas y las

prácticas institucionales qué se ha decidido desarrollar dentro de la institución con la finalidad de establecer la seguridad de los activos informáticos (MARGERIT, 2012).

Los controles y que puedan garantizar la seguridad de información se clasifican en controles preventivos, este tipo de control se enfocan en la reducción de las vulnerabilidades del sistema de información, los controles defectivos buscan determinar o identificar las amenazas y él contestó de manera anticipada antes de que pueda suceder la materialización de un riesgo, los controles defectivos contribuyen en la activación de los controles requeridos. los controles correctivos permiten la corrección del impacto d la materialización de una amenaza, y por último los controles dice así dos se enfocan en la reducción probabilística de que pueda ocurrir o concretizarse la amenaza (CISCO, 2018).

Ciclo de mejora continua. Para los propósitos de la presente investigación, cómo herramienta metodológica en el objetivo de estudiar y alcanzar un estudio planificado de seguridad, se va a utilizar el ciclo de mejora continua por qué, garantizar la seguridad de hardware y software en una institución edil constituye un proceso repetitivo y de mejora continua en el tiempo, para ello se va a utilizar el ciclo de Deming o ciclo PDCA y ciclo PHVA en español. esta metodología se va a concatenar con la norma ISO 27001:2014 con la cual se busca perfeccionar continuamente la adecuación, conveniencia y seguridad del sistema de información. Por su parte el PDCA forma parte de esta estructura normativa. El ciclo PDCA, para su aplicación correcta en los procesos de garantizar la seguridad de los activos informáticos, se estructura en un conjunto de tapas que van a contribuir en el establecimiento de un modelo ejecutable en el tiempo, ello va a permitir la observación y medición de la mejora de la seguridad informática logrado en función al tiempo (ISO 27000; 2018; Deming, 1982), las etapas son las siguientes:

Plan. En la etapa de planificación se busca implementar el sistema de gestión de la seguridad de la información, esta fase implica analizar el contexto institucional, definir metas, objetivos, así como también las políticas que van a contribuir lograr dichos objetivos. en la planificación se identifican las actividades o tareas a realizar en la implementación del sistema de seguridad de los activos informáticos.

Do. La segunda etapa de esta metodología consiste en hacer, por lo tanto esta fase implica implementar y poner en funcionamiento el sistema de gestión de seguridad de la información, por lo tanto, consiste en aplicar en la práctica los controles y las políticas relacionados con el análisis de riesgos encontrar, en esta fase se busca disponer y aplicar los procesos y actividades que van a permitir la identificación de las actividades que se debe realizar con la finalidad de asegurar un control adecuado y garantizar la seguridad de la información y todo el sistema.

Check. La tercera fase de esta metodología consiste en desarrollar el monitoreo y fiscalizar cómo se está llevando a cabo el plan de seguridad o el sistema de administración de seguridad de la información, consiste en controlar los procesos para que se apliquen en la forma indicada y que se estén cumpliendo las metas y objetivos establecidos dentro de un marco de eficacia y eficiencia.

Act. En la cuarta y última etapa esta metodología consiste en actuar, por lo tanto, se tienen como objetivo mejorar sostenidamente y de manera continua la administración de la seguridad de la información, para ello se tiene que definir y ejecutar acciones correctivas que se han encontrado y diseñado con el propósito de rectificar las vulnerabilidades o fallos encontrados en las etapas anteriores.

El presente estudio se justifica en lo social porque con esta investigacion del plan de seguridad de información para la Municipalidad Provincial de Huari en el presente año, Los usuarios del sistema de información de esta institución edil van a adquirir el conocimiento y las metodologías de cómo enfrentar problemas de riesgos de seguridad información, en ese sentido, los beneficiarios van a ser, los usuarios del sistema informático, la municipalidad porque su imagen como institución será mejor percibida por los usuarios , y la población que solicita servicios a la institución edil.

La presente investigación se justifica económicamente porque con la garantía de asegurar la información mediante el plan de seguridad de la información, los activos informáticos se van a mantener íntegros, disponibles y no se va a afectar la

confidencialidad de los archivos de importancia, ello va a evitar pérdidas económicas a la institución edil.

La presente investigación se justifica teóricamente porque se fundamenta en teóricamente en los principios fundamentales de la ciencia de los computadores, la ciencia de la información, concretamente en los principios de la seguridad de los activos informáticos, todo ello, en los principios de seguridad de las normas de seguridad nacionales e internacionales.

Se justifica metodológicamente porque los usuarios del sistema de información de la institución edil en estudio van a conocer los métodos de calidad continua PDCA, la metodología MARGERIT V3.0 y las normas contempladas en la presente investigación, los cuales van a servir de guía para desarrollar los procesos y actividades y el aseguramiento de la información relacionadas con liquidaciones de obras, licitaciones de proyectos de inversión social, información sobre tributaciones, de pagos a proveedores, documentos muy confidenciales para la institución, etc. el plan de seguridad que se alcanza va a permitir actores usuarios adopten una conducta de cómo actuar frente a los riesgos y ataques informáticos que pudieran darse dentro de la institución.

La presente investigación es importante porque se propone mejorar el nivel de protección de la información documentaria e información confidencial creados, distribuidos y almacenados en la municipalidad objeto de estudio. El estudio actual demuestra importancia y relevancia, en tanto que el aporte y los resultados que se pudieren obtener, mejoren el estado situacional actual de la seguridad de la información edil.

La seguridad de la información Siempre se ha constituido como un problema fundamental en todas las organizaciones que utilizan sistemas de información, específicamente en aquellas que generan y distribuyen información confidencial y en aquellos cuyos activos informáticos representan un alto valor para la institución. A nivel internacional, la seguridad de la información, ante los problemas encontrados, estas instituciones han aplicado diversas metodologías con la finalidad de minimizar los riesgos, vulnerabilidades, y ataques informáticos a sus sistemas (Dussan, 2006). Con el transcurrir del tiempo, instituciones internacionales también han contribuido con el

desarrollo de metodologías y políticas normativas para garantizar la seguridad de los activos informáticos, así como también, las comunidades internacionales, han creado leyes para castigar las actividades de ataques informáticos a cualquier tipo de organización (Andress, 2015).

A nivel nacional, los ataques a instituciones ediles no son tan significativos como los ataques que se evidencian en los sistemas financieros, no obstante, las municipalidades manejan información confidencial que deben ser resguardados y asegurados de personas naturales o jurídicas que podrían demostrar interés en atacar los atributos de los archivos de estas instituciones, específicamente en los casos de, confidencialidad, integridad y disponibilidad. la seguridad de la información en las instituciones ediles a nivel nacional se ve vulnerada generalmente por los ataques internos, y los archivos más vulnerables y atacados son los archivos que están relacionados con una inversión pública que desarrolla la municipalidad, específicamente en proyectos de alta inversión social, el propósito de ello consiste en conocer Los montos de inversión antes de que el proyecto sea asignado a un ganador; así como esos tipos de archivos existen otros que son altamente confidenciales, tales como los pagos de tributos de las empresas más distinguidas de la comunidad, documentos que puedan adoptar cambios en política y que puedan generar tendencias económicas positivas o negativas y que puedan ser aprovechadas por quienes tienen acceso a esta información. (Camapaza, 2019)

La Municipalidad Provincial de Huari, como parte del desarrollo de las prestaciones de servicio que tiene que cumplir con la sociedad de su jurisdicción, utiliza un sistema de información, la cual se encuentra integrada con todas las unidades que la estructuran, dentro de cada unidad, los usuarios del sistema presentan el problema de seguridad de los sistemas de información deficiente, se desconoce cómo los usuarios están usando el software y hardware de la institución respecto a las seguridad de la información, asimismo, se desconoce el nivel de conocimiento de los usuarios respecto al tratamiento de los riesgos, vulnerabilidad y ataques a las que puede estar expuesta los activos informáticos de la institución edil.

Ante esta realidad problemática, se plantea un plan de seguridad de la información, para la institución, con el propósito de determinar las relaciones entre los recursos de software y hardware, así como también, con los conocimientos de seguridad de información de los usuarios, uso del sistema respecto a la seguridad y la conducta que pueden adoptar frente a posibles riesgos de ataques al sistema de información de la Municipalidad Provincial de Huari, 2022. Por lo consigueinte se formuló el problema: ¿Cuál es la relación del plan de seguridad de la información con la seguridad de los activos informáticos de la Municipalidad Provincial de Huari, 2022?

A fin de lograr el objetivo del estudio, es fundamental desarrollar el plan estratégico de seguridad de la información que defina las acciones a tomar para proteger hardware, software e información, y de esta manera, evitar los riesgos que pueden dañar la información. En ese sentido se conceptualiza y operacionaliza la variable de estudio. o piratería por parte de ciberdelincuentes.

Plan de seguridad de la información. Son políticas, normas y estándares que orientan el control implementado con el propósito de asegurar los activos informáticos de una determinada institución, la seguridad de la información, se conceptúa al grado de protección de todo el sistema de información o parte de ella como los activos informáticos, es la capacidad de protección que el sistema brinda a datos, archivos, software, hardware en general, frente a ataques internos y externos con propósitos de hacer daño al sistema (CISCO, 2018).

Activos informáticos. Es todo software y hardware que las empresas utilizan con la finalidad de generar información y desarrollar sus actividades como empresa y que son vulnerables a posibles ataques informáticos internos y externos (CISCO, 2018)**.** Los activos informáticos están constituidos por todos los elementos que contiene un sistema de información, estos son, hardware, software, y el personal qué utiliza el sistema de información, por lo tanto, un activo importante con referencia al usuario, es el conocimiento que dispone cada uno de ellos con relación a la seguridad informática.

Dimensiones de la seguridad de la información. en el estudio se tomaron las dimensiones de **Gestión de riesgos.** dimensión que tiene como indicadores al Hardware, software, nube, redes sociales. Estos indicadores son los que contienen los riesgos que se

generan con su uso por parte de los usuarios. **Gestión de seguridad.** esta dimensión contiene a los siguientes indicadores: Identificación de riesgos, Identificación de vulnerabilidades, Conocimiento de ataques, y Nivel de protección (Zapata, 2020).

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:

Software. dimensión que contiene a los siguientes indicadores: Integridad, confidencialidad y disponibilidad. **Hardware** que contiene a los indicadores **a**menazas, ataques repelidos e incidentes, **Conocimientos,** que contiene a los indicadores: Conocimiento de ataques, conocimiento de software de seguridad y conocimiento de hardware de seguridad (Santana, 2012).

Tabla 1

Operacionalizacion de la variable

Variable	Dimensión	Ítems
Seguridad de la Información	Identificación	¿Cómo valora la identificación de los activos de información?
		¿Cómo califica la identificación de los riesgos de activos de información?
		¿Cómo evalúa la identificación de las responsabilidades del activo de información?
	Planificación	¿Cómo considera la planificación de la seguridad de la información?
		¿Cómo evalúa los temas de seguridad de hardware contemplados en el plan de seguridad de información?
		¿Cómo califica en las Políticas de seguridad implementadas en el plan de seguridad de la información en la Municipalidad Provincial de Huari, 2022?
		¿Cómo evalúa la capacitación considerada en el plan de seguridad de información?
	Hacer	¿Cómo considera la ejecución de la seguridad a nivel de hardware en el sistema de la información?
		¿Cómo califica la ejecución de la seguridad a nivel de software en el sistema de la información?
		¿Cómo valora la ejecución de la seguridad de la información en el sistema de la información?
		¿Cómo evalúa la ejecución de la capacitación en seguridad de la información?
	Verificar	¿Cómo considera la verificación de la seguridad a nivel de hardware en el sistema de la información?
		¿Cómo califica la verificación de la seguridad a nivel de software en el sistema de la información?
		¿Cómo valora la verificación de la seguridad de la información en el sistema de la información?
		¿Cómo evalúa la verificación de la capacitación en seguridad de la información?
	Actuar	¿Cómo considera el control de la seguridad a nivel de hardware en el sistema de la información?
		¿Cómo califica el control de la seguridad a nivel de software en el sistema de la información?
		¿Cómo valora el control de la seguridad de la información en el sistema de la información?

		¿Cómo evalúa el control de la capacitación en seguridad de la información?
Activos Informáticos	Seguridad de hardware	¿Cómo califica la seguridad física del sistema de información de la Municipalidad Provincial de Huari, 2022?
		¿Cómo considera la seguridad en el servidor de red del sistema de información?
		¿Cómo valora la seguridad en el servidor de base de datos sistema de información?
		¿Cómo evalúa la seguridad del sistema de cableado del sistema de información?
		¿Cómo califica la seguridad de los Access point del sistema de información?
		¿Cómo considera la seguridad de la computadora de escritorio del sistema de información?
	Seguridad de software	¿Cómo califica la seguridad del sistema operativo del sistema de información?
		¿Cómo considera la seguridad de los softwares de procesamiento de texto del sistema de información?
		¿Cómo valora la seguridad del sistema de base de datos del sistema de información?
		¿Cómo evalúa la seguridad de la información sensible y más importante en el sistema de información?
		¿Cómo califica el nivel de protección del software antivirus en el sistema de información?
		¿Cómo considera la seguridad del software frente a ataques internos o externos en el sistema de información?
		¿Cómo califica la seguridad lógica en general del sistema de información?
	Conocimiento del personal	¿Cómo califica el dominio de hardware por parte del personal?
		¿Cómo considera el dominio del software por parte del personal?
		¿Cómo valora la administración de las claves de acceso al sistema por parte del personal?
		¿Cómo evalúa el dominio de la seguridad informática del personal?
		¿Cómo califica el uso del software antivirus en el sistema de información por parte del personal?
		¿Cómo considera el dominio de la seguridad de los archivos de importancia?

En el estudio se planteó como hipótesis: El plan de seguridad de la información propuesto se relaciona positivamente con la seguridad de los activos informáticos de la Municipalidad Provincial de Huari, 2022.

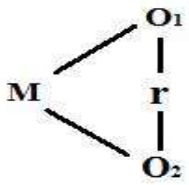
Por otro lado, se formuló el objetivo general: Determinar la relación del plan de seguridad de la información con la seguridad de los activos informáticos de la Municipalidad Provincial de Huari, 2022. Así mismo. Los objetivos específicos:

- Determinar la relación del plan de seguridad de la información con la seguridad de los recursos de software de la Municipalidad Provincial de Huari, 2022.
- Establecer la relación del plan de seguridad de la información con la seguridad de los recursos de hardware de la Municipalidad Provincial de Huari, 2022.
- Determinar la relación del plan de seguridad de la información con los conocimientos del personal de informática de la Municipalidad Provincial de Huari, 2022.

METODOLOGÍA

El tipo del presente estudio va a ser de tipo descriptivo correlacional, esto se explica porque, se van a establecer los grados de correlación entre las variables plan de seguridad de la información con la variable activos informáticos, así como también entre la variable plan de seguridad de la información con las dimensiones de la segunda variable, esto es, software, hardware y conocimiento (Bernal, 2010; Valarino, 2010).

En la investigación no se manipula la variable plan de seguridad de la información para luego observar el impacto los activos del objeto de estudio, por tanto, no experimental. Por la captación de datos, el tipo de investigación es transversal por qué se midió las variables una sola vez durante todo el proceso de investigación. El enfoque es positivista también considerado como cuantitativo, esto se debe a que las variables, sus dimensiones e indicadores, se van a medir cuantitativamente. (Hernández, Fernández y Baptista, 2010).



Dónde:

M = Sistema informático de la Municipalidad Provincial de Huari

O1 = Observación de la variable plan de seguridad de información

O2 = Observación de la variable activos informáticos de la Municipalidad Provincial de Huari

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

Los usuarios del sistema de información de Municipalidad Provincial de Huari, la misma que está constituida por 24 usuarios del sistema de información edil en el

desempeño de sus labores que se desarrollan en cada área o unidad, la siguiente tabla evidencia la cantidad de usuarios por cada unidad de prestación de servicios ediles.

Tabla 2

Población de usuarios del sistema de información

N°	Unidad o área	Cantidad de usuarios
01	Alcaldía	05
02	Gerencia Municipal	02
03	Gerencia Planificación y Presupuesto	02
04	Gerencia de desarrollo social	02
05	Gerencia de Administración Tributaria y Rentas	03
06	Gerencia de Administración y Finanzas	03
07	Gerencia de Infraestructura y Desarrollo Social	03
08	Gerencia de Desarrollo Económico y Ambiental	02
09	Secretaría General	02
	TOTAL	**24**

La muestra esta conformada por el mismo tamaño de la población, esto significa, 24 usuarios del sistema de información de la Municipalidad Provincial de Huari.

Técnica: Con la finalidad de recabar los datos e información de las dos variables en estudios se va a aplicar la técnica de la encuestan y se va a aplicar a los elementos de la muestra, esto es, a los empleados que utilizan el sistema informático de la Municipalidad Provincial de Huari.

Instrumento: El instrumento que se va a aplicar para obtener los datos e información de los elementos de la muestra será el cuestionario, la cual va a contener las preguntas pertinentes que van a permitir medir la relación entre la variable Plan de seguridad de la información con la variable activos

informáticos. Para que sea aplicado, se va a determinar la confiabilidad con el método de Alfa de Cronbach cuyo valor deberá ser mayor a 0.80; y la validez mediante el método de Juicio de Expertos, en este caso, para que sea aceptada, el instrumento deberá tener, en promedio, las calificaciones de muy o excelente.

Tabla 3

Técnicas e instrumentos de investigación

Técnicas	Instrumentos
Encuestas	Cuestionarios
Análisis documental	Textos, tesis, artículos científicos, revistas cientificas e investigaciones antecedentes

La metodología de desarrollo consistirá en lo siguiente: en el marco normativo se va a utilizar la norma internacional ISO 27001: 2014, como metodología se va a aplicar MAGERIT V3:

Análisis de riesgos: En esta fase se va a analizar los riesgos en cada una de las unidades de la Municipalidad Provincial de Huari, primero, se va a realizar un inventario de hardware software y personal a cargo de la seguridad de la información y usuarios, en este caso, se va a analizar los riesgos a los que está expuesto el hardware de la institución edil, se va a analizar las vulnerabilidades y los conocimientos de los usuarios en función a la seguridad de la información, se va a analizar el riesgo existente cuando hacen uso de la nube y las redes sociales. También se va a analizar la gestión de la seguridad actual respecto a cómo están identificando los riesgos, las vulnerabilidades, que conocimiento disponen sobre los ataques y los niveles de protección con los que cuentan. Se va a analizar el nivel se seguridad de la información, específicamente a los archivos más importantes en función a los atributos e disponibilidad, integridad y confidencialidad.

Tratamiento de riesgos: Respecto al tratamiento de riesgos, se va analizar en cada una de las unidades o áreas de la institución edil en relación a las

normas de seguridad de la información que están aplicando, los medios tecnológicos que disponen para enfrentar los riesgos; cómo están utilizando los medios de control de riesgos. También se va a analizar los conocimientos que los empleados usuarios del sistema información dispones respecto a la seguridad de la información, se va analizar los dominios sobre uso de hardware, software, seguridad e la información, etc.

Selección de salvaguardas: En este proceso se va analizar los mecanismos de control que están realizando los empleados de la municipalidad, los controles que se van a analizar hacen referencia a los controles en la seguridad de hardware, software y conocimiento de los usuarios aspecto a la seguridad de la información. Se va a controlar la seguridad de los archivos informáticos de alta confidencialidad, específicamente en el cuidado de sus tres principales atributos: confidencialidad, integración y disponibilidad.

Metodología del estudio: Se va a utilizar la metodología de la mejora continua o Ciclo PDCA o ciclo PHVA que consiste en **planificar** y que consiste en planificación la implementación del plan de seguridad de la información, se va a analizar el contexto institucional, definir metas, objetivos, así como también las políticas que van a contribuir lograr dichos objetivos. en la planificación se identifican las actividades o tareas a realizar en la implementación del sistema de seguridad de los activos informáticos. **Hacer.** La segunda etapa de esta metodología va a consistir en poner en funcionamiento el plan de gestión de seguridad de la información, estos significa que se va a poner en práctica los controles y las políticas relacionados con el análisis de riesgos encontrar, en esta fase se busca disponer y aplicar los procesos y actividades que van a permitir la identificación de las actividades que se debe realizar con la finalidad de asegurar un control adecuado y garantizar la seguridad de la información y todo el sistema. **Verificar.** En esta fase se va a desarrollar el monitoreo y fiscalización sobre cómo se está llevando a cabo el plan de seguridad de la

información, consiste en controlar los procesos para que se apliquen en la forma indicada y que se estén cumpliendo las metas y objetivos establecidos dentro de un marco de eficacia y eficiencia. **Actuar.** En esta etapa se va a tratar de mantener y mejorar la gestión de la seguridad de la información, para ello va a definir y ejecutar acciones correctivas que se han encontrado y diseñado con el propósito de rectificar las vulnerabilidades o fallos encontrados en las etapas anteriores.

RESULTADOS

Objetivo específico 1

Determinar la relación del plan de seguridad de la información con la seguridad de los recursos de software.

Tabla 4

Correlación entre la variable Plan de Seguridad con la dimensión Seguridad de software

		Plan de seguridad	Seguridad de software
Plan de seguridad	Correlación de Pearson	1	,745**
	Sig. (bilateral)		,000
	N	24	24
Seguridad de software	Correlación de Pearson	,745**	1
	Sig. (bilateral)	,000	
	N	24	24

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

La relación entre la variable Plan de seguridad y la dimensión seguridad de software encontrada fue 0.745, este resultado significa que existió una correlación positiva alta entre la variable Plan de seguridad y la dimensión seguridad de software. El p valor fue de 0.000, lo cual es menor a 0.05, lo cual confirma que los datos no correspondieron a una curva normal.

objetivo específico 2

Establecer la relación del plan de seguridad de la información con la seguridad de los recursos de hardware de la Municipalidad Provincial de Huari, 2022.

Tabla 5

Correlación entre la variable Plan de Seguridad con la dimensión Seguridad de hardware

			Plan de seguridad	Seguridad de hardware
Plan de seguridad	Rho de Spearman	Coeficiente de correlación	1,000	,763**
		Sig. (bilateral)	.	,000
		N	24	24
		Coeficiente de correlación	,763**	1,000
		Sig. (bilateral)	,000	.
		N	24	24

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

La relación entre la variable Plan de seguridad y la dimensión seguridad de hardware encontrada fue 0.763, este resultado significa que existió una correlación positiva alta entre la variable Plan de seguridad y la dimensión seguridad de hardware. El p valor fue de 0.000, lo cual es menor a 0.05, lo cual confirma que los datos no correspondieron a una curva normal.

Objetivo específico 6

Determinar la relación del plan de seguridad de la información con los conocimientos del personal de informática de la Municipalidad Provincial de Huari, 2022.

Tabla 7

Correlación entre la variable Plan de Seguridad con la dimensión Conocimiento del personal

			Plan de seguridad	Conocimiento del personal
Rho de Spearman	Plan de seguridad	Coeficiente de correlación	1,000	,794**
		Sig. (bilateral)	.	,000
		N	24	24
	Conocimiento del personal	Coeficiente de correlación	,794**	1,000
		Sig. (bilateral)	,000	.
		N	24	24

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

La relación entre la variable Plan de seguridad y la dimensión conocimiento del personal encontrada fue 0.794, este resultado significa que existió una correlación positiva alta entre la variable Plan de seguridad y la dimensión Conocimiento del personal. El p valor fue de 0.000, lo cual es menor a 0.05, lo cual confirma 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 8

Correlación entre la variable Plan de Seguridad con la variable Seguridad de los activos informáticos

			Plan de seguridad	Seguridad de los activos informáticos

Rho de Spearman	Plan de seguridad	Coeficiente de correlación	1,000	,788**
		Sig. (bilateral)	.	,000
		N	24	24
	Seguridad de los activos informáticos	Coeficiente de correlación	,788**	1,000
		Sig. (bilateral)	,000	.
		N	24	24

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

La relación entre la variable Plan de seguridad y la variable Seguridad de la información encontrada fue 0.788, este resultado significa que existió una correlación positiva alta entre la variable Plan de seguridad y la variable Seguridad de los activos informáticos. El p valor fue de 0.000, lo cual es menor a 0.05, lo cual confirma que los datos no correspondieron a una curva normal.

ANÁLISIS Y DISCUSIÓN

En este estudio se encontró que existió relación positiva alta de 0.788 entre la variable Plan de seguridad y la variable Seguridad de los activos informáticos, los cuales coinciden parcialmente con los resultados de la investigación de Huacón (2022) quien tuvo el resultado de que las empresas adquieren fragilidad cuando crecen y tienden a ser atacados generalmente por agentes externos para extorsionar y robar activos informáticos, etc., que las herramientas informáticas se seleccionan en función a las necesidades de obtención de los datos, el cual debe cumplir con parámetros alcanzados para su gestión. Que se encontraron conductas e información de vulnerabilidades que puede estar expuestos y que los datos permitieron realizar un estudio riguroso sobre seguridad informática institucional.

En el presente estudio se encontró que el plan de seguridad mejoró la seguridad de los activos informáticos de una institución edil con un valor de relación positiva alta de 0.788, estos resultados coinciden parcialmente con los obtenidos por Ramírez (2020) en donde se tuvo que las empresas a están expuestas a ataques informáticos

a medida que crecen, que los datos se vuelven vulnerables, aunque la investigación antecedente no mostró resultados de correlación, mostraron conductas e información de vulnerabilidades en donde se expuso a la institución, los datos permitieron llevar a cabo un estudio profundo y sistemático de la elaboración de probables resultados fundamentados en normas de seguridad.

En este estudio se tuvo que el plan de seguridad mejoró la seguridad de los activos informáticos de una institución edil con un valor de relación positiva alta de 0.788, estos resultados coinciden parcialmente y también difieren parcialmente con los resultados de la investigación antecedente de Zapata (2020) quién encontró que en el espacio estudiado no tuvieron políticas de seguridad de la información, que los procesos realizados no se fundamentaron en políticas establecidas, que aplicaron ciertas normas de manera general y aislada, por tanto, no garantizaron la seguridad del sistema de información a nivel de software y hardware, existieron deficiencias y errores adminsitrativos y gestión relacionados con la seguridad de la información, especialmente en los servidores debido a que procesaran datos importantes y estuvieron expuestos a diversas amenazas y vulnerabilidades.

Las conclusiones de la presente investigación indicaron que el plan de seguridad mejoró la seguridad de los activos informáticos de una institución edil con un valor de relación positiva alta de 0.788, estos resultados coinciden parcialmente y también difieren parcialmente con los resultados del antecedente de Vargas (2019) quien encontró que los procesos fueron evaluados por distintas personas, no hubo capacitación, tampoco información relacionados con los procesos y métodos utilizados, existió considerable nivel de confianza en las habilidades, capacidades y competencias del personal, no existió política de seguridad, tampoco privacidad de la información, que los conocimientos del personal sobre seguridad informática estuvieron bastante bajos, esto difirió significativamente con los resultados de la presente investigación.

En el presente estudio se encontró que el plan de seguridad mejoró la seguridad de los activos informáticos de una institución edil con un valor de relación positiva alta de 0.788, estos resultados coinciden parcialmente y también difieren parcialmente

con los resultados de la investigación antecedente de Pacheco (2018) quien concluyó que la implementación de un Plan de Políticas de Seguridad de la Información se constituyó como alternativa de solución que protegió y administró de manera eficiente los procesos de control, pudo prevenir las ocurrencias generados por riesgos a la información.

Los resultados del presente estudio indicaron que el plan de seguridad mejoró la seguridad de los activos informáticos de una institución edil con un valor de relación positiva alta de 0.788, estos resultados coinciden parcialmente con los resultados de la investigación antecedente de Camapaza (2019) en donde se encontró que el 100% indicaron divulgó información sensible, para el 75% nunca se realizó evaluación de riesgos, el 50% no realizó copia de seguridad, el 75% señala que su oficina no estuvo protegida contra ataques informáticos, que MARGERIT v.3 contribuyó en el dimensionamiento de posibles ocurrencias del riesgo, elaboraron la lista de controles de seguridad con la cual se pudo minimizar los riesgos de diferentes niveles establecidos para el diseño del Plan de Seguridad.

Se tuvo en la investigación se encontró que el plan de seguridad mejoró la seguridad de los activos informáticos de una institución edil con un valor de relación positiva alta de 0.788, estos resultados coinciden parcialmente y también difieren parcialmente con los resultados de la investigación antecedente de Monteza (2019) quién encontró que el 34% de los empleados fueron descuidados o inconscientes, el 26% indicaron que los controles de seguridad estuvieron obsoletos, para el 13% pueden ingresar al sistema sin autorización, que se encontraron 72% de activos de información con grado de alta criticidad, que existieron 44% de activos de información con alto riesgo alto y medio con un 44%.

En los resultados del presente estudio se encontró que el plan de seguridad mejoró la seguridad de los activos informáticos de una institución edil con un valor de relación positiva alta de 0.788, estos resultados coinciden parcialmente y también difieren con la investigación de Poicon y Ramírez (2020) quienes tuvieron que el nivel de amenaza fue alto con 57.50%, de amenazas, el impacto del riesgo fueron bajo y medio en los activos de la información; y el nivel de los riesgos fue 30%, en

riesgo de daños fue 15% y para un riesgo serio fue del 4%, que de 114 controles, 63 de estos no se cumplieron alguna evidencia, la cual no se encontró sistematizada, estuvo en directivas que todavía fueron aprobadas institucionalmente, por lo tanto, no se registraron indicadores relacionados con el diagnóstico antes de la seguridad de la información.

En esta investigación se tuvo que el plan de seguridad mejoró la seguridad de los activos informáticos de una institución edil con un valor de relación positiva alta de 0.788, estos resultados coinciden parcialmente y también difieren parcialmente con los resultados de la investigación antecedente de Vásquez y Rengifo (2019) quien concluyó que mediante análisis de riesgo determinaron los temas más importantes del cuidado y seguridad de los equipos, en función a presencia de vulnerabilidad con el propósito de dar protección y gestión de información, manteniendo la confidencialidad, integridad, y disponibilidad de la información en la institución edil, que el plan de acción y emergencia de procedimientos fue satisfactorio porque permitió conocer las deficiencias ediles, en base a la cual se logró alcanzar la mejora con el propósito de contrarrestar dicha problemática.

Se tuvo en la investigación se encontró que el plan de seguridad mejoró la seguridad de los activos informáticos de una institución edil con un valor de relación positiva alta de 0.788, estos resultados coinciden parcialmente y también difieren parcialmente con los resultados de la investigación antecedente de Armas y Pérez (2018) debido a que aplicaron la misma metodología MAGERIT, la cual permitió identificar los puntos importantes en el poseso de análisis y gestión de riesgos, permitió logar resultados del estado de riesgo.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Se concluyó a nivel general que existió relación positiva alta de 0.788 entre la variable Plan de seguridad y la variable Seguridad de los activos informáticos, el p valor fue de 0.000, esto indicó que los datos no correspondieron a una curva normal.

Existió relación positiva alta de 0.745 entre la variable Plan de seguridad y la dimensión seguridad de software, el p valor fue de 0.000, lo cual confirmó que los datos no correspondieron a una curva normal.

Existió relación positiva alta de 0.763 entre la variable Plan de seguridad y la dimensión seguridad de hardware el p valor fue de 0.000, lo cual indicó que los datos no correspondieron a una curva normal.

Existió relación positiva alta de 0.794 entre la variable Plan de seguridad y la dimensión conocimiento del personal el p valor fue de 0.000, lo cual indicó que los datos no correspondieron a una curva normal.

RECOMENDACIONES

La Gerencia Municipal y el jefe del Área de Informática de la Municipalidad Provincial de Huari deben tomar decisiones respecto a los resultados de la relación entre la variable Plan de seguridad y la variable Seguridad de los activos informáticos, estas decisiones deben enfocarse en la mejora de ambas variables, pero con la participación activa y decidida de la parte administrativa y operativa, específicamente de los empleados que utilizan cotidianamente el sistema de información edil.

La Gerencia Municipal y el jefe del Área de Informática de la Municipalidad Provincial de Huari deben seguir o continuar con la capacitación a los empleados ediles en las actualizaciones sobre la seguridad de software, específicamente en seguridad del sistema operativos, seguridad de base de datos, uso e instalación de programas antivirus, to ello dentro de las políticas del plan de seguridad, para ello deben contar con la participación de especialistas.

La Gerencia Municipal y el jefe del Área de Informática de la Municipalidad Provincial de Huari deben seguir o continuar con la capacitación a los empleados ediles en las actualizaciones sobre la seguridad de hardware, especialmente en el uso adecuado de la computadora y sus periféricos, así como, la adopción de conductas en el manejo de claves y acceso a los sistemas.

La Gerencia Municipal y el jefe del Área de Informática de la Municipalidad Provincial de Huari deben continuar con las capacitaciones en el conocimiento del personal en los temas de la seguridad de hardware y software, así como también en la concientización sobre la importancia de la seguridad de los activos informáticos de la institución edil.

AGRADECIMIENTOS

A Dios por permitirme el objetivo de ser profesional,

a la Municipalidad Provincial de Huari 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.

Maritza

REFERENCIAS BIBLIOGRÁFICAS

Abril, A., Pulido, J., & Bohada, J. A. (2013). *Análisis de Riesgos en Seguridad de la Información,* Recuperado de https://www.jdc.edu.co/revistas/index.php/rciyt/article/view/121/113

Andress, J. (2015). *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*. Massachusetts, Estados: Elsevier, 2015.

Areitio, J. (2008). *Seguridad de la Información, Redes, Informática y Sistemas de Información.* Madrid: Paraninfo.

Armas, Angélica Madeleine y Pérez, Flor Rosmery (2018). *Desarrollo de un sistema de gestión de seguridad de la información para minimizar riesgos en los activos de información en la sub gerencia de informática y telecomunicaciones de la Municipalidad Distrital de Independencia 2016*.
Universidad Nacional Santiago Antúnez de Mayolo. Huaraz Perú.

Bernal, C. (2010). *Metodología de la Investigación*. Tercera edición. Bogotá: Editorial Pearson Educación de Colombia Ltda.

Camapaza, Abdon Anders (2019) *Diseño del plan de seguridad informática basado en la NTP ISO/IEC 27001:2014 para la municipalidad del centro poblado de Salcedo – Puno.* Tesis de grado. Universidad Andina de Cusco. Perú.

CISCO. (2018). *Lo que usted necesita saber sobre seguridad de la red.* Obtenido de http://www.cisco.com/web/LA/soluciones/la/information_security/index.h

Cocho, J., & Romo, M. (2012). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.*

De Freitas, Vidalina (2012*). Sistema de Gestión de Seguridad de la Información*. Primera ed. Venezuela: EAE.

Deming, W. E. (1982). *Quality, productivity, and competitive position* (Vol. 183): Massachusetts Institute of Technology, Center for advanced engineering study.

Dussan, C. (2006). *Políticas de Seguridad Informática*. *Entramado*, *2*(1), 86–92.

Endler, D. (2007). *Hacking Exposed VoIP: Voice Over IP Security Secret & S*olutions. Osborne: Mc Graw-Hill.

Farias, M., Mendoza, M., & Gómez, L. (2003). Las Políticas de Seguridad como Apoyo a la Falta de Legislación Informática. *Techno-legal Aspects of Information Society and New Economy: An Overview*, *I*, 185–191.

Fitzgerald, T. (2007). *Information Security Governance*. En H. Tipton, & M. Krause, Information Security Management Handbook (págs. 15-34). USA: Auerbach.

Garre, S.; Tortajada, S. H. y Cruz, A. (2018). *Sistema de gestión de la seguridad de la información.* Primera ed. España: Editorial UOC.

Halvorson, N. (2008). *Information Risk Management: A Process Approach to Risk Diagnosis and Treatment. Information Security Management Handbook*. USA: Auerbach Publications.

Harold, F & Tipton, M. K. (2008). *Information security management handbook*. Sexto ed. Tipton HF, editor. Nueva York: Auerbach.

Hernández, R.; Fernández, C. y Baptista, P. (2010). *Metodología de la investigación*. Quinta edición. México: Mc Graw Hill. ISBN: 978-607-15-0291-9

Huacón (2022) *Vulnerabilidades de la seguridad de la información y su incidencia en el departamento de sistemas del Municipio de Babahoyo*. Tesis de grado. Universidad Estatal Península de Santa Elena, La Libertad, Ecuador.

INDECOPI. (2014*). Norma Técnica Peruana NTP-ISO/IEC 27001:2014. Tecnología de la información. Técnicas de seguridad. Sistema de gestión de seguridad de la información. Requisito.*". Lima: Segunda Edición.

ISO 27000. (2018). ISO 27000.es. Obtenido de El Portal de ISO 27001 en español: http://www.iso27000.es/iso27000.html

MARGERIT. (2012). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid: Ministerio de Hacienda y Administración Pública.

Miguel, C. (2015). *Protección de datos y seguridad de la información*. Cuarta ed. España: Ra-Ma; 2015.

Monteza Mera, Lisbet Odelly (2019). *Diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2013 para la Municipalidad Distrital de El Agustino.* Tesis de grado. Universidad Peruana de Ciencias Aplicadas. Lima. Perú.

Mujica, M., & Álvarez, J. (2009). *El Análisis de Riesgo en la seguridad de la* información, *4*, .33–37.

Pacheco, L. A. (2018). *Políticas de seguridad de la información de aprovechamiento estudiantil en la educación general básica basado en la norma ISO 27002*.

Tesis de maestría. Universidad Espíritu Santo. Ecuador.

Peltier, T., Peltier, J., & Blackley, J. (2005). *Information Security Fundamental*s. USA: Auerbach Publications.

Poicon, Junior Miguel Ángel y Ramírez, Oscar (2020*). Propuesta de un sistema de gestión de seguridad de la información para la Municipalidad Distrital de Marcavelica, mediante la NTP- ISO/IEC 27001:2014.* Tesis de grado. Universidad César Vallejo. Piura. Perú.

Ramírez, A. F. (2020). *Análisis proactivo de amenazas de la seguridad informática y de la información para la infraestructura de servidores y red de la dirección de tic de un GAD municipal*. Universidad Estatal Península de Santa Elena, La Libertad, Ecuador.

Rodríguez, J. M., & Peralta, I. (2013). *Gestión de Riesgos*. tiThink Consultoría. Recuperado de https://www.tithink.com/publicacion/MAGERIT.pdf

Santana, C. (2012). Seguridad Informática: ¿Qué es una vulnerabilidad, una amenaza y un riesgo? Recuperado de https://www.codejobs.com/es/blog/2012/09/07/seguridad-informatica-quees-una-vulnerabilidad-una-amenaza-y-un-riesgo

Sotelo, M., Torres, J., & Rivera, J. (2012). *Un Proceso Práctico de Análisis de Riesgos de Activos de Información*. Recuperado de http://www.comtel.pe/comtel2012/callforpaper2012/P26C.pdf

Stair, R., & Reynolds, G. (2017). *Fundamentals of information systems. Cengage Learning.* https://books.google.es/books?hl=es&lr=&id=GtVBDgAAQBAJ&oi=fnd&pg=PP1&dq=information+systems&ots=k24BRDcXuB&sig=xyQYIakwC

MLuoVoYjhU96JYjOXY#v=onepage&q=information%20systems&f=false

Stallings, W. (2004). *Fundamentos de Seguridad en Redes.* Madrid: Pearson Prentice Hall.

Valarino, E. (2010). *Metodología de la Inves*tigación. Paso a Paso. México DF: Trillas.

Vargas, H. (2019). *Plan de gestión de seguridad de la información para la secretaría de educación del municipio de yumbo, en cumplimiento de la estrategia de gobierno en línea de Colombia*. Tesis de maestría. Universidad Santiago de Cali, Colombia.

Vásquez, Dennis Alberto y Rengifo, Paulo Manuel (2019). *Propuesta de plan de seguridad informática para la sub gerencia de tecnología de la información de la municipalidad provincial de requena, en el año 2019*. Tesis de grado. Universidad Científica del Perú. Loreto.

Vega, L.; López, F.; Ramírez, J. F. y Orellana, A. (2020). *Impacto de las aplicaciones y servicios informáticos desarrollados por la Universidad de las Ciencias Informáticas para el sector de la salud. Artículo científico. Universidad de las Ciencias Informáticas, Cuba.* Revista Cubana de Informática Médica 2020:12(1)58-75.

Voutssas, J. (2010). Preservación documental digital y seguridad informática. Recuperado de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2010000100008

Yañez, N. A. (2017). *Sistema de gestión de seguridad de la información para la subsecretaria de economía y empresas de menor tamaño*. Santiago de Chile: Universidad de Chile, 2017.

Zapata, K. B. (2020). *Sistema de gestión de seguridad de la información basado en las normas ISO/IEC 27001, en el departamento de tecnologías de la información del gobierno autónomo descentralizado de la municipalidad de Ambato*. Tesis de grado. Universidad Técnica de Ambato. Ecuador.

ANEXOS Y APÉNDICES

Anexo 01:

Matriz de Consistencia

Plan de Seguridad de la Información para la Municipalidad Provincial de Huari, 2022

PROBLEMA DE INVESTIGACIÓN	OBJETIVOS	HIPÓTESIS	METODOLOGÍA
Problema General ¿Cuál es la relación del plan de seguridad de la información con la seguridad de los activos informáticos de la Municipalidad Provincial de Huari, 2022? **Problemas específicos** ¿Cuál es la relación del plan de seguridad de la información con la seguridad de los recursos de software de la Municipalidad Provincial de Huari, 2022? ¿Cuál es la relación del plan de seguridad de la información con la seguridad de los recursos de hardware de la Municipalidad Provincial de Huari, 2022? ¿Cuál es la relación del plan de seguridad de la información con los conocimientos del personal de informática de la Municipalidad Provincial de Huari, 2022?	**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. **Objetivos Específicos** Determinar la relación del plan de seguridad de la información con la seguridad de los recursos de software de la Municipalidad Provincial de Huari, 2022. Establecer la relación del plan de seguridad de la información con la seguridad de los recursos de hardware de la Municipalidad Provincial de Huari, 2022. Determinar la relación del plan de seguridad de la información con los conocimientos del personal de informática de la Municipalidad Provincial de Huari, 2022.	**Hipótesis General** El plan de seguridad de la información propuesto se relaciona positivamente con la seguridad de los activos informáticos de la Municipalidad Provincial de Huari, 2022. **Hipótesis Específicas** El plan de seguridad de la información propuesto se relaciona positivamente con la seguridad de los recursos de software de la Municipalidad Provincial de Huari. El plan de seguridad de la información propuesto se relaciona positivamente con la seguridad de los recursos de hardware de la Municipalidad Provincial de Huari, 2022. El plan de seguridad de la información propuesto se relaciona positivamente con los conocimientos del personal de informática de la Municipalidad Provincial de Huari, 2022.	Se considera que la investigación es de tipo no experimental. **Diseño de la Investigación** **Diseño:** Descriptivo correlacional. **Enfoque:** Cuantitativo **Población y Muestra:** Los elementos de la población reconformarán 27 trabajadores ediles quienes son usuarios del sistema de información de la Municipalidad Provincial de Huari. **Instrumentos de investigación** Encuesta

Anexo 02

UNIVERSIDAD SAN PEDRO

ENCUESTA

Bach. Chiquian Críspin Eda Maritza

Estimado encuestado: Sírvase responder con absoluta sinceridad la siguiente encuesta, que corresponde al estudio del un Plan de Seguridad de la Información para la Municipalidad Provincial de Huari, 2022. 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	CUESTIONARIO	ESCALA			
			1	2	3	4
PLAN DE SEGURIDAD						
01	**Identificación**	¿Cómo valora la identificación de los activos de información en la Municipalidad Provincial de Huari, 2022?				
02		¿Cómo califica la identificación de los riesgos de activos de información en la Municipalidad Provincial de Huari, 2022?				
03		¿Cómo evalúa la identificación de las responsabilidades del activo de información en la información en la Municipalidad Provincial de Huari, 2022?				
04	**Planificación**	¿Cómo considera la planificación de la seguridad de la información en la Municipalidad Provincial de Huari, 2022?				
05		¿Cómo evalúa los temas de seguridad de hardware contemplados en el plan de seguridad de información en la Municipalidad Provincial de Huari, 2022?				
06		¿Cómo califica en las Políticas de seguridad implementadas en el plan de seguridad de la información en la Municipalidad Provincial de Huari, 2022?				
07		¿Cómo evalúa la capacitación considerada en el plan de seguridad de información en la Municipalidad Provincial de Huari, 2022?				
08	**Hacer**	¿Cómo considera la ejecución de la seguridad a nivel de hardware en el sistema de la información en la Municipalidad Provincial de Huari, 2022?				

09		¿Cómo califica la ejecución de la seguridad a nivel de software en el sistema de la información en la Municipalidad Provincial de Huari, 2022?				
10		¿Cómo valora la ejecución de la seguridad de la información en el sistema de la información en la Municipalidad Provincial de Huari, 2022?				
11		¿Cómo evalúa la ejecución de la capacitación en seguridad de la información en la Municipalidad Provincial de Huari, 2022?				
12	**Verificar**	¿Cómo considera la verificación de la seguridad a nivel de hardware en el sistema de la información en la Municipalidad Provincial de Huari, 2022?				
13		¿Cómo califica la verificación de la seguridad a nivel de software en el sistema de la información en la Municipalidad Provincial de Huari, 2022?				
14		¿Cómo valora la verificación de la seguridad de la información en el sistema de la información en la Municipalidad Provincial de Huari, 2022?				
15		¿Cómo evalúa la verificación de la capacitación en seguridad de la información en la Municipalidad Provincial de Huari, 2022?				
16	**Actuar**	¿Cómo considera el control de la seguridad a nivel de hardware en el sistema de la información en la Municipalidad Provincial de Huari, 2022?				
17		¿Cómo califica el control de la seguridad a nivel de software en el sistema de la información en la Municipalidad Provincial de Huari, 2022?				
18		¿Cómo valora el control de la seguridad de la información en el sistema de la información en la Municipalidad Provincial de Huari, 2022?				
19		¿Cómo evalúa el control de la capacitación en seguridad de la información en la Municipalidad Provincial de Huari, 2022?				

LEYENDA

1 Malo 2 Regular 3 Bueno 4 Excelente

N°	DIM	CUESTIONARIO	ESCALA			
			1	2	3	4
SEGURIDAD DE LA INFORMACIÓN DE LA MUNICIPALIDAD DE HUARI						
01	**Seguridad de Hardware**	¿Cómo califica la seguridad física del sistema de información de la Municipalidad Provincial de Huari, 2022?				
02		¿Cómo considera la seguridad en el servidor de red del sistema de información de la Municipalidad Provincial de Huari, 2022?				
03		¿Cómo valora la seguridad en el servidor de base de datos sistema de información de la Municipalidad Provincial de Huari, 2022?				
04		¿Cómo evalúa la seguridad del sistema de cableado del sistema de información de la Municipalidad Provincial de Huari, 2022?				
05		¿Cómo califica la seguridad de los Access point del sistema de información de la Municipalidad Provincial de Huari, 2022?				
06		¿Cómo considera la seguridad de la computadora de escritorio del sistema de información de la Municipalidad Provincial de Huari, 2022?				
07	**Seguridad de Software**	¿Cómo califica la seguridad del sistema operativo del sistema de información de la Municipalidad Provincial de Huari, 2022?				
08		¿Cómo considera la seguridad de los software de procesamiento de texto del sistema de información de la Municipalidad Provincial de Huari, 2022?				
09		¿Cómo valora la seguridad del sistema de base de datos del sistema de información de la Municipalidad Provincial de Huari, 2022?				
10		¿Cómo evalúa la seguridad de la información sensible y más importante en el sistema de información de la Municipalidad Provincial de Huari, 2022?				
11		¿Cómo califica el nivel de protección del software antivirus en el sistema de información de la Municipalidad Provincial de Huari, 2022?				
12		¿Cómo considera la seguridad del software frente a ataques internos o externos en el sistema de información de la Municipalidad Provincial de Huari, 2022?				
13		¿Cómo califica la seguridad lógica en general del sistema de información de la Municipalidad Provincial de Huari, 2022?				
14	**Conocimiento del Personal**	¿Cómo califica el dominio de hardware por parte del personal de la Municipalidad Provincial de Huari, 2022?				
15		¿Cómo considera el dominio del software por parte del personal de la Municipalidad Provincial de Huari, 2022?				
16		¿Cómo valora la administración de las claves de acceso al sistema por parte del personal de la Municipalidad Provincial de Huari, 2022?				
17		¿Cómo evalúa el dominio de la seguridad informática del personal de la Municipalidad Provincial de Huari, 2022?				

16 18		¿Cómo califica el uso del software antivirus en el sistema de información por parte del personal de la Municipalidad Provincial de Huari, 2022?				
19		¿Cómo considera el dominio de la seguridad de los archivos de importancia en la Municipalidad Provincial de Huari, 2022?				

LEYENDA

1 Malo 2 Regular 3 Bueno 4 Excelente

Anexo 03

Alfa de Cronbach

N°	PLAN DE SEGURIDAD																						
	Identificación			TOT	Planificación				TOT	Hacer				TOT	Verificar				TOT	Actuar				TOT	TOT
	1	2	3		4	5	6	7		8	9	10	11		12	13	14	15		16	17	18	19		
1	2	1	1	4	1	2	1	1	5	2	1	2	1	6	1	4	1	1	7	3	1	4	1	9	31
2	2	1	1	4	2	2	2	1	7	3	1	3	1	8	2	2	1	2	7	2	2	3	1	8	34
3	4	3	4	11	3	4	4	4	15	4	3	4	4	15	4	3	4	3	14	4	4	4	3	15	70
4	1	1	1	3	1	2	1	2	6	2	1	2	2	7	4	1	2	3	10	1	1	1	1	4	30
4	2	3	2	7	1	1	2	1	5	1	2	1	1	5	1	3	1	2	7	1	3	2	2	8	32
6	2	2	1	5	4	4	4	3	15	4	2	4	2	12	1	2	1	2	6	3	2	4	4	13	51
7	2	4	2	8	3	4	3	2	12	4	2	4	3	13	4	1	4	4	13	4	4	2	4	14	60
8	1	1	2	4	2	1	1	3	7	1	1	1	1	4	1	1	1	3	6	2	1	1	2	6	27
9	1	2	3	6	1	2	1	1	5	2	1	2	2	7	2	2	1	1	6	1	2	1	1	5	29
10	3	4	2	9	2	1	1	3	7	1	4	1	1	7	2	4	3	2	11	1	4	2	2	9	43
Var				6.09					14.64					12.04					8.41					12.89	
																							Suma de varianzas parciales		54.07
																							Varianza General o total		199.61
																							Valor de Alfa		0.911

SEGURIDAD DE LA INFORMACIÓN DE LA MUNICIPALIDAD DE HUARI																												
N°	Seguridad de Hardware						TOT	Seguridad de Software												TOT	Conocimiento del Personal							TOT	TOT
	1	2	3	4	5	6		7	8	9	10	11	12	13		14	15	16	17	18	19		
1	2	1	2	1	1	1	8	2	2	1	2	1	2	1	11	1	1	2	1	2	1	8	27
2	1	1	1	1	1	1	6	1	1	1	1	1	1	1	7	1	1	1	1	1	1	6	19
3	2	3	1	3	4	4	17	4	4	3	4	3	4	4	26	4	3	4	3	4	3	21	64
4	2	1	2	1	2	2	10	4	2	4	2	1	4	2	19	2	1	2	1	1	1	8	37
5	1	2	1	2	1	1	8	1	1	2	1	2	1	1	9	1	2	1	2	1	2	9	26
6	4	2	4	2	2	4	18	4	4	2	4	2	4	4	24	4	2	4	2	4	2	18	60
7	2	4	1	3	4	4	18	3	4	1	4	4	4	1	21	4	4	4	4	4	4	24	63
8	1	1	4	1	1	3	11	1	1	2	3	1	1	3	12	1	1	1	1	1	1	6	29
9	2	1	2	1	2	2	10	2	2	1	2	1	2	2	12	2	1	4	1	2	1	11	33
10	1	4	1	4	1	1	12	1	1	4	1	4	1	1	13	1	1	4	1	4	1	12	37
Var							17.4								39.04							41.57	
																						Suma de varianzas	97.97
																						Varianza General	249.65
																						Valor de Alfa	0.911

Anexo 04

Validación de instrumento Anexo 05

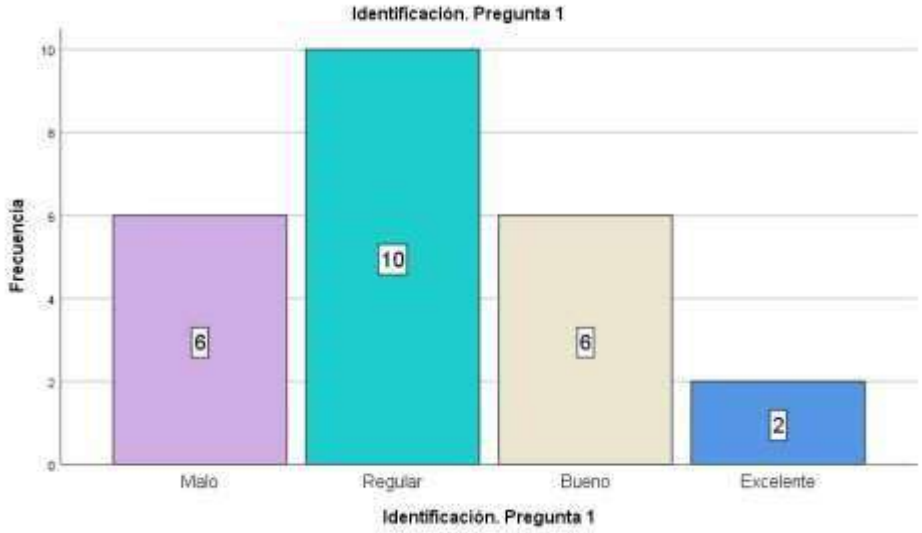
Procesamiento de datos

Identificación. Pregunta 1. ¿Cómo valora la identificación de los activos de información en la Municipalidad Provincial de Huari, 2022?

Tabla 9
Identificación. Pregunta 1

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	6	25,0	25,0	25,0
	Regular	10	41,7	41,7	66,7
	Bueno	6	25,0	25,0	91,7
	Excelente	2	8,3	8,3	100,0
	Total	24	100,0	100,0	

Figura 1
Identificación. Pregunta 1



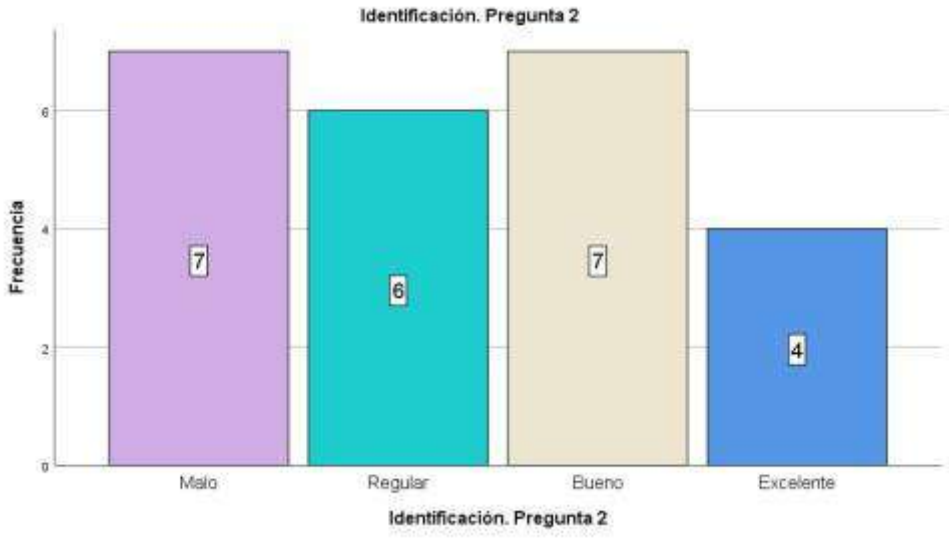
Con referencia a la pregunta sobre cómo valora la identificación de los activos de información en la Municipalidad se tuvo que 6 encuestados (25.0%) que fue malo, 10 de ellos (41.7%) fue regular, 6 encuestados (25.0%) valoraron como que fue bueno y, 2 de ellos (8.3%) manifestaron que fue excelente.

Identificación. Pregunta 2. ¿Cómo califica la identificación de los riesgos de activos de información en la Municipalidad Provincial de Huari, 2022?

Tabla 10
Identificación. Pregunta 2

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	7	29,2	29,2	29,2
	Regular	6	25,0	25,0	54,2
	Bueno	7	29,2	29,2	83,3
	Excelente	4	16,7	16,7	100,0
	Total	24	100,0	100,0	

Figura 2
Identificación. Pregunta 2



Con referencia a la pregunta sobre cómo valora la identificación de los riesgos de activos de información en la Municipalidad se tuvo que 7 encuestados (26.2%) que

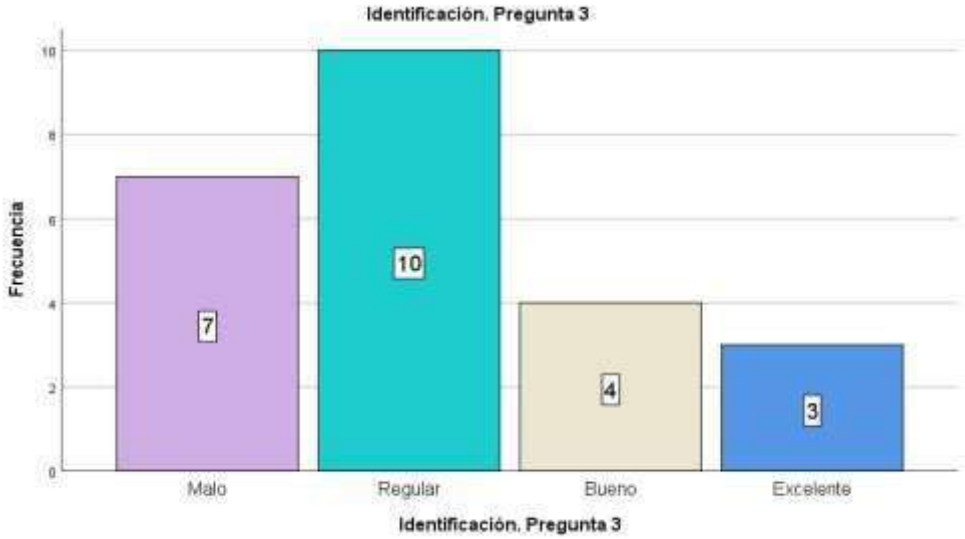
fue malo, 6 de ellos (25.0%) fue regular, 7 encuestados (29.2%) valoraron como que fue bueno y, 4 de ellos (16.7%) manifestaron que fue excelente.

Identificación. Pregunta 3. ¿Cómo evalúa la identificación de las responsabilidades del activo de información en la información en la Municipalidad Provincial de Huari, 2022?

Tabla 11
Identificación. Pregunta 3

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	7	29,2	29,2	29,2
	Regular	10	41,7	41,7	70,8
	Bueno	4	16,7	16,7	87,5
	Excelente	3	12,5	12,5	100,0
	Total	24	100,0	100,0	

Figura 3
Identificación. Pregunta 3



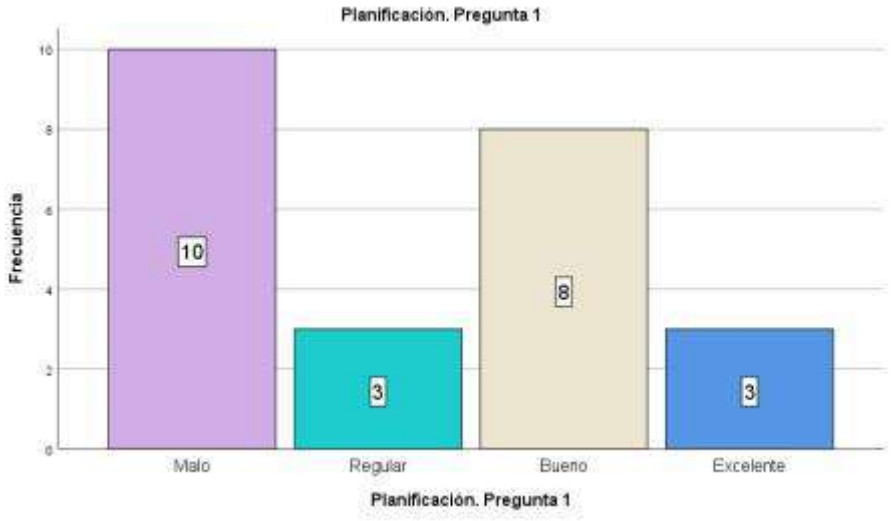
Con referencia a la pregunta sobre cómo valora la identificación de las responsabilidades del activo de información en la información en la Municipalidad se tuvo que 7 encuestados (29.2%) que fue malo, 10 de ellos (41.7%) fue regular, 4 encuestados (16.7%) valoraron como que fue bueno y, 3 de ellos (12.5%) manifestaron que fue excelente.

Planificación. Pregunta 1. ¿Cómo considera la planificación de la seguridad de la información en la Municipalidad Provincial de Huari, 2022?

Tabla 12
Planificación. Pregunta 1

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	10	41,7	41,7	41,7
	Regular	3	12,5	12,5	54,2
	Bueno	8	33,3	33,3	87,5
	Excelente	3	12,5	12,5	100,0
	Total	24	100,0	100,0	

Figura 4
Planificación. Pregunta 1



Con referencia a la pregunta sobre cómo valora la planificación de la seguridad de la información en la Municipalidad se tuvo que 10 encuestados (41.7%) que fue malo, 3 de ellos (12.5%) fue regular, 8 encuestados (33.37%) valoraron como que fue bueno y, 3 de ellos (12.5%) manifestaron que fue excelente.

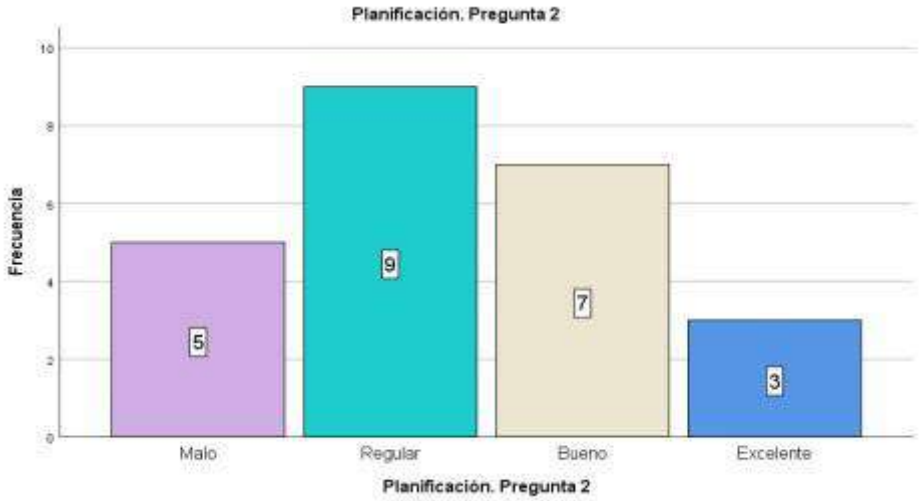
Planificación. Pregunta 2. ¿Cómo evalúa los temas de seguridad de hardware contemplados en el plan de seguridad de información en la Municipalidad Provincial de Huari, 2022?

Tabla 13
Planificación. Pregunta 2

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	5	20,8	20,8	20,8
	Regular	9	37,5	37,5	58,3
	Bueno	7	29,2	29,2	87,5
	Excelente	3	12,5	12,5	100,0

Total	24	100,0	100,0

Figura 5
Planificación. Pregunta 2



Con referencia a la pregunta sobre cómo evalúa los temas de seguridad de hardware contemplados en el plan de seguridad de información en la Municipalidad se tuvo que 5 encuestados (20.8%) que fue malo, 9 de ellos (37.5%) fue regular, 7 encuestados (29.2%) valoraron como que fue bueno y, 3 de ellos (12.5%) manifestaron que fue excelente.

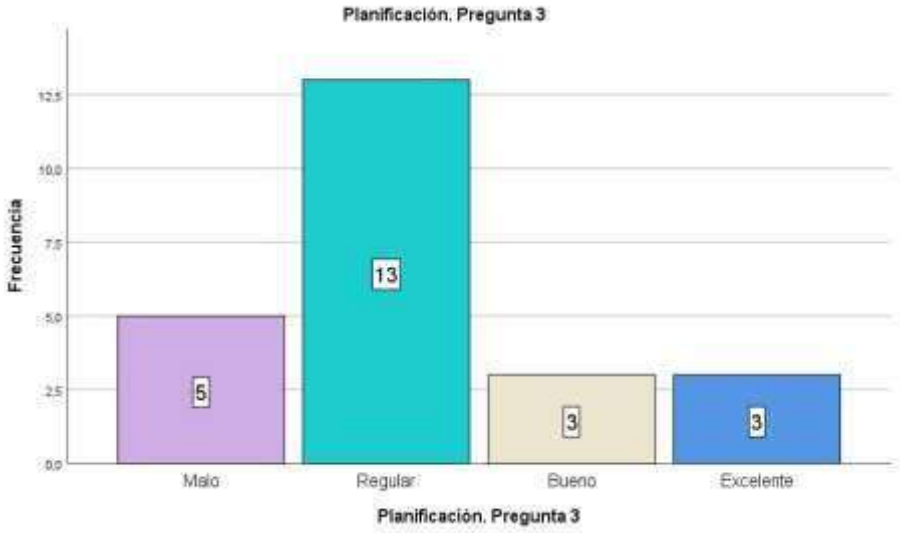
Planificación. Pregunta 3. ¿Cómo califica en las Políticas de seguridad implementadas en el plan de seguridad de la información en la Municipalidad Provincial de Huari, 2022?

Tabla 14
Planificación. Pregunta 3

	Frecuencia	Porcentaje	Porcentaje

					Porcentaje válido acumulado
Válido	Malo	5	20,8	20,8	20,8
	Regular	13	54,2	54,2	75,0
	Bueno	3	12,5	12,5	87,5
	Excelente	3	12,5	12,5	100,0
	Total	24	100,0	100,0	

Figura 6
Planificación. Pregunta 3



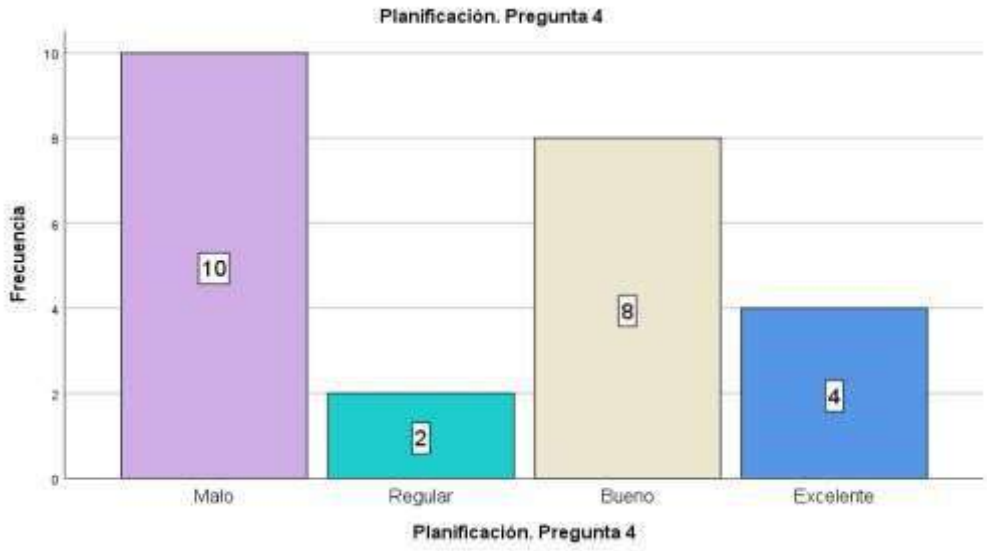
Con referencia a la pregunta sobre cómo califica las Políticas de seguridad implementadas en el plan de seguridad de la información en la Municipalidad se tuvo que 5 encuestados (20.8%) que fue malo, 13 de ellos (54.2%) fue regular, 3 encuestados (12.5%) valoraron como que fue bueno y, 3 de ellos (12.5%) manifestaron que fue excelente.

Planificación. Pregunta 4. ¿Cómo evalúa la capacitación considerada en el plan de seguridad de información en la Municipalidad Provincial de Huari, 2022?

Tabla 15
Planificación. Pregunta 4

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	10	41,7	41,7	41,7
	Regular	2	8,3	8,3	50,0
	Bueno	8	33,3	33,3	83,3
	Excelente	4	16,7	16,7	100,0
	Total	24	100,0	100,0	

Figura 7
Planificación. Pregunta 4



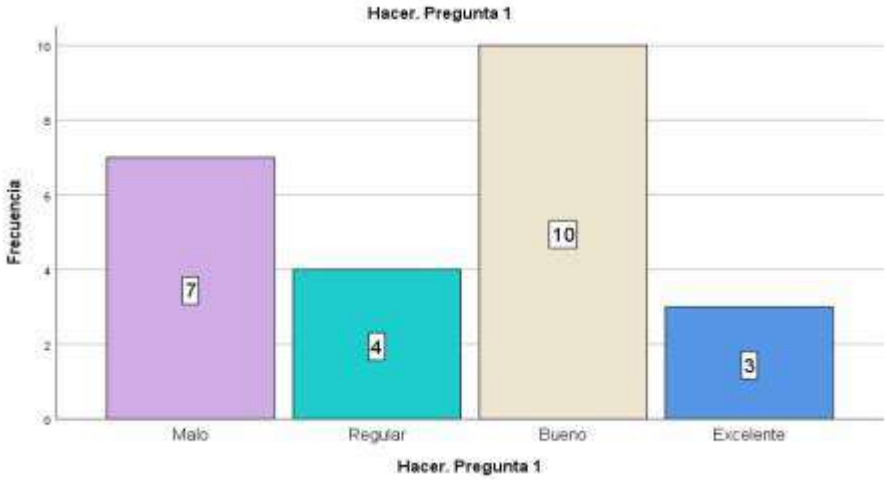
Con referencia a la pregunta sobre cómo evalúa la capacitación considerada en el plan de seguridad de información en la Municipalidad se tuvo que 10 encuestados (41.7%) que fue malo, 2 de ellos (8.3%) fue regular, 8 encuestados (33.3%) valoraron como que fue bueno y, 4 de ellos (16.7%) manifestaron que fue excelente.

Hacer. Pregunta 1. ¿Cómo considera la ejecución de la seguridad a nivel de hardware en el sistema de la información en la Municipalidad Provincial de Huari, 2022?

Tabla 16
Hacer. Pregunta 1

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	7	29,2	29,2	29,2
	Regular	4	16,7	16,7	45,8
	Bueno	10	41,7	41,7	87,5
	Excelente	3	12,5	12,5	100,0
	Total	24	100,0	100,0	

Figura 8
Hacer. Pregunta 1



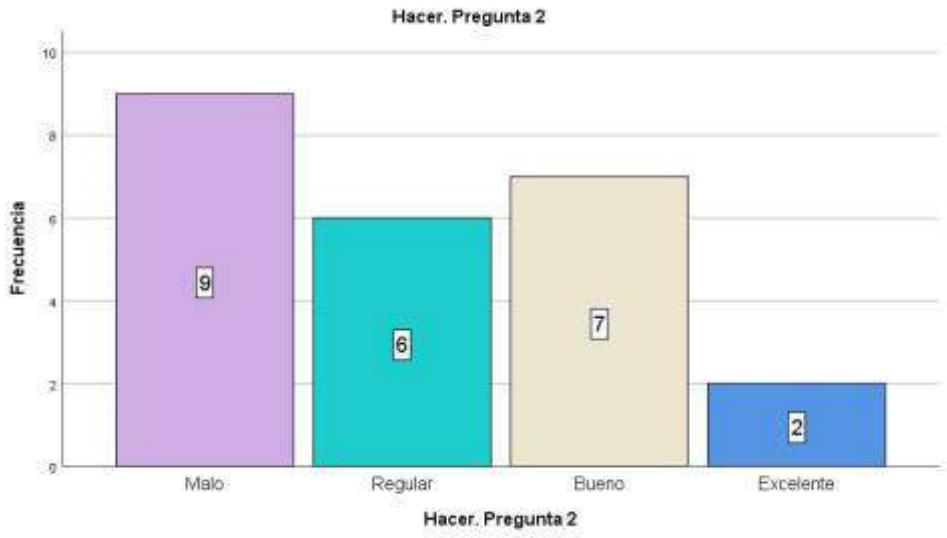
Con referencia a la pregunta sobre cómo considera la ejecución de la seguridad a nivel de hardware en el sistema de la información en la Municipalidad se tuvo que 7 encuestados (29.2%) que fue malo, 4 de ellos (16.7%) fue regular, 10 encuestados (41.7%) valoraron como que fue bueno y, 3 de ellos (12.5%) manifestaron que fue excelente.

Hacer. Pregunta 2. ¿Cómo califica la ejecución de la seguridad a nivel de software en el sistema de la información en la Municipalidad Provincial de Huari, 2022?

Tabla 17
Hacer. Pregunta 2

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	9	37,5	37,5	37,5
	Regular	6	25,0	25,0	62,5
	Bueno	7	29,2	29,2	91,7
	Excelente	2	8,3	8,3	100,0
	Total	24	100,0	100,0	

Figura 9
Hacer. Pregunta 2



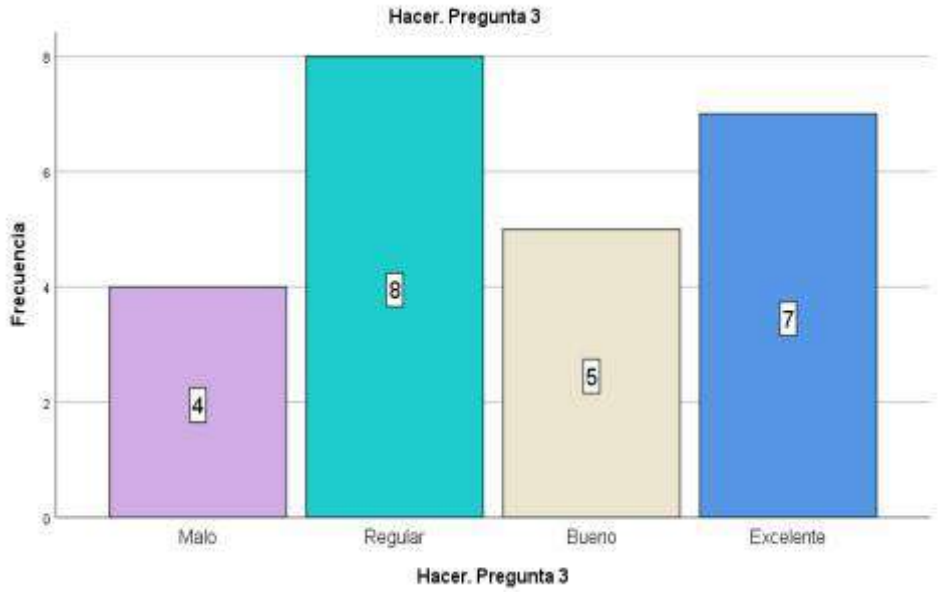
Con referencia a la pregunta sobre cómo califica la ejecución de la seguridad a nivel de software en el sistema de la información en la Municipalidad se tuvo que 9 encuestados (37.5%) que fue malo, 6 de ellos (25.0%) fue regular, 7 encuestados (29.2%) valoraron como que fue bueno y, 2 de ellos (8.3%) manifestaron que fue excelente.

Hacer. Pregunta 3. ¿Cómo valora la ejecución de la seguridad de la información en el sistema de la información en la Municipalidad Provincial de Huari, 2022?

Tabla 18
Hacer. Pregunta 3

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	4	16,7	16,7	16,7
	Regular	8	33,3	33,3	50,0
	Bueno	5	20,8	20,8	70,8
	Excelente	7	29,2	29,2	100,0
	Total	24	100,0	100,0	

Figura 10
Hacer. Pregunta 3



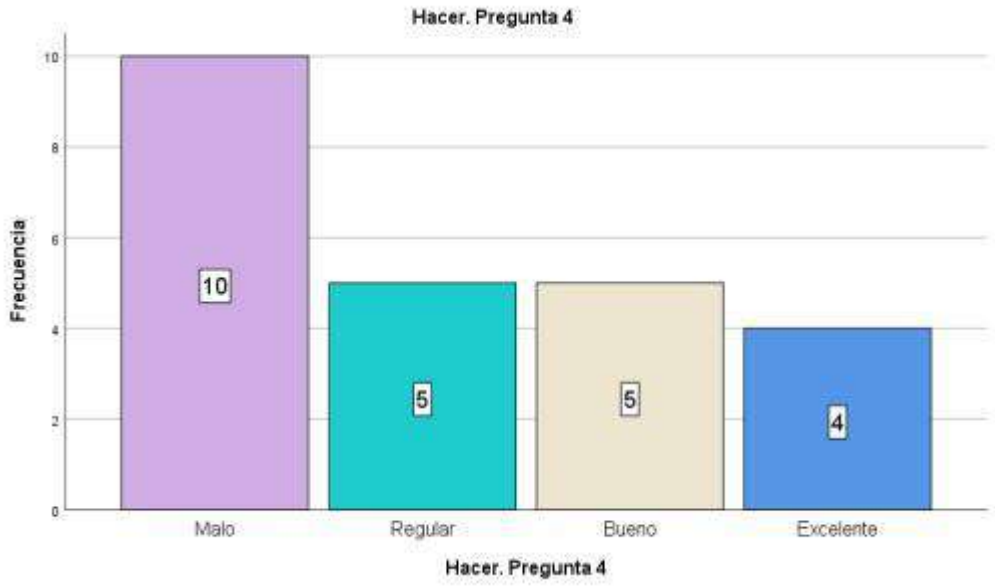
Con referencia a la pregunta sobre cómo valora la ejecución de la seguridad de la información en el sistema de la información en la Municipalidad se tuvo que 4 encuestados (16.7%) que fue malo, 8 de ellos (33.3%) fue regular, 5 encuestados (20.8%) valoraron como que fue bueno y, 7 de ellos (29.2%) manifestaron que fue excelente.

Hacer. Pregunta 4. ¿Cómo evalúa la ejecución de la capacitación en seguridad de la información en la Municipalidad Provincial de Huari, 2022?

Tabla 19
Hacer. Pregunta 4

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	10	41,7	41,7	41,7
	Regular	5	20,8	20,8	62,5
	Bueno	5	20,8	20,8	83,3
	Excelente	4	16,7	16,7	100,0
	Total	24	100,0	100,0	

Figura 11
Hacer. Pregunta 4



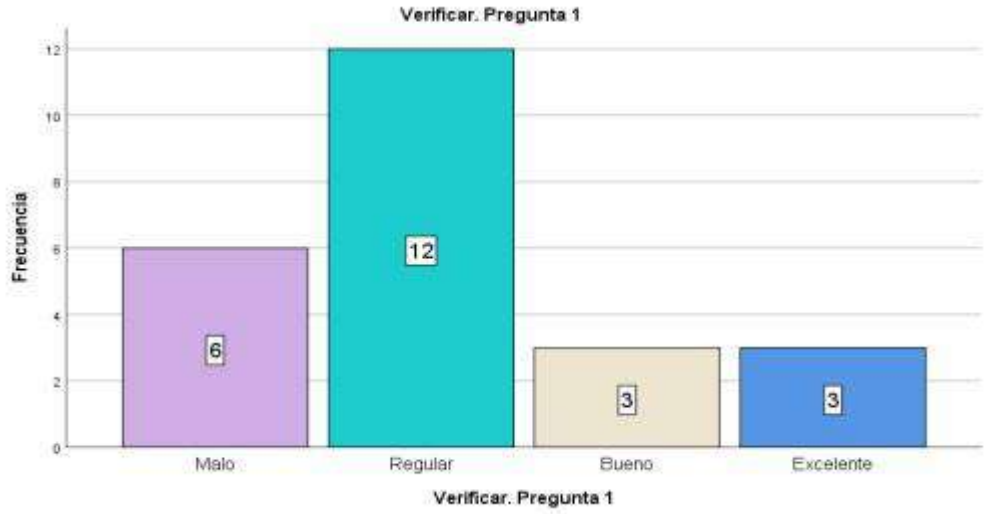
Con referencia a la pregunta sobre cómo evalúa la ejecución de la capacitación en seguridad de la información en la Municipalidad se tuvo que 10 encuestados (41.7%) que fue malo, 5 de ellos (20.8%) fue regular, 5 encuestados (20.8%) valoraron como que fue bueno y, 4 de ellos (16.7%) manifestaron que fue excelente.

Verificar. Pregunta 1. ¿Cómo considera la verificación de la seguridad a nivel de hardware en el sistema de la información en la Municipalidad Provincial de Huari, 2022?

Tabla 20
Verificar. Pregunta 1

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	6	25,0	25,0	25,0
	Regular	12	50,0	50,0	75,0
	Bueno	3	12,5	12,5	87,5
	Excelente	3	12,5	12,5	100,0
	Total	24	100,0	100,0	

Figura 12
Verificar. Pregunta 2



Con referencia a la pregunta sobre cómo considera la verificación de la seguridad a nivel de hardware en el sistema de la información en la Municipalidad se tuvo que

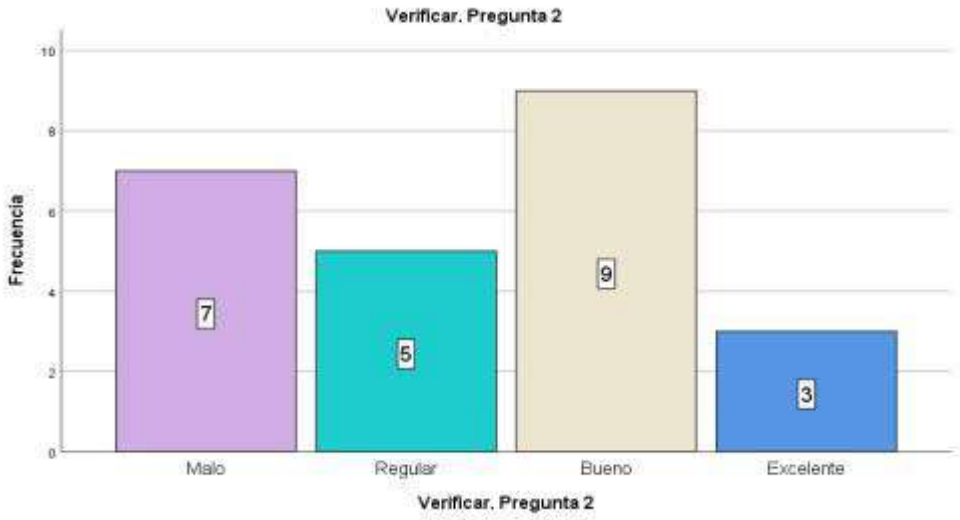
excelente.

6 encuestados (25.0%) que fue malo, 12 de ellos (50.0%) fue regular, 3 encuestados (12.5%) valoraron como que fue bueno y, 3 de ellos (12.5%) manifestaron que fue **Verificar. Pregunta 2.** ¿Cómo califica la verificación de la seguridad a nivel de software en el sistema de la información en la Municipalidad Provincial de Huari, 2022?

Tabla 21
Verificar. Pregunta 2

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	7	29,2	29,2	29,2
	Regular	5	20,8	20,8	50,0
	Bueno	9	37,5	37,5	87,5
	Excelente	3	12,5	12,5	100,0
	Total	24	100,0	100,0	

Figura 13
Verificar. Pregunta 2



Con referencia a la pregunta sobre cómo califica la verificación de la seguridad a excelente.

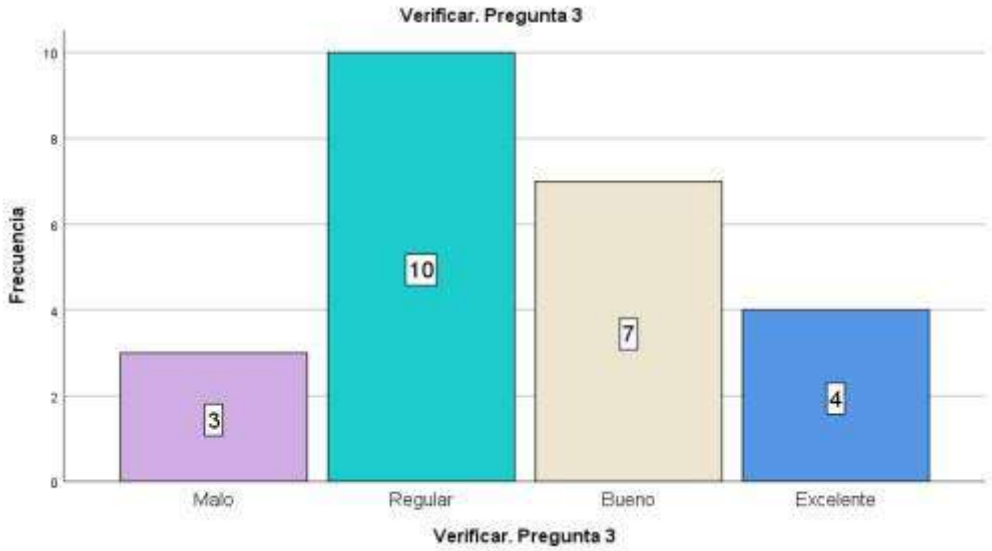
nivel de software en el sistema de la información en la Municipalidad se tuvo que 7 encuestados (29.2%) que fue malo, 5 de ellos (20.8%) fue regular, 9 encuestados (37.5%) valoraron como que fue bueno y, 3 de ellos (12.5%) manifestaron que fue excelente.

Verificar. Pregunta 3. ¿Cómo valora la verificación de la seguridad de la información en el sistema de la información en la Municipalidad Provincial de Huari, 2022?

Tabla 22
Verificar. Pregunta 3

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	3	12,5	12,5	12,5
	Regular	10	41,7	41,7	54,2
	Bueno	7	29,2	29,2	83,3
	Excelente	4	16,7	16,7	100,0
	Total	24	100,0	100,0	

Figura 14
Verificar. Pregunta 3



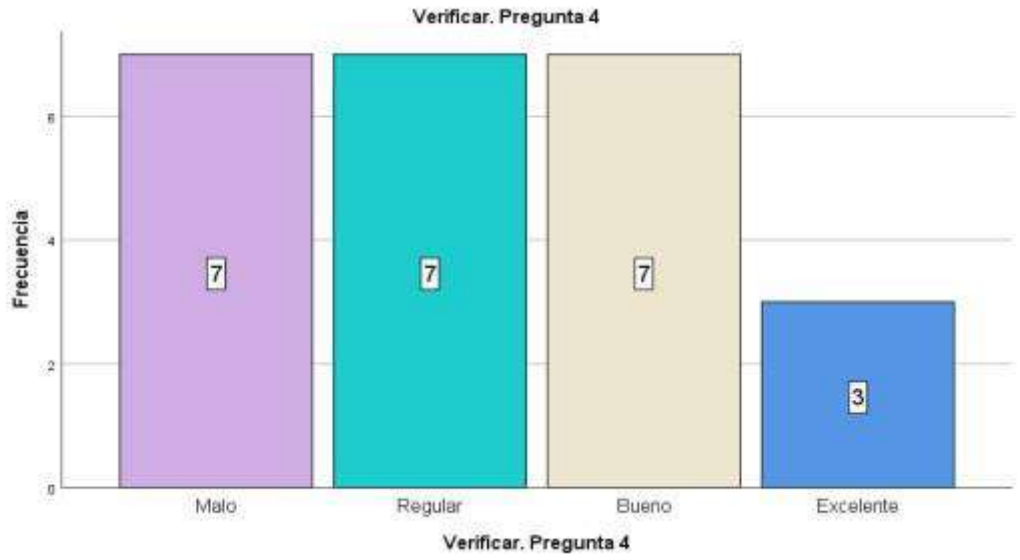
Con referencia a la pregunta sobre cómo valora la verificación de la seguridad de la información en el sistema de la información en la Municipalidad se tuvo que 3 encuestados (12.5%) que fue malo, 10 de ellos (41.7%) fue regular, 7 encuestados (29.2%) valoraron como que fue bueno y, 4 de ellos (16.7%) manifestaron que fue excelente.

Verificar. Pregunta 4. ¿Cómo evalúa la verificación de la capacitación en seguridad de la información en la Municipalidad Provincial de Huari, 2022?

Tabla 23
Verificar. Pregunta 4

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	7	29,2	29,2	29,2
	Regular	7	29,2	29,2	58,3
	Bueno	7	29,2	29,2	87,5
	Excelente	3	12,5	12,5	100,0
	Total	24	100,0	100,0	

Figura 15
Verificar. Pregunta 4



Con referencia a la pregunta sobre cómo evalúa la verificación de la capacitación en seguridad de la información en la Municipalidad se tuvo que 7 encuestados

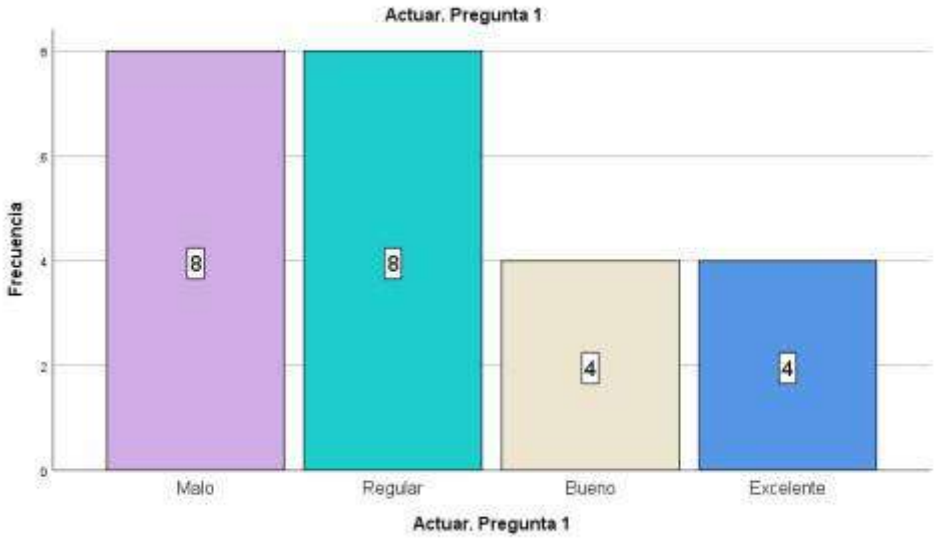
(29.2%) que fue malo, 7 de ellos (29.2%) fue regular, 7 encuestados (29.2%) valoraron como que fue bueno y, 3 de ellos (12.5%) manifestaron que fue excelente.

Actuar. Pregunta 1. ¿Cómo considera el control de la seguridad a nivel de hardware en el sistema de la información en la Municipalidad Provincial de Huari, 2022?

Tabla 24
Actuar. Pregunta 1

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	8	33,3	33,3	33,3
	Regular	8	33,3	33,3	66,7
	Bueno	4	16,7	16,7	83,3
	Excelente	4	16,7	16,7	100,0
	Total	24	100,0	100,0	

Figura 16
Actuar. Pregunta 1



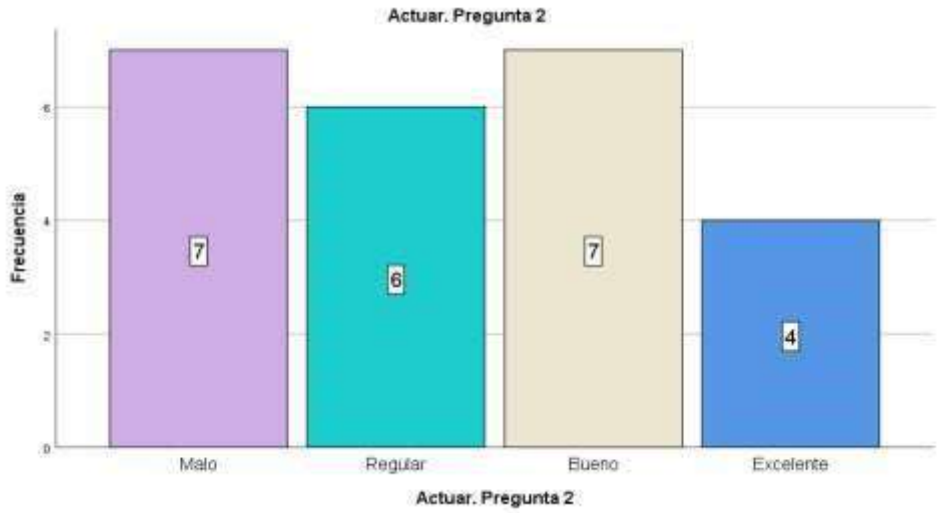
Con referencia a la pregunta sobre cómo considera el control de la seguridad a nivel de hardware en el sistema de la información en la Municipalidad se tuvo que 8 encuestados (33.3%) que fue malo, 8 de ellos (33.3%) fue regular, 4 encuestados (16.7%) valoraron como que fue bueno y, 4 de ellos (16.7%) manifestaron que fue excelente.

Actuar. Pregunta 2. ¿Cómo califica el control de la seguridad a nivel de software en el sistema de la información en la Municipalidad Provincial de Huari, 2022?

Tabla 25
Actuar. Pregunta 2

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	7	29,2	29,2	29,2
	Regular	6	25,0	25,0	54,2
	Bueno	7	29,2	29,2	83,3
	Excelente	4	16,7	16,7	100,0
	Total	24	100,0	100,0	

Figura 17
Actuar. Pregunta 2



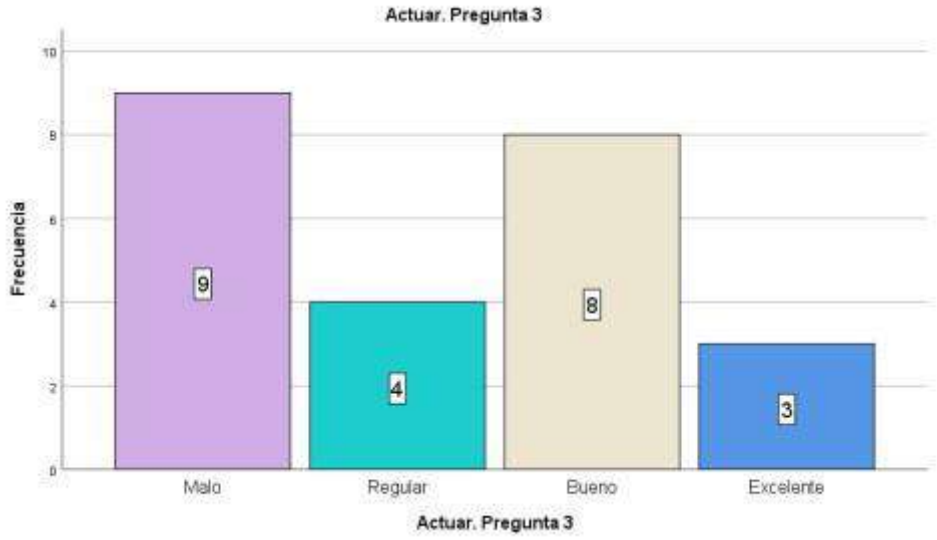
Con referencia a la pregunta sobre cómo califica el control de la seguridad a nivel de software en el sistema de la información en la Municipalidad se tuvo que 7 encuestados (29.2%) que fue malo, 6 de ellos (25.0%) fue regular, 7 encuestados (29.2%) valoraron como que fue bueno y, 4 de ellos (16.7%) manifestaron que fue excelente.

Actuar. Pregunta 3. ¿Cómo valora el control de la seguridad de la información en el sistema de la información en la Municipalidad Provincial de Huari, 2022?

Tabla 26
Actuar. Pregunta 3

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	9	37,5	37,5	37,5
	Regular	4	16,7	16,7	54,2
	Bueno	8	33,3	33,3	87,5
	Excelente	3	12,5	12,5	100,0
	Total	24	100,0	100,0	

Figura 18
Actuar. Pregunta 3



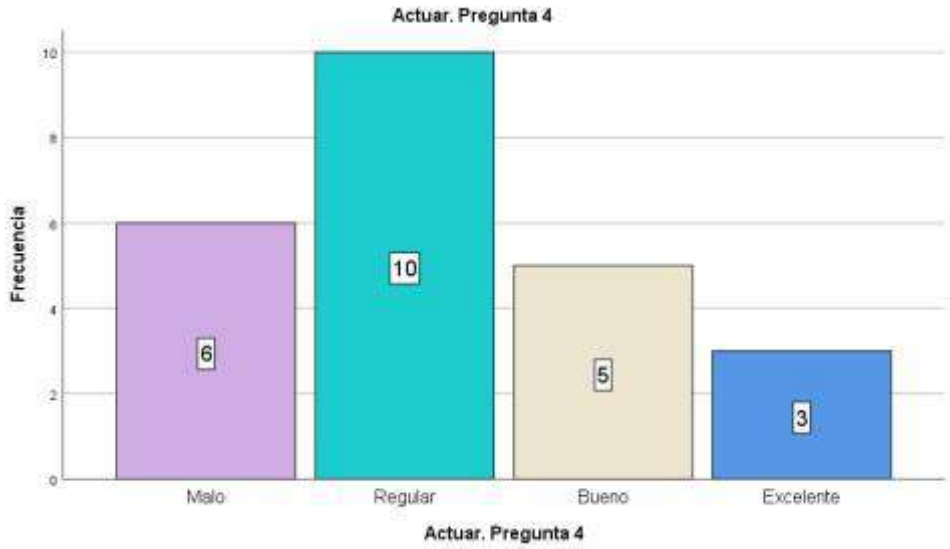
Con referencia a la pregunta sobre cómo valora el control de la seguridad de la información en el sistema de la información en la Municipalidad se tuvo que 9 encuestados (37.5%) que fue malo, 4 de ellos (16.7%) fue regular, 8 encuestados (33.3%) valoraron como que fue bueno y, 3 de ellos (12.5%) manifestaron que fue excelente.

Actuar. Pregunta 4. ¿Cómo evalúa el control de la capacitación en seguridad de la información en la Municipalidad Provincial de Huari, 2022?

Tabla 27
Actuar. Pregunta 4

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	6	25,0	25,0	25,0
	Regular	10	41,7	41,7	66,7
	Bueno	5	20,8	20,8	87,5
	Excelente	3	12,5	12,5	100,0
	Total	24	100,0	100,0	

Figura 19
Actuar. Pregunta 4



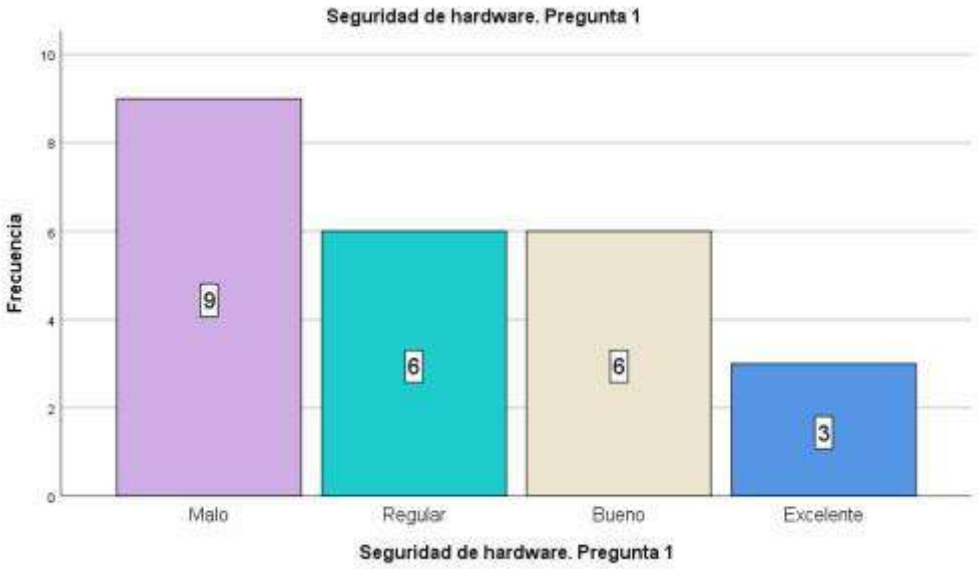
Con referencia a la pregunta sobre cómo evalúa el control de la capacitación en seguridad de la información en la Municipalidad se tuvo que 6 encuestados (25.0%) que fue malo, 10 de ellos (41.7%) fue regular, 5 encuestados (20.8%) valoraron como que fue bueno y, 3 de ellos (12.5%) manifestaron que fue excelente.

Seguridad de hardware. Pregunta 1. ¿Cómo califica la seguridad física del sistema de información de la Municipalidad Provincial de Huari, 2022?

Tabla 28
Seguridad de hardware. Pregunta 1

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	9	37,5	37,5	37,5
	Regular	6	25,0	25,0	62,5
	Bueno	6	25,0	25,0	87,5
	Excelente	3	12,5	12,5	100,0
	Total	24	100,0	100,0	

Figura 20
Seguridad de hardware. Pregunta 1



Con referencia a la pregunta sobre cómo califica la seguridad física del sistema de información de la Municipalidad se tuvo que 9 encuestados (37.5%) que fue malo, 6 de ellos (25.0%) fue regular, 6 encuestados (25.0%) valoraron como que fue bueno y, 3 de ellos (12.5%) manifestaron que fue excelente.

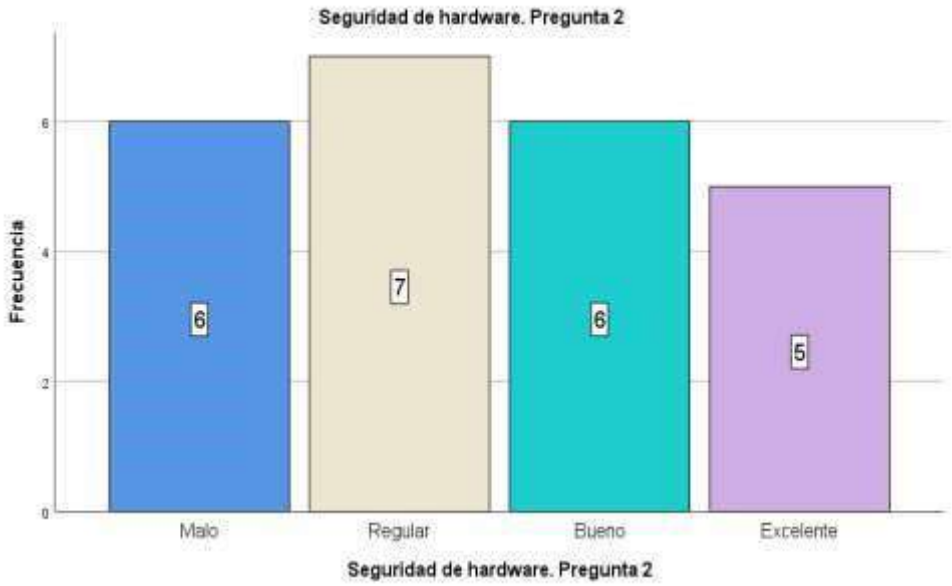
Seguridad de hardware. Pregunta 2. ¿Cómo considera la seguridad en el servidor de red del sistema de información de la Municipalidad Provincial de Huari, 2022?

Tabla 29
Seguridad de hardware. Pregunta 2

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	6	25,0	25,0	25,0
	Regular	7	29,2	29,2	54,2
	Bueno	6	25,0	25,0	79,2

Excelente	5	20,8	20,8	100,0
Total	24	100,0	100,0	

Figura 21
Seguridad de hardware. Pregunta 2



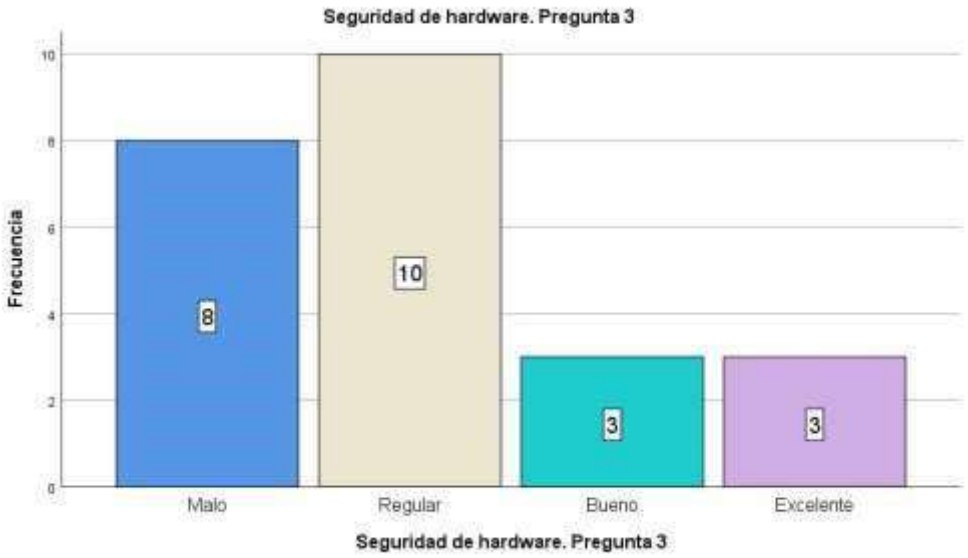
Con referencia a la pregunta sobre cómo considera la seguridad en el servidor de red del sistema de información de la Municipalidad se tuvo que 6 encuestados (25.0%) que fue malo, 7 de ellos (29.2%) fue regular, 6 encuestados (25.0%) valoraron como que fue bueno y, 5 de ellos (20.8%) manifestaron que fue excelente.

Seguridad de hardware. Pregunta 3. ¿Cómo valora la seguridad en el servidor de base de datos sistema de información de la Municipalidad Provincial de Huari, 2022?

Tabla 30
Seguridad de hardware. Pregunta 3

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	8	33,3	33,3	33,3
	Regular	10	41,7	41,7	75,0
	Bueno	3	12,5	12,5	87,5
	Excelente	3	12,5	12,5	100,0
	Total	24	100,0	100,0	

Figura 22
Seguridad de hardware. Pregunta 3



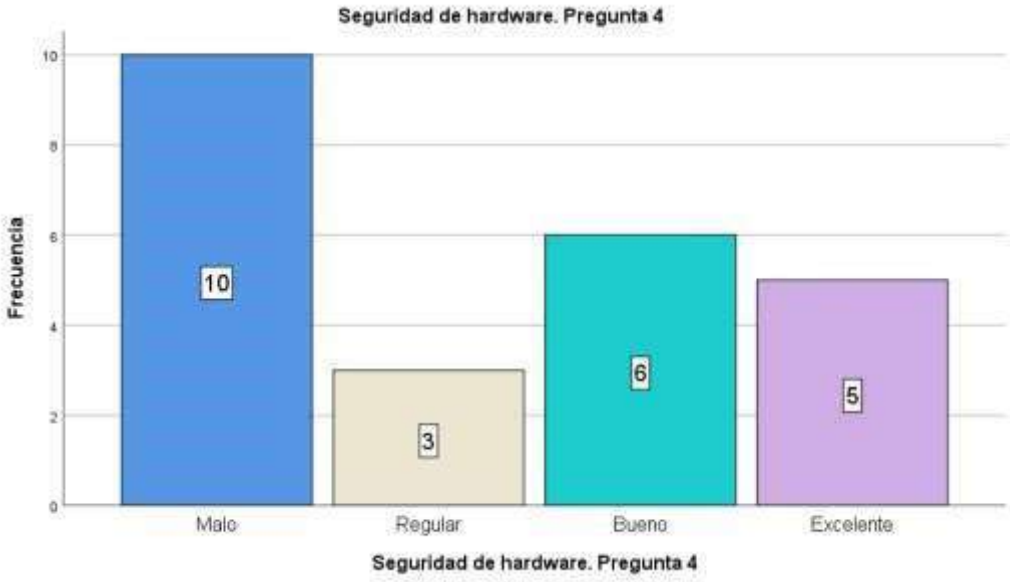
Con referencia a la pregunta sobre cómo valora la seguridad en el servidor de base de datos sistema de información de la Municipalidad se tuvo que 8 encuestados (33.3%) que fue malo, 10 de ellos (41.7%) fue regular, 3 encuestados (12.5%) valoraron como que fue bueno y, 3 de ellos (12.5%) manifestaron que fue excelente.

Seguridad de hardware. Pregunta 4. ¿Cómo evalúa la seguridad del sistema de cableado del sistema de información de la Municipalidad Provincial de Huari, 2022?

Tabla 31
Seguridad de hardware. Pregunta 4

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje válido acumulado
Válido	Malo	10	41,7	41,7	41,7
	Regular	3	12,5	12,5	54,2
	Bueno	6	25,0	25,0	79,2
	Excelente	5	20,8	20,8	100,0
	Total	24	100,0	100,0	

Figura 23
Seguridad de hardware. Pregunta 4



Con referencia a la pregunta sobre cómo evalúa la seguridad del sistema de cableado del sistema de información de la Municipalidad se tuvo que 10 encuestados (41.7%) que fue malo, 3 de ellos (12.5%) fue regular, 6 encuestados

(25.0%) valoraron como que fue bueno y, 5 de ellos (20.8%) manifestaron que fue

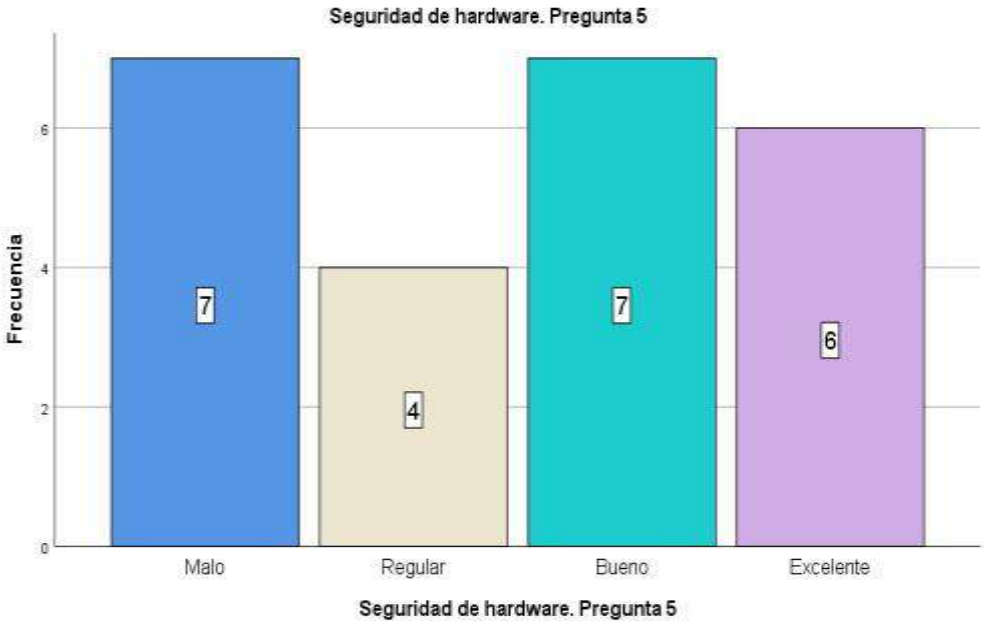
Seguridad de hardware. Pregunta 5. ¿Cómo califica la seguridad de los Access point del sistema de información de la Municipalidad Provincial de Huari, 2022?

Tabla 32
Seguridad de hardware. Pregunta 5

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	7	29,2	29,2	29,2
	Regular	4	16,7	16,7	45,8
	Bueno	7	29,2	29,2	75,0
	Excelente	6	25,0	25,0	100,0
	Total	24	100,0	100,0	

Figura 24
Seguridad de hardware. Pregunta 5

excelente.



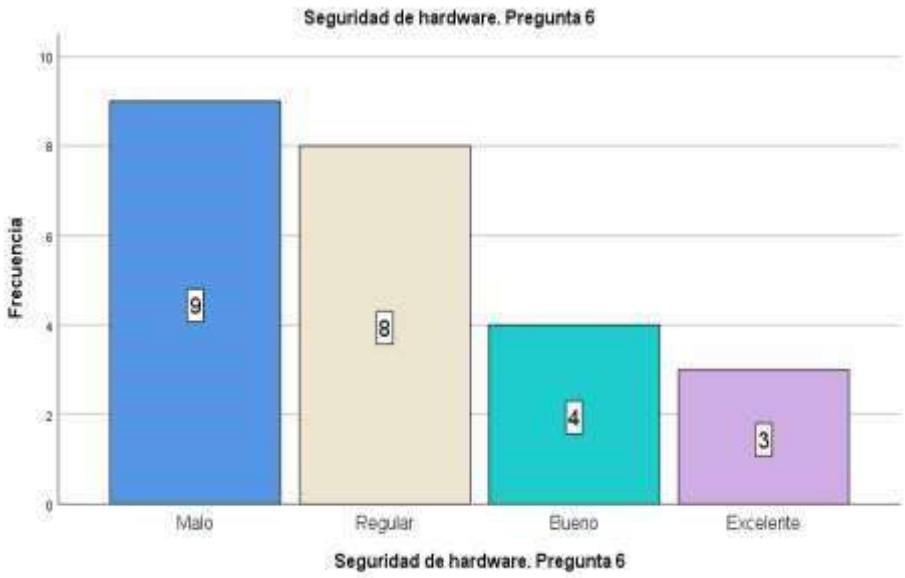
Con referencia a la pregunta sobre cómo califica la seguridad de los Access point del sistema de información de la Municipalidad se tuvo que 7 encuestados (29.2%) que fue malo, 4 de ellos (16.7%) fue regular, 7 encuestados (29.2%) valoraron como que fue bueno y, 6 de ellos (25.0%) manifestaron que fue excelente.

Seguridad de hardware. Pregunta 6. ¿Cómo considera la seguridad de la computadora de escritorio del sistema de información de la Municipalidad Provincial de Huari, 2022?

Tabla 33
Seguridad de hardware. Pregunta 6

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	9	37,5	37,5	37,5
	Regular	8	33,3	33,3	70,8
	Bueno	4	16,7	16,7	87,5
	Excelente	3	12,5	12,5	100,0
	Total	24	100,0	100,0	

Figura 25
Seguridad de hardware. Pregunta 6



Con referencia a la pregunta sobre cómo considera la seguridad de la computadora de escritorio del sistema de información de la Municipalidad se tuvo que 9

encuestados (37.5%) que fue malo, 8 de ellos (33.3%) fue regular, 4 encuestados (16.7%) valoraron como que fue bueno y, 3 de ellos (12.5%) manifestaron que fue **Seguridad de software. Pregunta 1.** ¿Cómo califica la seguridad del sistema operativo del sistema de información de la Municipalidad Provincial de Huari, 2022?

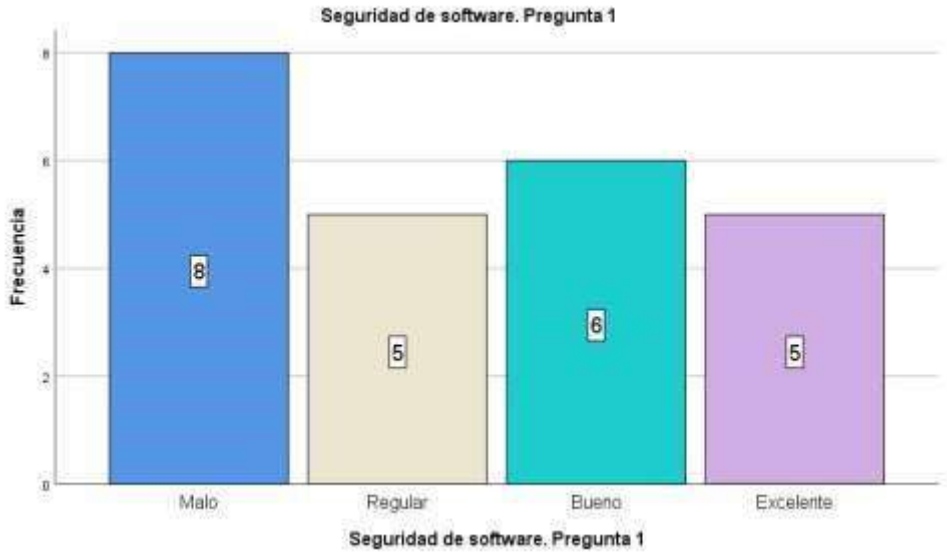
Tabla 34
Seguridad de software. Pregunta 1

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje válido acumulado

excelente.

	Malo	8	33,3	33,3	33,3
	Regular	5	20,8	20,8	54,2
Válido	Bueno	6	25,0	25,0	79,2
	Excelente	5	20,8	20,8	100,0
	Total	24	100,0	100,0	

Figura 26
Seguridad de software. Pregunta 1



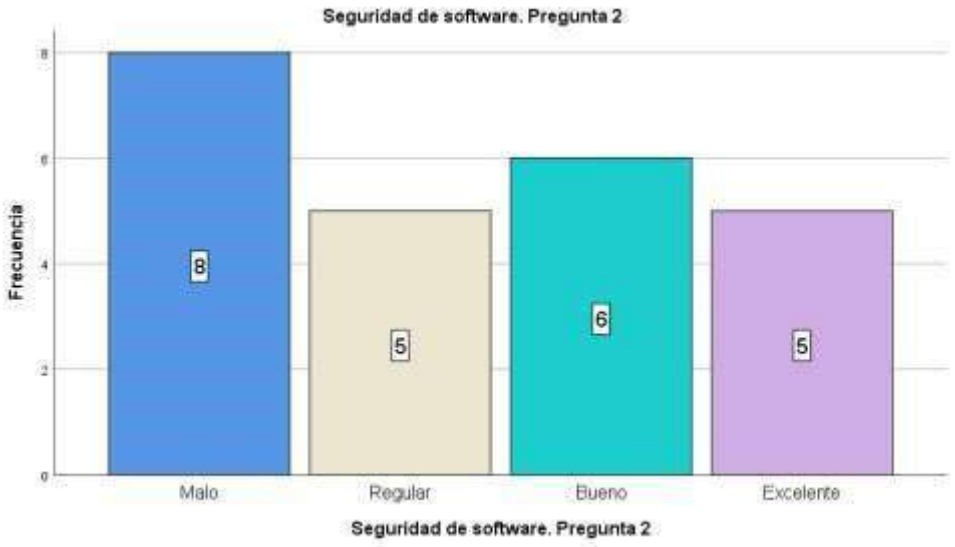
Con referencia a la pregunta sobre cómo califica la seguridad del sistema operativo del sistema de información de la Municipalidad se tuvo que 8 encuestados (33.3%) que fue malo, 5 de ellos (20.8%) fue regular, 6 encuestados (25.0%) valoraron como que fue bueno y, 5 de ellos (20.8%) manifestaron que fue excelente.

Seguridad de software. Pregunta 2. ¿Cómo considera la seguridad del software de procesamiento de texto del sistema de información de la Municipalidad Provincial de Huari, 2022?

Tabla 35
Seguridad de software. Pregunta 2

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje válido acumulado
Válido	Malo	8	33,3	33,3	33,3
	Regular	5	20,8	20,8	54,2
	Bueno	6	25,0	25,0	79,2
	Excelente	5	20,8	20,8	100,0
	Total	24	100,0	100,0	

Figura 27
Seguridad de software. Pregunta 2



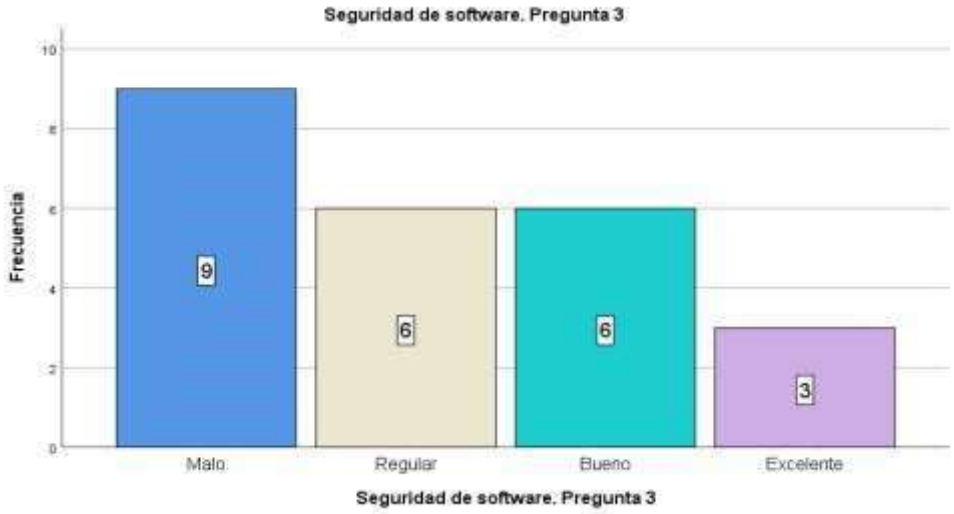
Con referencia a la pregunta sobre cómo considera la seguridad del software de procesamiento de texto del sistema de información de la Municipalidad se tuvo que 8 encuestados (33.3%) que fue malo, 5 de ellos (20.8%) fue regular, 6 encuestados excelente.

(25.0%) valoraron como que fue bueno y, 5 de ellos (20.8%) manifestaron que fue **Seguridad de software. Pregunta 3.** ¿Cómo valora la seguridad del sistema de base de datos del sistema de información de la Municipalidad Provincial de Huari, 2022?

Tabla 36
Seguridad de software. Pregunta 3

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	9	37,5	37,5	37,5
	Regular	6	25,0	25,0	62,5
	Bueno	6	25,0	25,0	87,5
	Excelente	3	12,5	12,5	100,0
	Total	24	100,0	100,0	

Figura 28
Seguridad de software. Pregunta 3



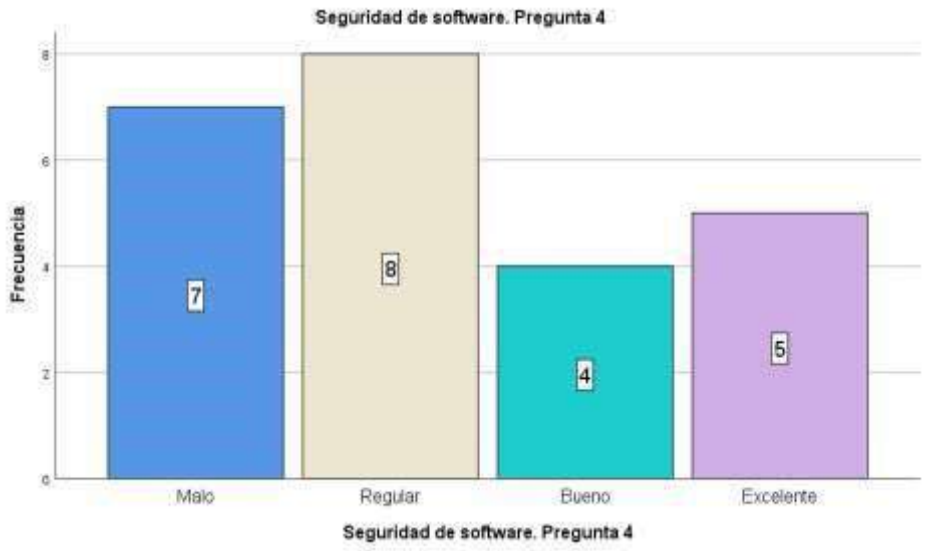
Con referencia a la pregunta sobre cómo valora la seguridad del sistema de base de datos del sistema de información de la Municipalidad se tuvo que 9 encuestados (37.5%) que fue malo, 6 de ellos (25.0%) fue regular, 6 encuestados (25.0%) valoraron como que fue bueno y, 3 de ellos (12.5%) manifestaron que fue excelente.

Seguridad de software. Pregunta 4. ¿Cómo evalúa la seguridad de la información sensible y más importante en el sistema de información de la Municipalidad Provincial de Huari, 2022?

Tabla 37
Seguridad de software. Pregunta 4

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	7	29,2	29,2	29,2
	Regular	8	33,3	33,3	62,5
	Bueno	4	16,7	16,7	79,2
	Excelente	5	20,8	20,8	100,0
	Total	24	100,0	100,0	

Figura 29
Seguridad de software. Pregunta 4



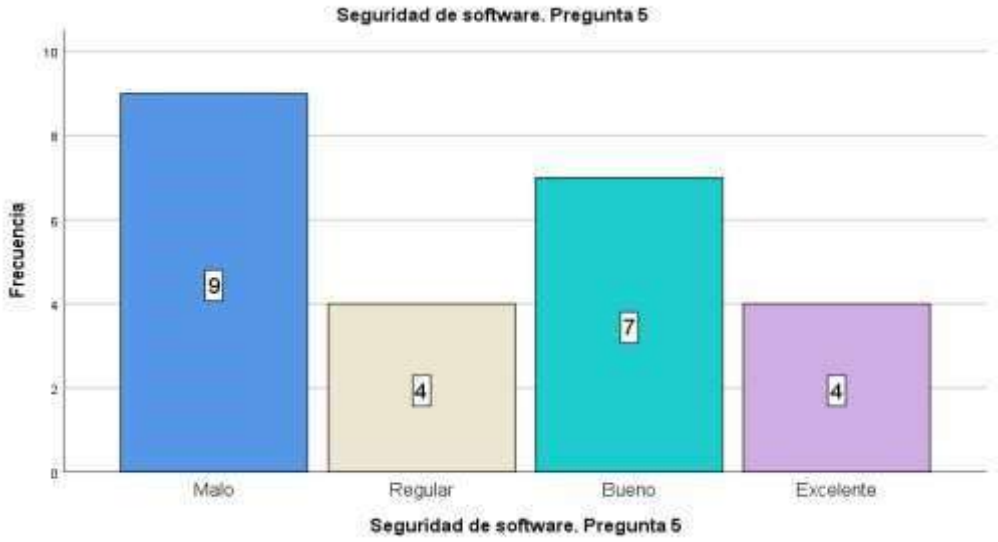
Con referencia a la pregunta sobre cómo evalúa la seguridad de la información sensible y más importante en el sistema de información de la Municipalidad se tuvo que 7 encuestados (29.2%) que fue malo, 8 de ellos (33.3%) fue regular, 4 encuestados (16.7%) valoraron como que fue bueno y, 5 de ellos (20.8%) manifestaron que fue excelente.

Seguridad de software. Pregunta 5. ¿Cómo califica el nivel de protección del software antivirus en el sistema de información de la Municipalidad Provincial de Huari, 2022?

Tabla 38
Seguridad de software. Pregunta 5

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	9	37,5	37,5	37,5
	Regular	4	16,7	16,7	54,2
	Bueno	7	29,2	29,2	83,3
	Excelente	4	16,7	16,7	100,0
	Total	24	100,0	100,0	

Figura 30
Seguridad de software. Pregunta 5



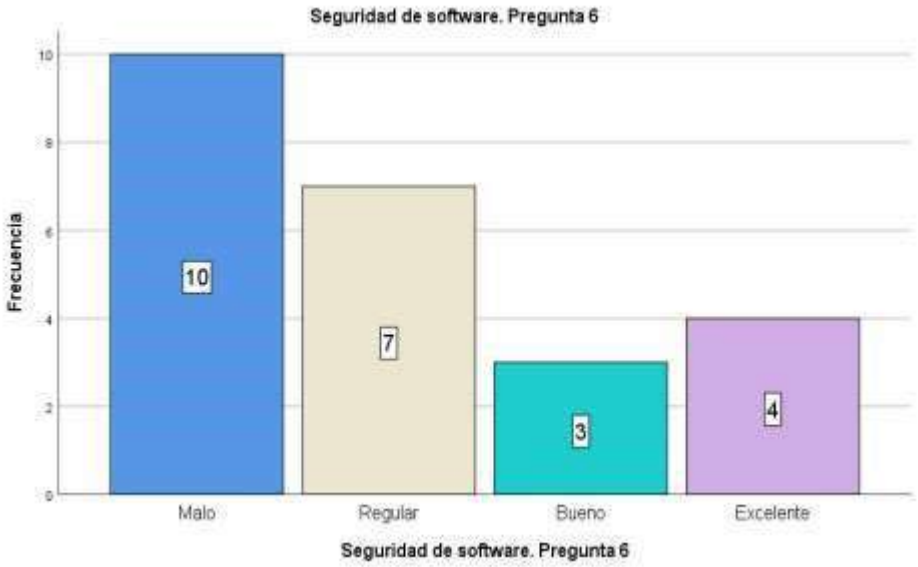
Con referencia a la pregunta sobre cómo evalúa la seguridad de la información sensible y más importante en el sistema de información de la Municipalidad se tuvo que 9 encuestados (37.5%) que fue malo, 4 de ellos (16.7%) fue regular, 7 encuestados (29.2%) valoraron como que fue bueno y, 4 de ellos (16.7%) manifestaron que fue excelente.

Seguridad de software. Pregunta 6. ¿Cómo considera la seguridad del software frente a ataques internos o externos en el sistema de información de la Municipalidad Provincial de Huari, 2022?

Tabla 39
Seguridad de software. Pregunta 6

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	10	41,7	41,7	41,7
	Regular	7	29,2	29,2	70,8
	Bueno	3	12,5	12,5	83,3
	Excelente	4	16,7	16,7	100,0
	Total	24	100,0	100,0	

Figura 31
Seguridad de software. Pregunta 6



Con referencia a la pregunta sobre cómo considera la seguridad del software frente a ataques internos o externos en el sistema de información de la Municipalidad se tuvo que 10 encuestados (41.7%) que fue malo, 7 de ellos (29.2%) fue regular, 3 encuestados (12.5%) valoraron como que fue bueno y, 4 de ellos (16.7%) manifestaron que fue excelente.

Seguridad de software. Pregunta 7. ¿Cómo califica la seguridad lógica en general del sistema de información de la Municipalidad Provincial de Huari, 2022?

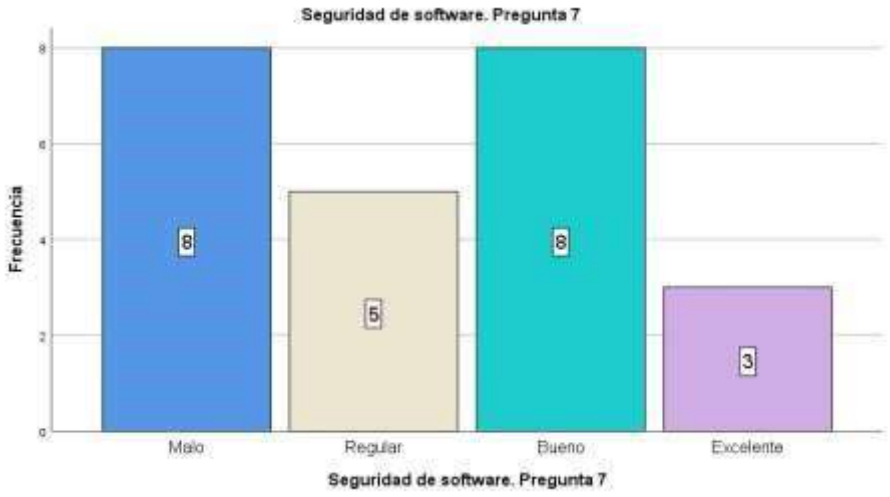
Tabla 40

Seguridad de software. Pregunta 7

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	8	33,3	33,3	33,3
	Regular	5	20,8	20,8	54,2
	Bueno	8	33,3	33,3	87,5
	Excelente	3	12,5	12,5	100,0
	Total	24	100,0	100,0	

Figura 32

Seguridad de software. Pregunta 7



Con referencia a la pregunta sobre cómo califica la seguridad lógica en general del sistema de información de la Municipalidad se tuvo que 8 encuestados (33.3%) que

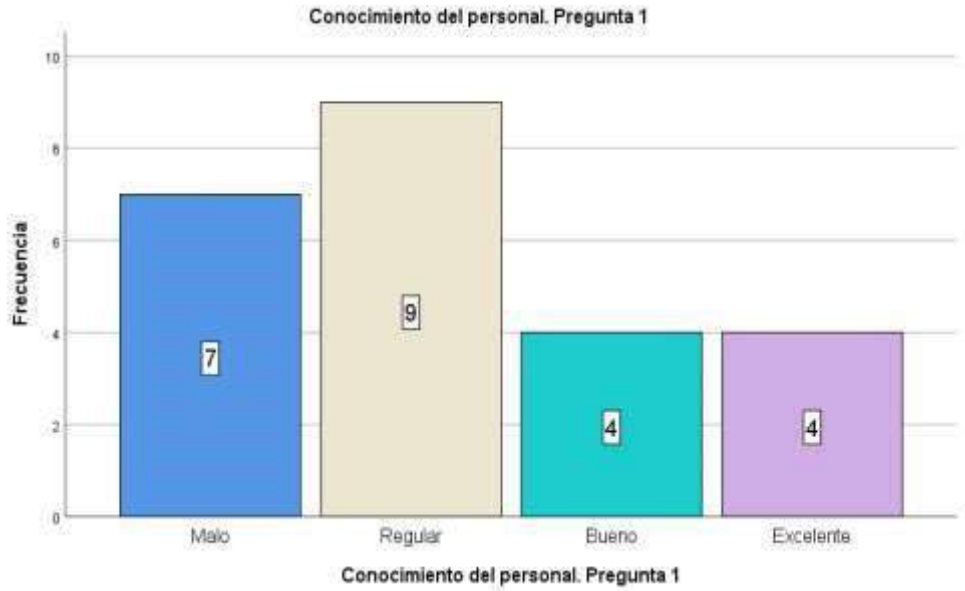
fue malo, 5 de ellos (20.8%) fue regular, 8 encuestados (33.3%) valoraron como que fue bueno y, 3 de ellos (12.5%) manifestaron que fue excelente.

Conocimiento del personal. Pregunta 1. ¿Cómo califica el dominio de hardware por parte del personal de la Municipalidad Provincial de Huari, 2022?

Tabla 41
Conocimiento del personal. Pregunta 1

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	7	29,2	29,2	29,2
	Regular	9	37,5	37,5	66,7
	Bueno	4	16,7	16,7	83,3
	Excelente	4	16,7	16,7	100,0
	Total	24	100,0	100,0	

Figura 33
Conocimiento del personal. Pregunta 1



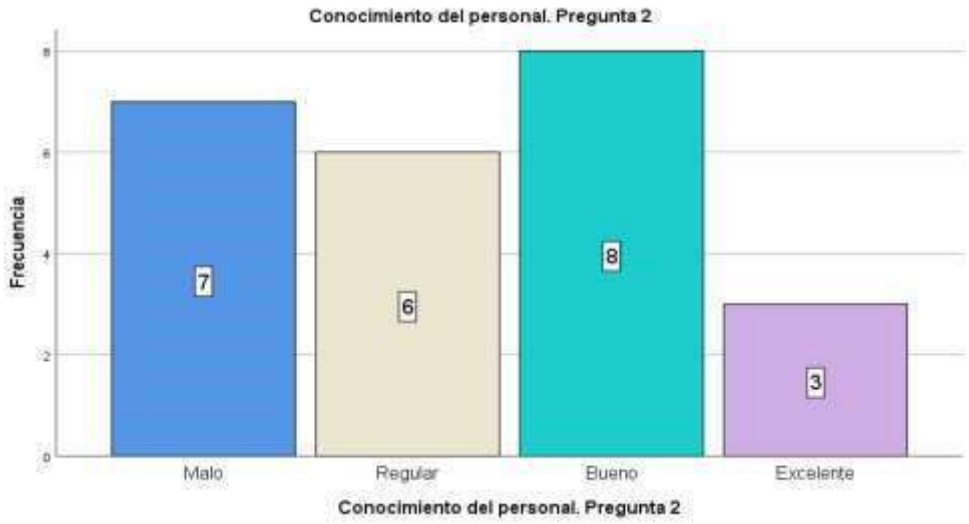
Con referencia a la pregunta sobre cómo califica el dominio de hardware por parte del personal de la Municipalidad se tuvo que 7 encuestados (29.2%) que fue malo, 9 de ellos (37.5%) fue regular, 4 encuestados (16.7%) valoraron como que fue bueno y, 4 de ellos (16.7%) manifestaron que fue excelente.

Conocimiento del personal. Pregunta 2. ¿Cómo considera el dominio del software por parte del personal de la Municipalidad Provincial de Huari, 2022?

Tabla 42
Conocimiento del personal. Pregunta 2

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	7	29,2	29,2	29,2
	Regular	6	25,0	25,0	54,2
	Bueno	8	33,3	33,3	87,5
	Excelente	3	12,5	12,5	100,0
	Total	24	100,0	100,0	

Figura 34
Conocimiento del personal. Pregunta 2



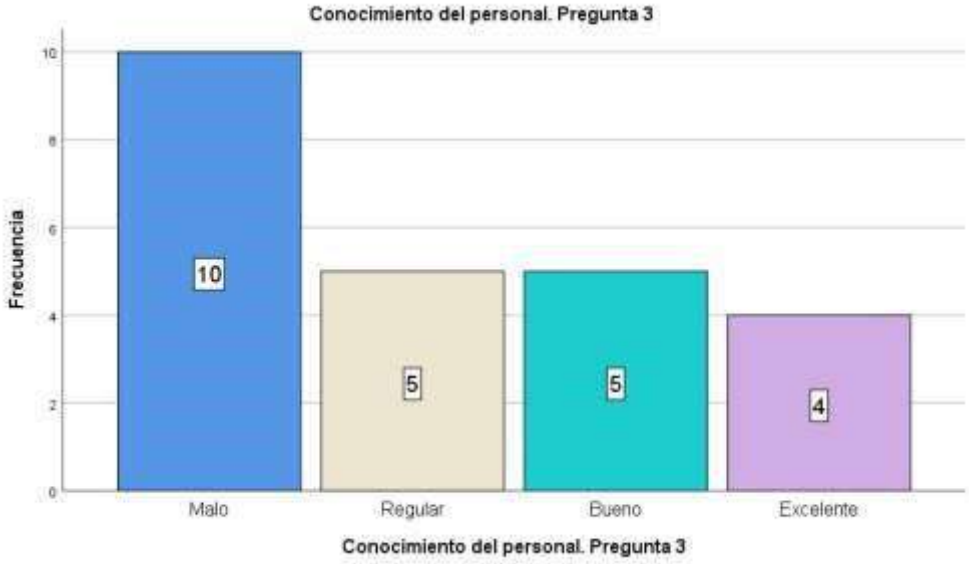
Con referencia a la pregunta sobre cómo considera el dominio del software por parte del personal de la Municipalidad se tuvo que 7 encuestados (29.2%) que fue malo, 6 de ellos (25.0%) fue regular, 8 encuestados (33.3%) valoraron como que fue bueno y, 3 de ellos (12.5%) manifestaron que fue excelente.

Conocimiento del personal. Pregunta 3. ¿Cómo valora la administración de las claves de acceso al sistema por parte del personal de la Municipalidad Provincial de Huari, 2022?

Tabla 43
Conocimiento del personal. Pregunta 3

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	10	41,7	41,7	41,7
	Regular	5	20,8	20,8	62,5
	Bueno	5	20,8	20,8	83,3
	Excelente	4	16,7	16,7	100,0
	Total	24	100,0	100,0	

Figura 35
Conocimiento del personal. Pregunta 3



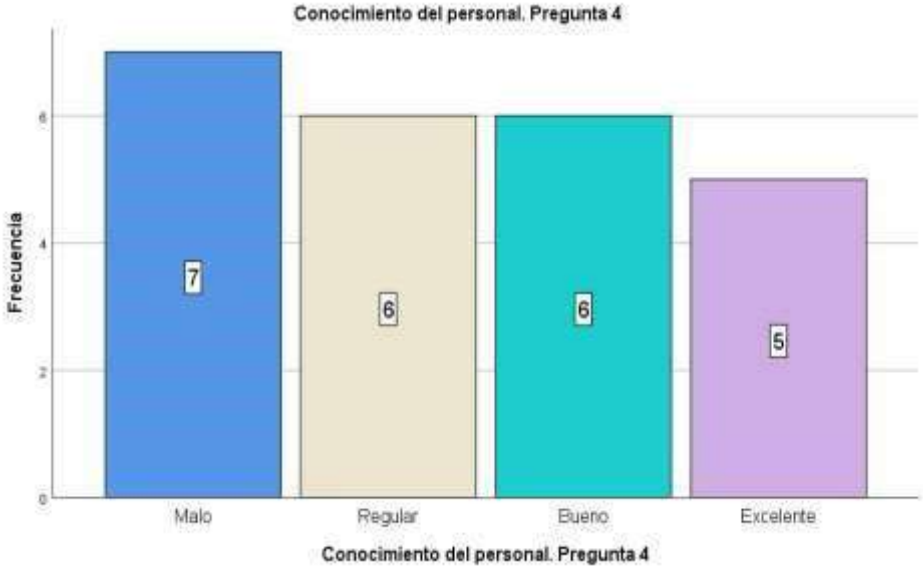
Con referencia a la pregunta sobre cómo valora la administración de las claves de acceso al sistema por parte del personal de la Municipalidad se tuvo que 10 encuestados (41.7%) que fue malo, 5 de ellos (20.8%) fue regular, 5 encuestados (20.8%) valoraron como que fue bueno y, 4 de ellos (16.7%) manifestaron que fue excelente.

Conocimiento del personal. Pregunta 4. ¿Cómo evalúa el dominio de la seguridad informática del personal de la Municipalidad Provincial de Huari, 2022?

Tabla 44
Conocimiento del personal. Pregunta 4

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	7	29,2	29,2	29,2
	Regular	6	25,0	25,0	54,2
	Bueno	6	25,0	25,0	79,2
	Excelente	5	20,8	20,8	100,0
	Total	24	100,0	100,0	

Figura 36
Conocimiento del personal. Pregunta 4



Con referencia a la pregunta sobre cómo evalúa el dominio de la seguridad informática del personal de la Municipalidad se tuvo que 7 encuestados (29.2%) que fue malo, 6 de ellos (25.0%) fue regular, 6 encuestados (25.0%) valoraron como que fue bueno y, 5 de ellos (20.8%) manifestaron que fue excelente.

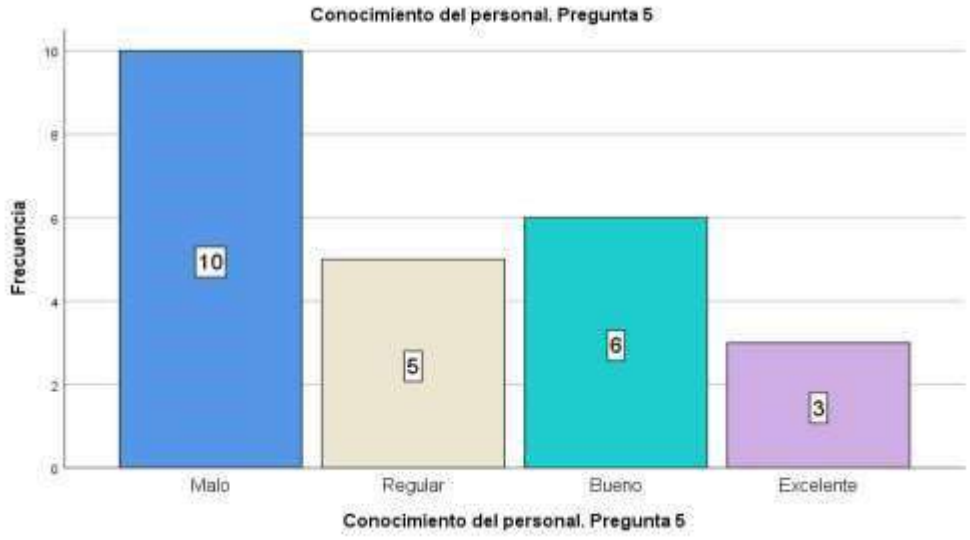
Conocimiento del personal. Pregunta 5. ¿Cómo califica el uso del software antivirus en el sistema de información por parte del personal de la Municipalidad Provincial de Huari, 2022?

Tabla 45
Conocimiento del personal. Pregunta 5

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	10	41,7	41,7	41,7
	Regular	5	20,8	20,8	62,5
	Bueno	6	25,0	25,0	87,5

Excelente	3	12,5	12,5	100,0
Total	24	100,0	100,0	

Figura 37
Conocimiento del personal. Pregunta 5



Con referencia a la pregunta sobre cómo califica el uso del software antivirus en el sistema de información por parte del personal de la Municipalidad se tuvo que 10 encuestados (41.7%) que fue malo, 5 de ellos (20.8%) fue regular, 6 encuestados (25.0%) valoraron como que fue bueno y, 3 de ellos (12.5%) manifestaron que fue excelente.

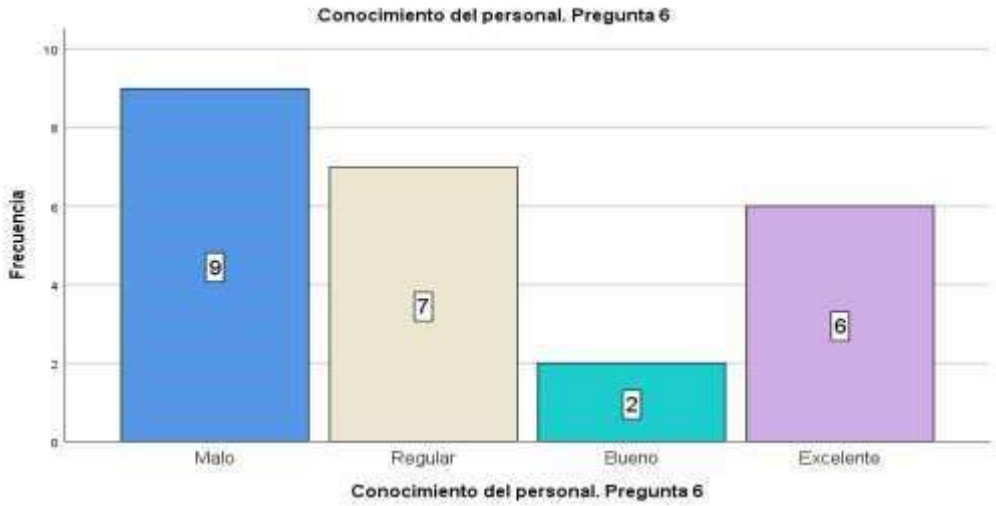
Conocimiento del personal. Pregunta 6. ¿Cómo considera el dominio de la seguridad de los archivos de importancia en la Municipalidad Provincial de Huari, 2022?

Tabla 46
Conocimiento del personal. Pregunta 6

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado

Válido	Malo	9	37,5	37,5	37,5
	Regular	7	29,2	29,2	66,7
	Bueno	2	8,3	8,3	75,0
	Excelente	6	25,0	25,0	100,0
	Total	24	100,0	100,0	

Figura 38
Conocimiento del personal. Pregunta 6



Con referencia a la pregunta sobre cómo considera el dominio de la seguridad de los archivos de importancia en la Municipalidad se tuvo que 9 encuestados (37.5%) que fue malo, 7 de ellos (29.2%) fue regular, 2 encuestados (8.3%) valoraron como que fue bueno y, 6 de ellos (25.0%) manifestaron que fue excelente.

Anexo 06

Plan de Seguridad de la Información para la Municipalidad Provincial de Huari, 2022

1. Introducción

El propósito de esta investigación es alcanzar un Plan de Seguridad de la Información para la Municipalidad Provincial de Huari para que contribuya en la

preservación de la confidencialidad, disponibilidad e integridad de los recursos informáticos de la municipalidad, el presente plan de seguridad se fundamenta la Norma Técnica Peruana ISO/IEC 27001:2014.

La municipalidad actualmente tiene el encargo social para ejercer el gobierno dentro de su jurisdicción para poder atender las diversas necesidades de la ciudadanía y de esta manera contribuir a su crecimiento y desarrollo económico, social y cultural, en esa tarea, la institución edil dispone de un sistema de información con la cual atiende los diversos procesos de atención al usuario. con la finalidad de que esta tecnología esté siempre disponible, y se ha usado de la mejor manera, debe tener el mantenimiento y cuidado respecto a su seguridad buen funcionamiento.

La institución edil, con el pasar de los años ha ido adquiriendo diversos tipos y modelos de sistemas informáticos de acuerdo a las necesidades de las diversas administraciones municipales que han antecedido a la actual administración, en el sistema de información actual se puede identificar que todavía existe una falta de política de seguridad respecto al capital informático mm activos de información, existen deficiencias en los lineamientos relacionados con la seguridad, ligeras deficiencias en el tratamiento de riesgos, los cuales son generados por falta de conocimiento de las vulnerabilidades y amenazas a los que se encuentra expuesta el sistema de información, así como también, se evidencia inadecuada gestión, de vigencia de uso de la tecnología, problemas en el conocimiento del uso de hardware y software, situaciones que pueden afectar la seguridad de la información debido a que no se cuenta con un plan o programa que pueda mitigar los diversos riesgos indicados.

En esta investigación se está considerando el uso de la metodología PDCA también conocida como círculo de Deming, por lo tanto, la investigación implica que se deba planificar, hacer chequear y actuar; así mismo, el estudio se fundamenta en la norma NTP-ISO/IEC 27001:2014.

2. Situación actual

La municipalidad provincial de huari, en la actualidad dispone de un sistema de información conformado por servidor, impresoras computadoras personales, laptops, sistemas de red, software, Empleados que utilizan el sistema de información, así como también un área que se encarga de su administración denominado área de informática.

2.1 Activos de información

La municipalidad provincial de huari cuenta con hardware, software, sistema de red y personal que utiliza todo este aparato tecnológico. en la siguiente tabla se encuentran cada una de en cuanto a cantidad y ubicación.

2.2 Las políticas de seguridad

Actualmente la municipalidad no dispone de políticas de seguridad de la información bien definidas y claras, Los documentos son generados por los usuarios y cada uno de ellos cumple las funciones que sí están normadas, el problema que se presenta es que nos están usando adecuadamente el sistema de información, Es por ello que en el presente estudio se trata de alcanzar los lineamientos necesarios para que los usuarios puedan garantizar la seguridad de la información antes, durante y después del uso del sistema de información.

2.2.1 Política de seguridad física y ambiental 2.2.2 Política de uso de Internet

Todos los empleados de la municipalidad provincial de huari deben utilizar el sistema de información estricta y específicamente para temas laborales, está terminantemente prohibido el uso del sistema de la información para cualquier otro tipo de trabajo que no sea o implique el cumplimiento de sus funciones laborales.

2.3 Control de seguridad de la información

2.3.1 Seguridad de los equipos fuera de las instalaciones

La utilización equipamiento destinado al procesamiento de información, fuera del ámbito de la Municipalidad Provincial de Huari debe ser autorizado por el área de informática previa coordinación con la alcaldía. En el caso de que en el mismo se

almacene información clasificada, deberá ser aprobado además por el propietario de la misma.

2.3.2. Análisis de riesgos

Los riesgos a los que puede estar sujeto un sistema de información de una institución edil son los siguientes:

- Accesos físico no autorizado
- Exponer información de alta importancia o confidencial
- Acceso al sistema por personal no autorizado
- Uso no autorizado de una información, registro o hardware o software en general
- Eliminación, apropiación de registros o archivos de la municipalidad
- Instalación no autorizada de software
- Acceso a sitios o páginas de internet indebidas
- Uso del sistema para trabajos que no sean propios de la municipalidad
- Comprometer información de importancia o confidencial
- Malograr deliberadamente algún elemento del sistema de información
- Acceso físico o lógico indebido
- Realizar cambios a los contenidos de los archivos o registros lógicos y digitales
- Tener claves de sus compañeros de trabajo

2.3.3. Vulnerabilidades

La vulnerabilidad que presentan mayores frecuencias en un sistema de información edil son los siguientes:

- Falta de conciencia y formación sobre la seguridad física y lógica del sistema de información
- Poner contraseñas sencillas o clásicas
- Dar contraseñas o claves a compañeros de trabajo
- No cambiar contraseñas cada cierto tiempo
- No instalara adecuadamente sistemas antivirus

- No actualizar periódicamente el sistema antivirus
- No disponer de una política de seguridad
- Falta de conciencia de seguridad
- Bajar archivos indebidos de Internet
- Obsolescencia de hardware y software
- Mal estado del sistema de cableado o conectividad
- Copia no controlada de la información y datos
- Deficiencias en la gestión del sistema de información
- Deficiencias en el control de datos de entrada y salida
- Protección física deficiente

Aplicación de controles

OBJETIVO	**CONTROLES**	**CUMPLIMIENTO**	
		SI	**NO**
Política de Seguridad	Se verifica las políticas de seguridad de información edil.		
	Existen perfiles que garantice la Seguridad de la información edil.		
	La gerencia edil está comprometida con la seguridad de la información.		
	Existe coordinación entre la gerencia edil y otras áreas en función de mejorar la seguridad de información.		
	Se asignan responsabilidades relacionados con la seguridad de la información.		
	Existen procesos de autorización de cambios de procesamiento de información edil.		
	Existen normas de confidencialidad.		
	Se hacen revisiones rutinarias que aseguren la seguridad de la información.		
	Se identifica la existencia de riesgos relacionados con entidades externas		
Gestión de	Existe registros de inventarios de activos.		

Activos	Se verifican registros de manera periódica, para asegurar el sistema de información		
	Se planifica el uso adecuado de hardware y software		
	Se clasifican los activos de acuerdo a categorías.		
	Existe técnicas para la atomización del registro de activos.		
Seguridad de los Recursos Humanos	Se asignan responsabilidades de los usuarios.		
	Existe un proceso de selección para asignar responsables de las copias de seguridad de información.		
	Se realizan verificaciones de términos y condiciones de uso del sistema de información		
	Existe una gestión de responsabilidades		
	Se planifica capacitación y educación en seguridad de la información		
	Existen procedimientos disciplinarios con respecto a la vulnerabilidad de la seguridad de la información.		
	Se registran las incidencias de vulnerabilidad y/o amenazas de la seguridad de la información.		
	El personal devuelve los activos que han terminado el contrato o personal en actividad		
	Se verifica la eliminación de derechos de acceso al usuario cesado.		
Seguridad Física y Ambiental	Existe seguridad física aceptable		
	Existen controles en las entradas de ambientes físico		

	Se verifica la seguridad de oficinas, ambientaciones y medios.		
	Existe protección contra riesgos y amenazas externas, respecto a los ambientes.		

	Se comprueba los trabajos en áreas seguras.		
	Se comprueba las áreas de acceso público a las instalaciones del sistema de información		
	Se ubican y protegen los elementos del sistema de información		
	Las computadoras se encuentra en un nivel de temperatura adecuado		
	Existe seguridad adecuada para el cableado.		
	Existe mantenimiento de equipo.		
	Existe verificación de seguridad del equipo fuera del local.		
	Se comprueba eliminación segura o rehusó del equipo.		
	Se comprueba el traslado de propiedades		
Gestión de la Comunicación y Operaciones	Realizan procedimientos de operación debidamente documentadas.		
	La gestión de cambio son verificados.		
	Existe responsabilidades y deberes		
	Se verifica la separación de los medios de desarrollo y operacionales.		
	Existe alguna entrega de servicios.		
	Se comprueba monitoreo y revisión de los servicios de terceros.		
	Existe alguna gestión de la capacidad.		
	Se comprueba la aceptación del sistema.		
	Existe algún control sobre Software maliciosos.		
	Se evidencia los controles contra códigos móviles		
	Existen evidencias de Backup o controles de la información.		
	Existe algún control de Red		
	Se comprueba la seguridad de los servicios de Red.		

	Se verifica la gestión de los medios removibles		
	Se comprueba la eliminación de medios		

	Existe algún Procedimientos de los manejos de información		
	Se comprueba la seguridad de documentación del sistema		
	Existen procedimientos y políticas de información y Software.		
	Se verifica el registro de acuerdos de intercambios.		
	Se comprueba medios físicos en tránsito.		
	Se verifican los mensajes electrónicos.		
	Existe algunos sistemas de información comercial		
	Existe verificación de registro de comercio electrónico.		
	Se comprueba Transacciones en línea		
	Se verifica la información disponible públicamente.		
	Existe algún Registro de auditoria		
	Se verifica la existencia del sistema de monitoreo.		
	Existe alguna protección del sistema de monitoreo.		
	Se vírica la protección de la información del registro.		
de	Se comprueba los registros del administrador y operador.		
	Existe algún Registro de fallas		
Control acceso	Existe verificación de sincronización de relojes.		
	Se comprueba las políticas del control de accesos.		
	Existe alguna inscripción del usuario.		
	Existe una verificación de gestión de privilegios.		

	Existe alguna gestión de clave de usuarios.		
	Revisión de los accesos de los derechos del usuario.		
	Existe algún uso de clave.		
	Equipamiento de usuario desatendido		
	Existe alguna política de pantalla y escritorio limpio.		
	Existe alguna política sobre el uso de servicios en Red.		
	Se comprueba Autenticación del usuario para conexiones externas.		
	Se comprueba la identificación del equipo en Red.		
	Existe alguna protección del puerto de diagnóstico remoto.		
	Segregación en redes		
	Existe algún control de conexiones en redes.		
	Se comprueba el control de routing en redes.		
	Existe algún procedimiento de registro en el terminal.		
	Se verifica la identificación y autenticación del usuario.		
	Se comprueba el sistema de gestión de claves.		
	Se verifica el uso de utilidades del sistema.		
	Existe alguna sesión inactiva.		
	Se comprueba la limitación de tiempo de conexión.		
	Existe alguna restricción al acceso a la información.		
	Existe algún aislamiento del sistema sensible.		
	Se verifica la existencia de computación móvil y comunicación		

	Existe algún Tele-trabajo.		

VALORACIÓN DE ACTIVOS

En cuanto a la valoración de los activos, se consideró la siguiente tabla:

VALOR	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
1	Se puede difundir, es de dominio publico	Se puede tolerar que no esté disponible al menos una semana	Los errores o modificaciones no autorizadas no generan impacto en la organización
2	Restringido para uso interno, si se filtra no ocasiona riesgo	Se puede tolerar que no esté disponible al menos un día	Los errores o modificaciones no autorizadas generan impacto leve en la organización
3	Protegido es necesario controles para su acceso, si se filtra ocasiona riesgo moderado a la organización	Se puede tolerar que no esté disponible al menos una hora	Los errores o modificaciones no autorizadas generan impacto moderado en la organización
4	Confidencial, información muy sensible, si se filtra se ocasiona un daño grave a la organización	No se tolera que el activo no se encuentre disponible	Los errores o modificaciones no autorizadas generan impacto critico en la organización

PROBABILIDAD DE OCURRENCIA

Se debe determinar la probabilidad de ocurrencia de la amenaza relacionados con la seguridad de hardware y software en función de lo indicado en la siguiente tabla:

PROBABILIDAD DE OCURRENCIA		
CATEGORIA	**VALOR**	**DESCRIPCIÓN**

Casi certeza	5	Riesgo cuya probabilidad de ocurrencia es muy alta, se posee un muy alto grado de seguridad que ocurra en el año
Probable	4	Riesgo cuya probabilidad de ocurrencia es alta, se posee un alto grado de seguridad que ocurra en el año
Moderado	3	Riesgo cuya probabilidad de ocurrencia es media, se posee un moderado grado de seguridad que ocurra en el año
improbable	2	Riesgo cuya probabilidad de ocurrencia es baja se posee un bajo grado de seguridad que ocurre en el año
Muy improbable	1	Riesgo cuya probabilidad de ocurrencia es muy baja se posee un muy bajo grado de seguridad que ocurra en el año

NIVEL DEL RIESGO

IMPACTO		PROBABILIDAD DE OCURRENCIA				Total
		Muy rara vez	Hasta dos veces al Año	Hasta una vez al mes	Más de una vez al mes	
	Menor	8	0	51	0	59
	Significativo	25	7	1	0	33
	Dañino	2	0	15	0	17
	Serio	0	0	0	4	4
		35	**7**	**67**	**4**	**113**

MAGERIT V3:

ANÁLISIS DE RIESGOS

En esta fase se tienen que analizar los riesgos en cada una de las unidades de la Municipalidad Provincial de Huari.

- ✓ Realizar inventario de hardware software y personal a cargo de la seguridad de la información y usuarios
- ✓ **A**nalizar los riesgos a los que está expuesto el hardware
- ✓ Analizar las vulnerabilidades
- ✓ Analizar los conocimientos de los usuarios en función a la seguridad de la información

- ✓ Analizar el riesgo existente cuando hacen uso de la nube y las redes sociales.
- ✓ Analizar la gestión de la seguridad actual respecto a cómo están identificando los riesgos, las vulnerabilidades, que conocimiento disponen sobre los ataques y los niveles de protección con los que cuentan.
- ✓ Analizar el nivel se seguridad de la información, específicamente a los archivos más importantes en función a los atributos e disponibilidad, integridad y confidencialidad.

TRATAMIENTO DE RIESGOS

En esta fase se tienen que analizar a cada una de las unidades o áreas de la institución edil en relación a las normas de seguridad de la información que están aplicando, los medios tecnológicos que disponen para enfrentar los riesgos; cómo están utilizando los medios de control de riesgos.

Analizar los conocimientos que los empleados usuarios del sistema información dispones respecto a la seguridad de la información, se va analizar los dominios sobre uso de hardware, software, seguridad e la información, etc.

SELECCIÓN DE SALVAGUARDAS

En esta fase se tiene que realizar los siguiente:

Analizar los mecanismos de control que están realizando los empleados de la municipalidad

Analizar los controles en la seguridad de hardware, software y conocimiento de los usuarios aspecto a la seguridad de la información.

Controlar la seguridad de los archivos informáticos de alta confidencialidad, específicamente en el cuidado de sus tres principales atributos: confidencialidad, integración y disponibilidad.

METODOLOGÍA

Se propone utilizar la metodología de la mejora continua o Ciclo PDCA o ciclo PHVA cuyas fases son las siguientes:

PLANIFICAR

En esta fase, la alcaldía, la gerencia municipal y el área de informática deben encabezar el proceso de planificación e implementación del plan de seguridad de la información, la fase de planificación consiste en realizar las siguientes actividades:

- Analizar las amenazas y vulnerabilidades del sistema de información

TIPOS DE AMENAZA	FRECUENCIA
Acceso físico no autorizado	
Comprometer información confidencial	
TIPOS DE AMENAZA	**FRECUENCIA**
Acceso a la red o al sistema de información por personas no autorizadas	
Revelación de información	
Uso no autorizado de material con copyright	
Infracción legal	
Destrucción de registros	
Uso no autorizado de software	
Comprometer información confidencial	
Instalación no autorizada de software	
Mal funcionamiento de los enlaces de comunicación	
Fallo de los enlaces de comunicación	
Perdida de electricidad	
Errores en mantenimiento	
Comprometer información confidencial	
Acceso físico no autorizado	
Perdida de servicios de apoyo	
Cambios no autorizados de registros	

VULNERABILIDADES	FRECUENCIA

Contraseñas predeterminadas no modificadas	
Falta de formación y conciencia sobre seguridad	
Ausencia de sistemas de identificación y autenticación	
Falta de documentación interna	
Clasificación inadecuada de la información	
Gestión inadecuada del cambio	
Falta de política de acceso o política de acceso remoto	
No validación de los datos procesados	
Protección física no apropiada	
Falta de políticas para el uso de la criptografía	
Descarga no controlada de internet	
Inadecuada gestión de red	
Falta de control sobre los datos de entrada y salida	
Sensibilidad del equipo a la humedad, temperatura o contaminantes	
Inadecuada seguridad del cableado	
Copia no controlada de datos	
Sensibilidad del equipo a los cambios de voltaje	
Falta de política de acceso o política de acceso remoto	

- Definir metas, objetivos y las políticas que van a contribuir lograr los objetivos que se planifiquen. Los objetivos y las políticas deben estar enfocados en la seguridad de hardware, software y en los conci9mientos del personal en uso y protección del sistema de información frente a los ataques internos y externos.
- Identificación de actividades o tareas a realizar con relación a l seguridad del sistema de información. En cada área se deben identificar al personal que hace uso del sistema, sus niveles de conocimiento, los softwares que utiliza, y el hardware asignado.

HACER

En esta segunda etapa consiste en:

- ❖ Poner en funcionamiento el plan de gestión de seguridad de la información de todas las áreas de la municipalidad
- ❖ Poner en práctica los controles y las políticas relacionados con el análisis de riesgos.

OBJETIVO	CONTROLES	CUMPLIMIENTO	
		SI	NO
Política de Seguridad	Se verifica las políticas de seguridad de información edil.		
	Existen perfiles que garantice la Seguridad de la información edil.		
	La gerencia edil está comprometida con la seguridad de la información.		
	Existe coordinación entre la gerencia edil y otras áreas en función de mejorar la seguridad de información.		
	Se asignan responsabilidades relacionados con la seguridad de la información.		
	Existen procesos de autorización de cambios de procesamiento de información edil.		
	Existen normas de confidencialidad.		
	Se hacen revisiones rutinarias que aseguren la seguridad de la información.		
	Se identifica la existencia de riesgos relacionados con entidades externas		
Gestión de Activos	Existe registros de inventarios de activos de hardware y software.		

OBJETIVO	CONTROLES	CUMPLIMIENTO	
		SI	NO
	Se verifican registros de información de manera frecuente para asegurar el sistema de información		
	Se planifica el uso adecuado de hardware y software		
	Se clasifican los activos de acuerdo a categorías.		

	Existe técnicas para la atomización del registro de activos.		
Conocimiento del personal	Se asignan responsabilidades de los usuarios.		
	Existe un proceso de selección para asignar responsables de las copias de seguridad de información.		
	Se realizan verificaciones de términos y condiciones de uso del sistema de información		
	Dominio de uso de hardware relacionado con la seguridad		
	Dominio de uso de software relacionado con la seguridad		
	Existe una gestión de responsabilidades		
	Se planifica capacitación y educación en seguridad de la información		
	Existen procedimientos disciplinarios con respecto a la vulnerabilidad de la seguridad de la información.		
	Se registran las incidencias de vulnerabilidad y/o amenazas de la seguridad de la información.		
	El personal devuelve los activos que han terminado el contrato o personal en actividad		
	Se verifica la eliminación de derechos de acceso al usuario cesado.		
Seguridad Física y Ambiental	Existe seguridad física aceptable		
	Existen controles en las entradas de ambientes físico		
	Se verifica la seguridad de oficinas, ambientaciones y medios.		
	Existe protección contra riesgos y amenazas externas, respecto a los ambientes.		

OBJETIVO	**CONTROLES**	**CUMPLIMIENTO**	
		SI	**NO**

	Se comprueba los trabajos en áreas seguras.		
	Se comprueba las áreas de acceso público a las instalaciones del sistema de información		
	Se ubican y protegen los elementos del sistema de información		
	Las computadoras se encuentra en un nivel de temperatura adecuado		
	Existe seguridad adecuada para el cableado.		
	Existe mantenimiento de equipo.		
	Existe verificación de seguridad del equipo fuera del local.		
	Se comprueba eliminación segura o rehusó del equipo.		
	Se comprueba el traslado de propiedades		
Gestión de la Comunicación y Operaciones	Realizan procedimientos de operación debidamente documentadas.		
	La gestión de cambio son verificados.		
	Existe responsabilidades y deberes		
	Se verifica la separación de los medios de desarrollo y operacionales.		
	Existe alguna entrega de servicios.		
	Se comprueba monitoreo y revisión de los servicios de terceros.		
	Existe alguna gestión de la capacidad.		
	Se comprueba la aceptación del sistema.		
	Existe algún control sobre Software maliciosos.		
	Se evidencia los controles contra códigos móviles		
	Existen evidencias de Backup o controles de la información.		
	Existe algún control de Red		
	Se comprueba la seguridad de los servicios de Red.		

	Se verifica la gestión de los medios removibles		
	Se comprueba la eliminación de medios		
	Existe algún Procedimientos de los manejos de información		

OBJETIVO	CONTROLES	CUMPLIMIENTO	
		SI	NO
	Se comprueba la seguridad de documentación del sistema		
	Existen procedimientos y políticas de información y Software.		
	Se verifica el registro de acuerdos de intercambios.		
	Se comprueba medios físicos en tránsito.		
	Se verifican los mensajes electrónicos.		
	Existe algunos sistemas de información comercial		
	Existe verificación de registro de comercio electrónico.		
	Se comprueba Transacciones en línea		
	Se verifica la información disponible públicamente.		
	Existe algún Registro de auditoria		
	Se verifica la existencia del sistema de monitoreo.		
	Existe alguna protección del sistema de monitoreo.		
	Se vírica la protección de la información del registro.		
Control de acceso	Se comprueba los registros del administrador y operador.		
	Existe algún Registro de fallas		
	Existe verificación de sincronización de relojes.		
	Se comprueba las políticas del control de accesos.		
	Existe alguna inscripción del usuario.		

	Existe una verificación de gestión de privilegios.		
	Existe alguna gestión de clave de usuarios.		
	Revisión de los accesos de los derechos del usuario.		
	Existe algún uso de clave.		
	Equipamiento de usuario desatendido		
	Existe alguna política de pantalla y escritorio limpio.		
	Existe alguna política sobre el uso de servicios en Red.		
OBJETIVO	**CONTROLES**	**CUMPLIMIENTO**	
		SI	**NO**
	Se comprueba Autenticación del usuario para conexiones externas.		
	Se comprueba la identificación del equipo en Red.		
	Existe alguna protección del puerto de diagnóstico remoto.		
	Segregación en redes		
	Existe algún control de conexiones en redes.		
	Se comprueba el control de routing en redes.		
	Existe algún procedimiento de registro en el terminal.		
	Se verifica la identificación y autenticación del usuario.		
	Se comprueba el sistema de gestión de claves.		
	Se verifica el uso de utilidades del sistema.		
	Existe alguna sesión inactiva.		
	Se comprueba la limitación de tiempo de conexión.		
	Existe alguna restricción al acceso a la información.		

	Existe algún aislamiento del sistema sensible.		
	Se verifica la existencia de computación móvil y comunicación		
	Existe algún Tele trabajo.		

- Disponer y aplicar los procesos y actividades que van a permitir la identificación de las actividades que se debe realizar con la finalidad de asegurar un control adecuado y garantizar la seguridad de la información y todo el sistema.

VERIFICAR

En la tercera fase de la metodología PHVA se deben desarrollar las siguientes actividades:

Desarrollar el monitoreo y fiscalización sobre cómo se está llevando a cabo el plan de seguridad de la información, consiste en controlar los procesos para que se apliquen en la forma indicada y que se estén cumpliendo las metas y objetivos establecidos dentro de un marco de eficacia y eficiencia. El control deber de realizarse mensualmente a cada una de las áreas. Se deben asignar puntuaciones a cada usuario en función del uso del hardware y software para después ellos sean premiados en función a os establezca la gerencia de la municipalidad.

VERIFICACIÓN	**CUMPLE**	
	SI	**NO**
Políticas de seguridad de la información		
Orientación de la dirección para la gestión de la seguridad de la información		
Políticas para la seguridad de la información		
Revisión de las políticas para la seguridad de la información		
Organización de la seguridad de la información		
Roles y responsabilidades para la seguridad de la información		
Separación de deberes		

Contacto con las autoridades		
Seguridad de la información en la gestión de proyectos		
Dispositivos móviles y trabajo virtual		
Política para dispositivos móviles		
Seguridad de los recursos humanos		
Responsabilidades de la dirección		
Toma de conciencia, educación y formación en la seguridad de la información		
Gestión de activos		
Responsabilidad por los activos		
Inventario de activos		
Propiedad de los activos		
Uso aceptable de los activos		
Devolución de activos		
Clasificación de la información		
Manejo de medios		
Gestión de medios removibles		
Disposición de los medios		
Transferencia de medios físicos		
Control de acceso		
Requisitos del negocio para control de acceso		
Política de control de acceso		
Acceso a redes y a servicios en red		
Gestión de acceso de usuarios		

VERIFICACIÓN	**CUMPLE**	
	SI	**NO**
Registro y cancelación del registro de usuarios		
Suministros de acceso de usuarios		
Gestión de derechos de acceso privilegiado		
Gestión de información de autenticación secreta de usuarios		
Revisión de los derechos de acceso de los usuarios		
Retiro o ajuste de los derechos de acceso		
Responsabilidades de los usuarios		
Uso de información de autenticación secreta		
Control de acceso a sistemas y aplicaciones		

Restricción de acceso a la información		
Procedimiento de ingreso seguro		
Sistema de gestión de contraseñas		
Uso de programas utilitarios privilegiados		
Control de acceso a códigos fuente de programas		
Política sobre el uso del sistema de información		
Seguridad física del entorno		
Áreas seguras		
Perímetro de seguridad física		
Controles de acceso físico		
Seguridad de oficinas, recintos e instalaciones		
Protección contra amenazas externas y ambientales		
Trabajo en áreas seguras		
Ubicación y protección de hardware		
Servicios de suministro		
Seguridad del cableado		
Mantenimiento de hardware		
Retiro de activos		
Seguridad de hardware y activos fuera de las instalaciones		
Disposición segura o reutilización de hardware		
Política de escritorio limpio y pantalla limpia		
Seguridad de las operaciones		
Procedimientos operacionales y responsabilidades		
Procedimientos de operación documentados		
Separación de los ambientes de desarrollo, pruebas y operación		
Protección contra códigos maliciosos		
Controles contra códigos maliciosos		
Copias de respaldo		
Respaldo de la información		
Registro y seguimiento		
Registro de eventos		
Protección de la información de registro		
Registro del administrador y del usuario edil		
Sincronización de relojes		
Control de software operacional		
Instalación de software en sistemas operativos		

Gestión de la vulnerabilidad técnica		

VERIFICACIÓN	CUMPLE	
	SI	NO
Gestión de las vulnerabilidades técnicas		
Restricciones sobre la instalación de software		
Consideraciones sobre auditorias de sistemas de información		
Controles de auditoria de sistemas de información		
Seguridad de las comunicaciones		
Gestión de la seguridad de las redes		
Controles de redes		
Seguridad de los servicios de red		
Separación en las redes		
Trasferencia de información		
Políticas y procedimientos de transferencia de información		
Acuerdos sobre transferencia de información		
Mensajería electrónica		
Acuerdos de confidencialidad o de no divulgación		
Adquisición, desarrollo y mantenimiento de sistemas		
Requisitos de seguridad de los sistemas de información		
Análisis y especificación de requisitos de seguridad de información		
Seguridad de servicios de las aplicaciones en redes públicas		
Protección de transacciones de los servicios de las aplicaciones		
Seguridad en los procesos de desarrollo y soporte		
Política de desarrollo seguro		
Procedimientos de control de cambios en sistemas		
Revisiones técnicas de las aplicaciones después de cambios en la plataforma de operación		
Restricciones en los cambios a los paquetes de software		
Principios de construcción de los sistemas seguros		
Ambiente de desarrollo seguro		
Pruebas de seguridad de sistemas		
Protección de datos de prueba		
Seguridad de la información en las relaciones con los proveedores		

Política de seguridad de la información para las relaciones con los proveedores		
Tratamiento de seguridad dentro de los acuerdos con proveedores		
Cadena de suministro de tecnología de información y comunicación		
Gestión de la presentación de servicios de proveedores		
Seguimiento y revisión de los servicios de los proveedores		
Gestión de incidentes de seguridad de la información		
Gestión de incidentes y mejoras en la seguridad de la información		
Gestión de incidentes y mejoras en la seguridad de la información		
Responsabilidades y procedimientos		
Reporte de eventos de seguridad de la información		
VERIFICACIÓN	**CUMPLE**	
	SI	**NO**
Reporte de debilidades de seguridad de la información		
Evaluación de eventos de seguridad de la información y decisiones sobre ellos		
Respuesta a incidentes de seguridad de la información		
Aprendizaje obtenido de los incidentes de seguridad de la información		
Recolección de evidencia		
Aspectos de seguridad de la información de la gestión de continuidad del negocio		
Continuidad de seguridad de la información		
Planificación de la continuidad de la seguridad de la información		
Verificación, revisión y evaluación de la continuidad de la seguridad de la información		
Disponibilidad de instalaciones de procesamiento de información		
Cumplimiento de requisitos legales y contractuales		
Protección de registros		
Privacidad y protección de información de datos personales		
Revisiones de seguridad de información		
Revisión independiente de seguridad de la información		
Cumplimiento con las políticas y normas de seguridad		

Revisión del cumplimiento técnico		
Conocimientos del personal sobre seguridad de software		
Conocimientos del personal sobre seguridad de hardware		

ACTUAR

En la última etapa de la metodología PHVA se tienen que mantener y mejorar la gestión de la seguridad de la información mediante la definición y ejecución de acciones correctivas que se han encontrado y diseñado con el propósito de rectificar las vulnerabilidades o fallos encontrados en las etapas anteriores en todas las áreas de la municipalidad. El jefe de informática debe actuar sobre la seguridad de hardware y software sin descuidar las capacitaciones de los usuarios del sistema de información. Deben actuar sobre el riesgo físico del sistema de información.

La actuación termina con la información de riesgos

Riesgo Físico – Pérdida de servicio, equipos o instalación (disponibilidad del servicio de TI)			
Id: Riesgo: 1	Fecha:	Probabilidad	Impacto:
Descripción: Cambios en el software y hardware			
Refinamiento **Condición 1:** Falta de licencia, no existe plan de mantenimiento y vigilancia tecnológica **Condición 2:** no realizan controles de consumo de recursos hardware de los sistemas, escasa realización de mantenimiento de computadoras **Condición 3:** No disponen de plan de mantenimiento de equipos, plan de contingencia			
Acciones a seguir contra el riesgo **Acción 1**: Elaboración de un plan de mantenimiento y actualización de software **Acción 2**: Elaboración de un plan de contingencia			

Acción 3: Monitoreo preventivo de consumo de recursos Hardware y software **Acción 4**: Equipos de contingencia **Acción 5**: Plan de mantenimiento de hardware
Asignado: Área de informática

Riesgo Lógico – identificación de protocolos en el tráfico de la red que sobrecargan el servicio			
Id: Riesgo: 2	Fecha:	Probabilidad	Impacto:
Descripción: Gestión del tráfico en la red			
Refinamiento **Condición 1:** inexistencia de plan de configuración **Condición 2:** inadecuada administración de seguridad, contraseñas no seguras, inexistencia de los eventos de seguridad			
Acciones a seguir contra el riesgo **Acción 1**: Elaboración del manual de configuración de servidores. **Acción 2**: Crear un control de prevención y de detección del uso de software de origen dudoso **Acción 4**: Establecimiento de métodos de cifrado y backup. **Acción 5**: Gestión de permisos			
Asignado: Área de informática			

Riesgo Lógico – incumplimientos de políticas, normas y/o procedimientos sobre seguridad de la información			
Id: Riesgo: 3	Fecha:	Probabilidad	Impacto:
Descripción: compromiso con el cumplimiento de políticas, normas y/o procedimientos sobre seguridad de la información			

Refinamiento **Condición 1:** no hay difusión de las políticas de información **Condición 2:** usuarios no están informados
Acciones a seguir contra el riesgo **Acción 1**: Realizar un plan de difusión **Acción 2**: evaluar el nivel de compromiso entorno a políticas, normas y/o procedimientos sobre seguridad de la información **Acción 3**: Asignar responsabilidades de activos de información **Acción 4**: procedimientos disciplinarios establecidos en los contratos de cada usuario
Asignado: Área de informática

Riesgo Lógico – Cambios no controlados en los sistemas (software y hardware) y servicios.			
Id: Riesgo: 4	Fecha:	Probabilidad	Impacto:
Descripción: Gestión del control de cambios de software y hardware			
Refinamiento **Condición 1: F**alta de licencia, inexistencia de monitorización de software/versiones **Condición 2:** Falta de licencia, inexistencia de plan de mantenimiento y vigilancia tecnológica			
Acciones a seguir contra el riesgo **Acción 1**: Adquisición de licencia de programas y/o evaluación del uso de software libre **Acción 2**: Gestión de vulnerabilidades **Acción 3**: Elaboración de un plan de mantenimiento y actualización de software. **Acción 4**: Elaboración de un plan de contingencia			
Asignado: Área de informática			

Riesgo Lógico– Violaciones de acceso a los sistemas.			
Id: Riesgo: 5	Fecha:	Probabilidad	Impacto:
Descripción: Los sistemas deben poseer programa de auditorías, control de versiones de acuerdo a los roles y permisos			
Refinamiento **Condición 1:** Falta de políticas de acceso y auditorías internas. (cuentas de usuarios sin auditor) **Condición 2:** Inexistencia de normas de seguridad, mala configuración de roles y permisos			
Acciones a seguir contra el riesgo **Acción 1**: Elaboración de políticas de acceso. Diseñar esquemas de seguridad basado en roles y permisos **Acción 2**: Diseñar un esquema de privilegios sobre el file Server **Acción 3**: control de versiones de software. **Acción 4**: Procedimiento formal de control de cambios **Acción 5**: Verificación de roles y permisos			
Asignado: Área de informática			

Plan de seguridad de la información en la seguridad de los activos informáticos de la Municipalidad Provincial de Huari, 2022

por Eda Maritza Chiquian Crispín

Fecha de entrega: 17-ago-2023 01:44p.m. (UTC-0500)
Identificador de la entrega: 2147179952
Nombre del archivo: Tesis_Maritza_Crispin_08-2023.pdf (1.58M)
Total de palabras: 11426
Total de caracteres: 62541

[redacted]

[redacted]

[redacted]

Plan [redacted] seguridad de los activos informáticos de [redacted] Huari, 2022

[redacted]

en Informática y [redacted]

Autora

Chiquian Crispín Eda Maritza

Asesor

Wilmer Carrasco Alvarado

[redacted]

[redacted]

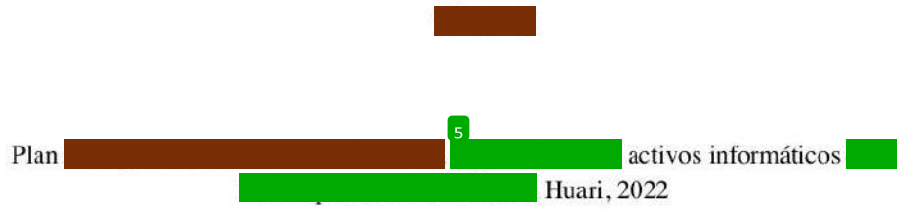
[redacted]	Seguridad Informática
[redacted]	Sistemas [redacted] información

KEYWORDS:

[redacted]	Computing Security
Specialty	[redacted]

[redacted]

[redacted]	Sistema [redacted] Gestión
[redacted]	Ciencias Sociales
[redacted]	Economía [redacted]
[redacted]	[redacted]


Plan
5
activos informáticos
Huari, 2022

estudio establecer la relación plan con seguridad Municipalidad Provincial Huari, 2022; la hipótesis consistió en que el plan de propuesto positivamente seguridad los activos informáticos. investigación fue de tipo no experimental propositiva, de diseño 24 usuarios sistema información edil. Se aplicó encuesta y cuestionario. La relación entre la variable Plan de seguridad y la seguridad de los activos informáticos fue 0.788, lo cual significa que existió correlación positiva alta entre ambas variables, el p valor fue de 0.000, lo cual confirmó que los datos no correspondieron a una curva normal. Que existió relación positiva alta de 0.745 entre la variable Plan de seguridad y la dimensión Seguridad de Software. Que existió relación positiva alta de 0.763 entre la variable Plan de seguridad y la dimensión Seguridad de Hardware. Que existió relación positiva alta de 0.794, entre la variable Plan de seguridad y la dimensión Conocimientos del personal, en todos los casos el p valor fue de 0.000, por lo tanto, los datos no correspondieron a una curva normal.

proposal of an security plan security computer assets Provincial Municipality Huari, 2022; The hypothesis was proposed plan positively security of IT assets. The research was propositional, 24 users building information system. A survey and questionnaire were applied. variable Plan security of computer assets was 0.788, which both , the p value 0.000, which confirmed that the data did not correspond to a normal curve. was relationship .745 Security Plan variable Software Security dimension. was relationship .763 Security Plan variable Hardware Security dimension. was relationship .794, variable Security Plan dimension Knowledge of personnel, in all cases the p value was 0.000, therefore, the data did not correspond to a normal curve.

INTRODUCCIÓN

conocer ha hecho analisis de los antecedentes locales, nacionales e internacionales para que puedan ser discutidos posteriormente con los resulatdos de la presnte investigación.

Huacón (2022) en la tesis de grado denominada “ “desarrollada en realizar un análisis a la plataforma de . Trabajó con investigación no experimental de diseño descriptivo, de enfoque cualitativo. Concluyó que las empresas conforme fueron creciendo en volumen de datos e información se volvió más frágil y con tendencia a presentar mayores vulnerabilidaes, riesgos y ser atacados desde adentro y afuera de la empresa, los ataques mas usados fueron extorción, robo de información, etc., se evidenció que en , tuvo mayores deficiencias constituyó su prioridad despues de los ataques recibidos. Que las tecnologías de pretesting se seleccionaron obtención de información, para ello, se cumpleiron los parámetros sugeridos para su administración. Que los reportes generados por Kali Linux, mostraron conductas bastante vulnerables que estaban poniendo en alto riesgos a la institucion, con los datos reportados por el sistema operativo se pudo realziar un analisis profundo y riguroso sobre el desarrollo de las posibles soluciones a los problemas de seguridad informática.

Ramírez (2020) en la tesis de grado denominada “ ”, desarrollada en , la libertad, en Ecuador. Se plantearon como objetivo realziar la deteccion de las vulnerabilidades de servidores y red en

de la institucion edil, con aplicación de software libre de código abierto, [redacted] sistema de [redacted] edil. Trabajó estudio no experimental, descriptivo, de enfoque cualitativo. Concluyeron que las empresas conforme crecen, también crecen los datos e información, y a lavez se vuelven más vulnerables y los riesgos se incrementan, los atacantes ven estas vulnerabilidades y atacan con la finalidad de apoderarse de los activos informáticos, también se encontró que la seguridad informática era muy baja, no se le daba mucha importancia por la empresa. Se encontró que las herramientas de prueba informático fueron escogidas teniendo en cuenta los requerimientos de obtención de información. Que los reportes generados por Kali Linux, mostraron conductas bastante vulnerables que estaban poniendo en alto riesgos a la institucion, con los datos reportados por el sistema operativo se pudo realziar un analisis profundo y riguroso sobre el desarrollo de las posibles soluciones a los problemas de seguridad informática.

Poicon y Ramírez (2020) en la tesis de grado denominada "[redacted]" realizada [redacted]. Piura. [redacted] general [redacted] elaborar una propuesta [redacted] un Sistema de [redacted] de Seguridad informática en el objeto de estudio. Aplicó como método a Magerit 3.0 y análisis de riesgos, trabajó un estudio [redacted], de diseño [redacted]. Concluyeron que [redacted] encontraron tres tipos de activos de información, software y hardware; de la clase de equipo de proceso de datos tuvo 50.44% de los activos, de los cuales el 85.84% fue hardware, el nivel de amenaza fue alto con 57.50%, ataques con mayor probabilidad de ocurrencia debido a deficiencias de operatividad de equipos. Que los valores de criticidad de datos e información estuvieron en nivel bajo y medio; respecto a los riesgos se encontró nivel de 30%, sobre riesgo dañino se tuvo 15%, respecto al riesgo de nivel serio se encontró 4%, en este nivel de porcentaje se recomendó realziar control con fines de evitar la concreción de las amenazas. Que se operó 114 controles, 63 de estos no se cumplieron alguna evidencia, la cual no

se encontró sistematizada debido a las directivas que no fueron aprobadas, la institucion edil alguno sobre . Que alcanzaron normas realizar monitoreos control edil.

Zapata (2020) tesis grado denominada "", realizada la universidad Técnica Ambato ciudad Ambato, Ecuador. Se plantearon como objetivo realizar la concordancia con . Trabajó con investigación tipo no experimental, descriptivo respecto al diseño, de enfoque cualitativo. Concluyeron que no se contó con políticas y procesos que ayuden el la salvaguarda de la seguridad informática, las actividades desarrolladas no se basaron en las normas o políticas previamente acordadas, por el contrario, emplearon normas que no contribuyeron en dar la garantía parcial o total de la disponibilidad, confodencialidad e integridad de los activos informáticos. Qué existieorn falencias , en cpomputadoras, servidores y software, ello permitió que los archivos de información muy importante de la institución estuvieron vulnerables y propuestos ariesgos y amenazas.

Vargas (2019) en la tesis de maestría se trazó como objetivo realizar Plan con finalidad dar cumplimiento la estrategia gobierno. investigación no experimental, descriptivo resepcto al diseño, de enfoque cuantitativo. Concluyeron que existió un nivel de la efectividad aceptable cuando se implementaron los controles en concordancia con la norma ISO 27001:2013 debido a que como resulatdos se tuvo una calificación de 30, debido a ello, los procesos y los controles siguieron un patrón regular, las actividades fueron desarrolladas de tal manera que diferentes procesos fueron realziados por diferentes personas, no hubo capacitación ni comunicación formal relacionados con los procesos y estándares, se evidenció un nivel considerable de confianza relacioandos con los dominios de conocimientos , existió probabilidad fallas. No existió

, tampoco nivel logrado fue cero debido a la evaluación de la efectividad del control, ello condujo a que se tenga que desarrollarla, aprobarla y firmarla, tambien se tuvo que revisar y actualizar con cierta frecuencia.

A nivel nacional, Camapaza (2019) en la tesis de grado denominada "
" realizada en Universidad Andina Cusco. Perú; se planteó como en plan cimentada norma indicada propósito de seguridad informática objeto de estudio. Como metodología aplicó Margerit V.3, tratamiento de riesgos, la norma NTP-ISO/IEC 27001:2014, la investigación fue de tipo en donde se manipuló la variable independiente, de diseño pre experimental, de enfoque positivista. Encontró que el 100% indicaron que se divulgó información bastante importante y sensible, para el 75% nunca se realizó evaluación de riesgos, el 50% no realiza copia de seguridad, el 75% señala que su oficina no está protegida contra ataques informáticos. Concluyó que MARGERIT v.3 como metodología contribuyó en el dimensionamiento de la posibilidad de que ocurra cierto nivel de riesgo, ayudó en la confección de la lista de controles de seguridad con el proposito de reducir los riesgos de niveles altos y medios.

Monteza (2019) en la tesis de grado titulada "
en
. Realizada la UPC. Lima, Perú; se trazó como objetivo general desarrollar
la con fines protección con referencia a actividades de tributación. Aplicó metodología COBIT, OISM3, Magerit, método MEHARI y OCTAVE ALLEGRO. Como resultado encontró que el 92% de las instituciones que usan sistemas de información se preocupan por la seguridad de sus sistemas de datos; el 34% de los empleados son descuidados o inconscientes, el 26% indicaron que los controles de seguridad estuvieron

obsoletos, para el 13% pueden ingresar al sistema sin autorización. Concluyó que se encontraron 72% de [redacted], que existieron 44% de activos de información con alto riesgo alto y medio con un 44%. Que [redacted] propuesto puede minimiziar cuantitativamente los riesgos que afectan al sistema de información con grado de aceptabilidad de la organización.

Vásquez y Rengifo (2019) en la tesis denominada "[redacted]" realizada en la [redacted], se trazaron el objetivo de proponer [redacted] en [redacted] espacio [redacted] estudio. Como metodología aplicaron [redacted] NTP [redacted], políticas [redacted] seguridad [redacted] evaluación integral. Concluyeron que se plantearon políticas de seguridad aplicando análisis de riesgo mediante al determinación de elementos computacionales más importantes para ques ean protegidos en funcion o de acuerdo a los riesgos y vulnerabilidades que presenten con la finalidad de garantizar sus resepctivas protecciones y adminsitración de la información, cuidando siempre las dimensiones [redacted] edil. Que [redacted] desarrolló [redacted] emergencia [redacted] procedimientos para ser puestos en prácticas en caso de que suceda un ataque a la seguridad de la infraestructura del objeto de estudio. Que la investigación fue satisfactorio porque contribuyó en el conocimeinto de las deficiencias ediles, en base a la cual se logró alcanzar propuestas de mejora con el propósito de contrarrestar dicha problemática.

Armas y Pérez (2018) en la tesis de grado denominada "[redacted] Municipalidad Distrital [redacted] Independencia 2016" realizada en la UNASAM, Huaraz Perú; se trazó como objetivo general aplicar el desarrollo de un [redacted] propósito [redacted] reducir [redacted] riesgos en los [redacted] Sub Gerencia [redacted] Informática y Telecomunicaciones en el objeto de estudio. Aplicó metodología de análisis y observación de los datos. Concluyeron que la metodología MAGERIT

permitió identificar los puntos importantes en las actividades de analziar y gestionar los riesgos, logró resultados del estado de riesgo del espacio de estudio, que se tuvo un documento de seguridad que permitirá desarrolar leyes y normas [redacted] y para [redacted] personal del espacio [redacted] estudio.

Pacheco (2018) en la tesis de maestría denominada "[redacted]" desarrollada en la [redacted] en [redacted] se plantearon como objetivo general hacer el diseño y aplicación de las [redacted] mediante la aplicación [redacted] e [redacted] manejar los riesgos y cumplir con el aseguramiento de los requisitos del sistema de información. Trabajó con investigación de tipo no experimental de diseño descriptivo, de enfoque cuantitativo Concluyeron que se encontró que la implementación [redacted] cimentada [redacted], así como en [redacted] procesos [redacted] los cuales fueron creados por el personal técnico [redacted] las [redacted] y tambien participaron autoridades institucionales, fue una alternativa de solución en la protección y adminsitración eficiente de las actividades de control de gestión, así como también, se trató de dar protección proteger, prevención y minimziación de los incidentes generados por amenazas a los activos de información.

[redacted] de cualquier organización, ya que contiene datos importantes y sensibles sobre sus estrategias comerciales, procesos, clientes, proveedores y muchos otros datos que deben protegerse y mantenerse confidenciales, independientemente de su tamaño, integridad y disponibilidad. siempre debe estar garantizado. En ese sentido, se fundamenta científicamente en bases teóricas.

Seguridad Informática. Se entiende a la seguridad informática como las medidas y controles que las autoridades de [redacted] establecen [redacted]

[redacted] dar seguridad a [redacted] sistemas [redacted] evitando que cualquier atacante interno o externo ejecuten ataques o procesos no autorizados en el hardware y software del sistema; de acuerdo con Corletti (2016), el establecimiento de una adecuada protección [redacted] elementos [redacted] evitar cualquier configuración de problemas de seguridad, el software aplicativo tiene que ser descargado de fuentes bastante confiables y además tienen que ser actualizadas con significativa frecuencia. Para [redacted] la [redacted] con frecuencia se hace necesario desarrollar copias de seguridad, revisar el cifrado de datos, almacenamiento redundante de datos, así como también, deshabilitar o desconectar ciertos elementos de entrada y de salida de información que no ha sido debidamente autorizada. Con el propósito de evitar robos, se tiene que descifrar la información altamente confidencial y crítica, evitar conexiones de equipos internos y externos no autorizados, así como también llevar un control de los mantenimientos preventivos de los elementos de [redacted]

[redacted]. también [redacted] entendida cómo es [redacted] protección con el [redacted] se cuenta en un determinado tiempo en la red, para tener la capacidad de dar proteción a la información, archivos, software, hardware en general, frente a cualquier tipo de atacante informático que traten de llevar a cabo procesos de espionaje, modificación de archivos, intercepción y eliminación de infromación, asimismo, como disponer de normas, políticas, métodos, procesos de recuperación de información en casos de ataques al sistema de infromación (CISCO, 2016).

Política de seguridad. Debido a que la seguridad informática, siempre ha sido un problema para cualquier institución pública o privada, internacionalmente se han establecido políticas de seguridad con la finalidad de documentar normas y procesos de cómo las instituciones deben de actuar en casos de ataques informáticos. (Stallings, 2004). La política de seguridad, por lo tanto, es un documento elaborado con la participación principales integrantes de la

organización, en este documento se indican los términos generales, objetivos, metas, así como también, las líneas principales de acción qué los usuarios del sistema deban realizar para dar protección a los activos informáticos. En términos de seguridad, la política relacionada a esta misma variable, en primer lugar, debe contener todos los lineamientos implican dar seguridad a todo el sistema de información, específicamente al software, hardware y sin descuidar el nivel de conocimientos que debe tener el personal te gusta el sistema de información con los dominios tipos de ataques, conocimiento de software antivirus, , conocimiento hardware involucrado en informática, etc. (Garre, Tortajada. y Cruz, 2018; Miguel, 2015).

La política de seguridad se conceptúa como un conjunto de directivas, procedimientos, guías y estándares que Norman ciertas actividades y procesos en el uso del sistema de información, así como también se establecen responsabilidades, métodos y técnicas, buenas prácticas y consideraciones que debe tener quienes usen el sistema aborda los temas uso software y hardware, y recomienda que el personal debe estar altamente capacitado, sobre todo en el caso de los ataques informáticos cuando el sistema hace uso de la red de redes (cumple un rol al interior de la institución, esto significa que, las políticas van dirigidas a su comprensión y aplicación por parte de los elementos o Recursos Humanos que utilizan el sistema de información dentro de la institución, la política hace referencia a cómo ellos deben utilizar los sistemas en función de la seguridad en el cumplimiento de sus funciones operativas o administrativas (Stair & Reynold, 2017; Santana, 2012).

La política de seguridad también cumple un rol externo, esto sucede cuando la institución demuestra al entorno de cómo se está trabajando con el sistema de información dentro de la organización, cómo se está concientizando al recurso

humano en los requerimientos de [redacted] también de [redacted] clientes y proveedores, que, de alguna manera u otra, se concatenan o conectan al sistema de información institucional (Yañez, 2017; Peltier, Peltier & Blackley, 2005).

[redacted] activo fundamental y [redacted] mucho valor para las organizaciones son los activos de información, estos pueden ser los archivos generados dentro de la institución, archivos generados fuera de ella, software, hardware, o cualquier otro elemento digital. específicamente la información generada como consecuencia del desarrollo de las actividades operativas o administrativas presentan tres atributos [redacted] accesibilidad o también conocida como disponibilidad. La confidencialidad se refiere a que un archivo o documento es confidencial cuando solo su contenido puede ser conocido por uno o más personas debidamente autorizadas, este activo informático, adquiere el atributo de confidencialidad cuando representa un alto valor para la organización (Vega et al, 2020). El atributo integridad hace referencia a que el archivo o documento debe mantenerse completo, sin variación, sin que le falte ninguna parte en toda su extensión. por último, el atributo accesibilidad o disponibilidad significa que el archivo digital o físico debe ser accesible a las personas autorizadas en el espacio y tiempo especificado. Cuando un activo informático no ha sido variado en estos tres atributos, se puede decir que el sistema presenta un nivel de seguridad aceptable o adecuado (Harold & Tipton, 2008; Fitzgerald, 2007).

Riesgo. Los activos informáticos en cualquier tipo de institución se encuentran expuestos a distintos niveles o grados qué riesgos, el riesgo es definido como un suceso de ocurrencia de un determinado evento que pueda causar daño o efectos negativos, o que podría amenazar a los activos y objetivos de la organización. La posibilidad de que pueda ocurrir un riesgo obedece a una función probabilística (Mujica & Álvarez, 2009; Halvorson, 2008).

Dentro de cualquier sistema de información pueden ocurrir tres tipos de riesgos, riesgos estratégicos, los cuales hacen referencia explícitamente su cuidado adecuado este capital repercute en la imagen de seguridad institucional, esto se explica porque la institución está tomando decisiones estratégicas decididas y que están haciendo frente a los ataques informáticos internos y externos; los riesgos tácticos se refiere a los riesgos ubicados en los sistemas de control y de fiscalización que puedan estar afectarlo a los datos e información institucional, estos riesgos dañan principalmente a estos activos; mientras que los riesgos operacionales se relacionan con los riesgos que se encuentran en los activos con los que se busca lograr los objetivos institucionales, estos pueden ser hardware, software, sistema de red, cronogramas, presupuestos, etc. (MARGERIT. (2012; Cocho & Romo, 2012).

El riesgo también es definido como una cuantificación estimada del nivel de exposición o grado en que una amenaza pueda materializarse en cualquier parte del sistema de información y que tiene una potencialidad de causar perjuicio a este activo institucional, siempre en cuando no se tomen los controles decisiones para garantizar dichos activos. encargados institucional deben saber priorizar la seguridad en función de la importancia y el valor activos en función a ellos, elaborar una estrategia de seguridad de los activos informáticos para poder protegerlos con éxito, y en la misma medida garantizar la sostenibilidad de la organización en el tiempo (MARGERIT, 2012; Endler, 2007).

Análisis un sistema de conlleva al desarrollo actividades y procesos sistemáticos con el propósito de cuantificar la magnitud o tamaño de los riesgos a la que se expone dicho sistema, el análisis consiste en estudiar por separado cada uno de los elementos del activo informático y determinar cuantitativamente el grado de exposición a los riesgos y en función a ello tomar las decisiones correspondientes sobre seguridad informática (Abril, Pulido & Bohada, 2013). La evaluación

consiste en medir el nivel de riesgo, identificar las causas y las vulnerabilidades que dispone frente a la materialización de un determinado riesgo (MARGERIT, 2012; Areitio, 2008).

Amenaza. Se define a las amenazas, que puedan ocurrir en un sistema de información, a las causas potenciales de un evento probabilístico no deseado y que tiene la potencia o capacidad de causar daños a dicho sistema. las amenazas se clasifican por su naturaleza, en este caso, las amenazas provienen por acción de los fenómenos naturales, tales como, sismos, inundaciones, calor excesivo, etc. las amenazas humanas, son aquellos tipos de amenazas generados por usuarios de computadora que tienen la capacidad de poder atacar un determinado sistema de información, lo realizan de manera intencional con intereses propios, la tercera clasificación consiste en amenaza tecnológica, esto se manifiesta en los virus informáticos con los cuales puede causar daños al sistema de información (Rodríguez & Peralta, 2013; Sotelo, Torres & Rivera, 2012).

Vulnerabilidades. La manifiesta el la cual va a permitir según ataque informático se pueda realizar con facilidad, las vulnerabilidades son aprovechadas por los atacantes con la finalidad de hacer daño al sistema de información, principalmente robar la información para después concretar los objetivos que generaron el ataque. se considera vulnerabilidad al escaso conocimiento que puede tener un usuario de computadora los elementos de la seguridad informática. Se hace necesario que una organización busque eliminar sus posibilidades porque de esta manera estaría asegurando un cierto nivel de seguridad informática (CISCO, 2018).

Control. El control de medios permiten manipular y manejar el riesgo, estos medios son las normas nacionales e internacionales sobre seguridad informática, las políticas establecidas por función del sistema

procedimientos, directivas y las prácticas institucionales qué se ha decidido desarrollar dentro de [redacted] establecer [redacted] los activos informáticos (MARGERIT, 2012).

Los controles y que puedan [redacted] clasifican en controles preventivos, este tipo de control se enfocan en la reducción de las vulnerabilidades del sistema de información, los controles defectivos buscan determinar o identificar las amenazas y él contestó de manera anticipada antes de que pueda suceder la materialización de un riesgo, los controles defectivos contribuyen en la activación de los controles requeridos. los controles correctivos permiten la corrección del impacto d la materialización de una amenaza, y por último los controles dice así dos se enfocan en la reducción probabilística de que pueda ocurrir o concretizarse la amenaza (CISCO, 2018).

Ciclo de mejora continua. Para los propósitos de la presente investigación, cómo herramienta metodológica en el objetivo de estudiar y alcanzar un estudio planificado de seguridad, se va a utilizar el ciclo de mejora continua por qué, garantizar la seguridad de hardware y software en una institución edil constituye un proceso repetitivo y de mejora continua en el tiempo, para ello se va a utilizar el ciclo de Deming o ciclo PDCA y ciclo PHVA en español. esta metodología se va a concatenar con la norma ISO 27001:2014 con la cual se busca perfeccionar continuamente la adecuación, conveniencia y seguridad del sistema de información. Por su parte el PDCA forma parte de esta estructura normativa. El ciclo PDCA, para su aplicación correcta en los procesos de garantizar la seguridad de los activos informáticos, se estructura en un conjunto de tapas que van a contribuir en el establecimiento de un modelo ejecutable en el tiempo, ello va a permitir la observación y medición de la mejora de la seguridad informática logrado en función al tiempo (ISO 27000; 2018; Deming, 1982), las etapas son las siguientes:

Plan. En la etapa de planificación se busca implementar [redacted] de [redacted] fase implica analizar [redacted] contexto

institucional, definir metas, objetivos, así como también las políticas que van a contribuir lograr dichos objetivos. en la planificación se identifican las actividades o tareas a realizar en la implementación del sistema de seguridad de los activos informáticos.

Do. La segunda etapa de esta metodología consiste en hacer, por lo tanto esta fase implica implementar y poner en funcionamiento [redacted], por [redacted] tanto, consiste [redacted] aplicar en [redacted] práctica los controles y las políticas relacionados con el análisis de riesgos encontrar, en esta fase se busca disponer y aplicar los procesos y actividades que van a permitir la identificación de las actividades que se debe realizar con la finalidad de asegurar un control adecuado y garantizar la seguridad de la información y todo el sistema.

Check. La tercera fase de esta metodología consiste en desarrollar el monitoreo y fiscalizar cómo se está llevando a cabo el plan de seguridad o [redacted] administración [redacted], consiste [redacted] controlar [redacted] procesos para [redacted] apliquen en la forma indicada y que se estén cumpliendo las metas y objetivos establecidos dentro de un marco de eficacia y eficiencia.

Act. En la cuarta y última etapa esta metodología consiste en actuar, por lo tanto, se tienen como objetivo mejorar sostenidamente y de manera continua la [redacted], para ello [redacted] tiene que definir [redacted] ejecutar [redacted] correctivas [redacted] se han encontrado y diseñado con el propósito de rectificar las vulnerabilidades o fallos encontrados en las etapas anteriores.

El presente estudio se justifica en lo social porque con esta investigacion del plan [redacted] para [redacted] Huari [redacted] presente [redacted], Los usuarios del sistema de información de esta institución edil van a adquirir el conocimiento y las metodologías de cómo enfrentar problemas de riesgos de seguridad información, en ese sentido, los beneficiarios van a ser, los

usuarios del sistema informático, la municipalidad porque su imagen como institución será mejor percibida por los usuarios , y la población que solicita servicios a la institución edil.

La presente investigación se justifica económicamente porque [redacted] garantía [redacted] asegurar [redacted] mediante [redacted] plan [redacted], los activos informáticos se van a mantener íntegros, disponibles y no se va a afectar la confidencialidad de los archivos de importancia, ello va a evitar pérdidas económicas a la institución edil.

La presente investigación se justifica teóricamente porque se fundamenta en teóricamente en los principios fundamentales de la ciencia de los computadores, la ciencia de la información, concretamente en los principios de la seguridad de los activos informáticos, todo ello, en los principios [redacted] de seguridad [redacted].

Se justifica metodológicamente porque [redacted] institución edil en estudio van a conocer los métodos de calidad continua PDCA, la metodología MARGERIT V3.0 y las normas contempladas en la presente investigación, los cuales van a servir de guía para desarrollar los procesos y actividades y el aseguramiento de la información relacionadas con liquidaciones de obras, licitaciones de proyectos de inversión social, información sobre tributaciones, de pagos a proveedores, documentos muy confidenciales para la institución, etc. el plan de seguridad que se alcanza va a permitir actores usuarios adopten una conducta de cómo actuar frente a los riesgos y ataques informáticos que pudieran darse dentro de la institución.

La presente investigación es importante porque se propone mejorar el nivel de protección de la información documentaria e información confidencial creados, distribuidos y almacenados en la municipalidad objeto de estudio. El estudio actual demuestra importancia y relevancia, en tanto que el aporte y los resultados que se

pudieren obtener, mejoren [redacted] situacional [redacted] edil.

[redacted] seguridad [redacted] información Siempre se ha constituido como un problema fundamental en todas las organizaciones que utilizan sistemas de información, específicamente en aquellas que generan y distribuyen información confidencial y en aquellos cuyos activos informáticos representan un alto valor para [redacted] nivel internacional, [redacted], ante los problemas encontrados, estas instituciones han aplicado diversas metodologías con la finalidad de minimizar los riesgos, vulnerabilidades, y ataques informáticos a sus sistemas (Dussan, 2006). Con el transcurrir del tiempo, instituciones internacionales también han contribuido con el desarrollo de metodologías y políticas normativas para garantizar la seguridad de los activos informáticos, así como también, las comunidades internacionales, han creado leyes para castigar las actividades de ataques informáticos a cualquier tipo de organización (Andress, 2015).

A nivel nacional, los ataques a instituciones ediles no son tan significativos como los ataques que se evidencian en los sistemas financieros, no obstante, las municipalidades manejan información confidencial que deben ser resguardados y asegurados de personas naturales o jurídicas que podrían demostrar interés en atacar los atributos de los archivos de estas instituciones, específicamente en los casos [redacted] la [redacted] las instituciones ediles a nivel nacional se ve vulnerada generalmente por los ataques internos, y los archivos más vulnerables y atacados son los archivos que están relacionados con una inversión pública que desarrolla la municipalidad, específicamente en proyectos de alta inversión social, el propósito de ello consiste en conocer Los montos de inversión antes de que el proyecto sea asignado a un ganador; así como esos tipos de archivos existen otros que son altamente confidenciales, tales como los pagos de tributos de las empresas más distinguidas de la comunidad, documentos que puedan adoptar cambios en política y que puedan

generar tendencias económicas positivas o negativas y que puedan ser aprovechadas por quienes tienen acceso a esta información. (Camapaza, 2019)

La Municipalidad Provincial de Huari, como parte del desarrollo de las prestaciones de servicio que tiene que cumplir con la sociedad de su jurisdicción, utiliza un sistema de información, la cual se encuentra integrada con todas las unidades que la estructuran, dentro de cada unidad, los usuarios presentan problema seguridad deficiente, desconoce cómo los usuarios están usando el software y hardware de la institución respecto a las , asimismo, desconoce conocimiento los usuarios respecto al tratamiento de , vulnerabilidad ataques puede estar de edil.

Ante esta realidad problemática, se plantea un plan institución, determinar las relaciones entre los recursos de software y hardware, así como también, con los conocimientos , uso sistema respecto a la seguridad y la conducta que pueden adoptar frente a posibles riesgos de ataques al sistema Huari, 2022. Por consigueinte se formuló el problema: ¿Cuál es la relación del plan con seguridad Municipalidad Provincial Huari, 2022?

A fin de lograr el objetivo del estudio, es fundamental desarrollar estratégico defina las acciones a tomar para proteger hardware, software e información, y de esta manera, evitar los riesgos que pueden dañar la información. En ese sentido se conceptualiza y operacionaliza la variable de estudio. o piratería por parte de ciberdelincuentes.

Plan . Son , normas que orientan el control implementado con el propósito de asegurar los activos

informáticos de una determinada institución, la [redacted] conceptúa al grado [redacted] protección [redacted] todo el [redacted] información o parte de ella como los activos informáticos, es la capacidad de protección que el sistema brinda a datos, archivos, software, hardware en general, frente a ataques internos y externos con propósitos de hacer daño al sistema (CISCO, 2018).

Activos informáticos. Es todo software y hardware que las empresas utilizan con la finalidad de generar información y desarrollar sus actividades como empresa y que son vulnerables a posibles ataques informáticos internos y externos (CISCO, 2018).. Los activos informáticos están constituidos por todos los elementos que contiene un sistema de información, estos son, hardware, software, y el personal qué utiliza el sistema de información, por lo tanto, un activo importante con referencia al usuario, es el conocimiento que dispone cada uno de ellos [redacted] seguridad informática.

Dimensiones [redacted] la [redacted]. en [redacted] estudio se tomaron las dimensiones de **Gestión de riesgos.** dimensión que tiene como indicadores al Hardware, software, nube, redes sociales. Estos indicadores son los que contienen los riesgos que se generan con su uso por parte de los usuarios. **Gestión de seguridad**. esta dimensión contiene [redacted] indicadores: [redacted] riesgos, [redacted] vulnerabilidades, Conocimiento [redacted] ataques, y Nivel de protección (Zapata, 2020).

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: **Software**. dimensión que contiene a los siguientes indicadores: Integridad, confidencialidad y disponibilidad. **Hardware** que contiene a los indicadores amenazas, ataques repelidos e incidentes, **Conocimientos,** que contiene a los indicadores: Conocimiento de ataques, conocimiento de software de seguridad y conocimiento de hardware de seguridad (Santana, 2012).

Tabla 1

Operacionalizacion de la variable

Variable	Dimensión	Ítems
[redacted]	Identificación	¿Cómo valora la identificación [redacted]?
		¿Cómo califica [redacted] identificación [redacted]?
		¿Cómo evalúa [redacted] identificación [redacted] las responsabilidades [redacted] activo [redacted] información?
	Planificación	¿Cómo considera la planificación de [redacted]?
		¿Cómo evalúa [redacted] temas [redacted] hardware contemplados en [redacted] plan [redacted] seguridad [redacted] información?
		¿Cómo califica en las [redacted] implementadas [redacted] plan [redacted] seguridad [redacted] en [redacted] Provincial [redacted] Huari, 2022?
		¿Cómo evalúa la capacitación considerada en [redacted]?
	Hacer	¿Cómo [redacted] ejecución [redacted] seguridad a nivel [redacted] hardware [redacted] sistema [redacted]?
		¿Cómo califica la ejecución de la seguridad a nivel de software en el sistema de la información?
		¿Cómo valora la ejecución de [redacted] el sistema de [redacted]?
		¿Cómo evalúa [redacted] ejecución [redacted] capacitación en [redacted]?
	Verificar	¿Cómo considera [redacted] verificación [redacted] seguridad a nivel [redacted] hardware en el sistema de la información?
		¿Cómo califica la verificación de la seguridad a nivel de software en el sistema de la información?
		¿Cómo valora la verificación de [redacted] en [redacted] sistema [redacted] información?
		¿Cómo evalúa [redacted] verificación [redacted] capacitación en [redacted]?
	Actuar	¿Cómo considera el control de la seguridad a nivel de hardware en el sistema de la información?
		¿Cómo [redacted]fica el control de la seguridad a nivel de software en el sistema [redacted]?
		¿Cómo va[redacted] [redacted] control [redacted] la [redacted] en [redacted]
		[redacted] evalúa [redacted] control [redacted] capacitación en [redacted]?
		¿Cómo califica [redacted] física del sistema [redacted]?

Activos Informáticos	Seguridad hardware	¿Cómo considera la seguridad en el servidor de red del sistema de información?
		¿Cómo valora la seguridad en sistema ?
		¿Cómo evalúa la cableado del
		califica la de los Access point del sistema de información?
		¿Cómo considera computadora escritorio información?
	software	¿Cómo califica la seguridad del sistema operativo del sistema de información?
		¿Cómo considera la seguridad de los softwares de procesamiento de texto del ?
		¿Cómo valora seguridad base datos del sistema ?
		¿Cómo evalúa la seguridad de más importante ?
		¿Cómo califica del software antivirus en el sistema de información?
		¿Cómo considera la seguridad del software frente a ataques internos o externos en el sistema de información?
		¿Cómo califica la seguridad lógica en general del sistema de información?
	Conocimiento del personal	¿Cómo califica el dominio de hardware por parte del personal?
		¿Cómo considera el dominio del software por parte del personal?
		¿Cómo valora la administración de las claves de acceso al sistema por parte del personal?
		¿Cómo evalúa el dominio de la seguridad informática del personal?
		¿Cómo califica el uso del software antivirus en el sistema de información por parte del personal
		¿Cómo considera el dominio de importancia?

el se planteó como hipótesis: El plan de propuesto relaciona positivamente con seguridad informáticos Municipalidad Provincial de Huari, 2022.

Por otro lado, se formuló el objetivo general: Determinar la relación del plan con seguridad Municipalidad Provincial Huari, 2022. Así mismo. Los objetivos específicos:

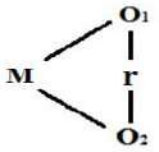
- Determinar la relación del plan con recursos software Municipalidad Provincial de Huari, 2022.

- Establecer la relación del plan [redacted] con [redacted] recursos [redacted] hardware [redacted] Municipalidad Provincial de Huari, 2022.
- Determinar la relación [redacted] los conocimientos [redacted] informática de [redacted] Municipalidad Provincial de Huari, 2022.

METODOLOGÍA

El tipo del presente estudio va a ser de tipo descriptivo correlacional, esto se explica porque, se van a establecer los grados de [redacted] plan [redacted] información [redacted] variable activos informáticos, así como también entre [redacted] plan [redacted] con las dimensiones [redacted] segunda [redacted], esto es, software, hardware y conocimiento (Bernal, 2010; Valarino, 2010).

En la investigación no se manipula la variable plan de [redacted] luego observar [redacted] impacto [redacted] del objeto [redacted] estudio, por tanto, no experimental. Por la captación de datos, el tipo de investigación es transversal por qué se midió las variables una sola vez durante todo el proceso de investigación. El enfoque es positivista también considerado como cuantitativo, esto se debe a que las variables, sus dimensiones e indicadores, se van a medir cuantitativamente. (Hernández, Fernández y Baptista, 2010).



Dónde:

M = Sistema informático de la Municipalidad Provincial de Huari

O1 = Observación [redacted] plan [redacted]

O2 = Observación [redacted] activos informáticos [redacted] la Municipalidad Provincial de Huari

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

Los usuarios del sistema de información de Municipalidad Provincial de Huari, la misma que está constituida por 24 usuarios del sistema de información edil en el desempeño de sus labores que se desarrollan en cada área o unidad, la siguiente tabla evidencia la cantidad de usuarios por cada unidad de prestación de servicios ediles.

Tabla 2

Población de usuarios del sistema de información

N°	Unidad o área	Cantidad de usuarios
01	Alcaldía	05
02	Gerencia Municipal	02
03	Gerencia Planificación y Presupuesto	02
04	Gerencia de desarrollo social	02
05	Gerencia de Administración Tributaria y cntas	03
06	[redacted]	03
07	[redacted] Infraestructura [redacted] Desarrollo Social	03
08	[redacted] y Ambiental	02
09	Secretaría General	02
	TOTAL	**24**

La muestra esta conformada por el mismo tamaño de la población, esto significa, 24 usuarios del sistema de información de [redacted] Huari.

Técnica: [redacted] recabar [redacted] datos e información de las dos variables en estudios se va a aplicar la técnica de la encuestan y se va a aplicar a los elementos de la muestra, esto es, a los empleados que utilizan el sistema informático [redacted].

Instrumento: El instrumento [redacted] va [redacted] aplicar para obtener los datos e información de los elementos de la muestra será el cuestionario, la cual va a contener las preguntas pertinentes que van a permitir medir la relación [redacted] Plan de [redacted] con [redacted] activos

informáticos. Para que sea aplicado, se va a determinar la confiabilidad con [redacted] cuyo valor deberá ser mayor a 0.80; y la validez mediante el método de Juicio de Expertos, en este caso, para que sea aceptada, el instrumento deberá tener, en promedio, las calificaciones de muy o excelente.

Tabla 3

Técnicas e instrumentos de investigación

Técnicas	Instrumentos
Encuestas	Cuestionarios
Análisis documental	Textos, tesis, artículos científicos, revistas cientificas e investigaciones antecedentes

La metodología de desarrollo consistirá en lo siguiente: en el marco normativo se va a utilizar la norma internacional ISO 27001: 2014, como metodología se va a aplicar MAGERIT V3:

[redacted] va a analizar [redacted] riesgos en cada una de las unidades de la Municipalidad Provincial de Huari, primero, se va a realizar un inventario de hardware software y personal a cargo [redacted] y usuarios, en [redacted] caso, se va [redacted] riesgos a los que está expuesto el hardware de la institución edil, se va a analizar las vulnerabilidades y los conocimientos de los usuarios [redacted], se va a analizar el riesgo existente cuando hacen uso de la nube y las redes sociales. También se va a analizar la gestión de la seguridad actual respecto a cómo están identificando los riesgos, las vulnerabilidades, que conocimiento disponen sobre los ataques y los niveles de protección con los que cuentan. Se va a analizar el nivel se seguridad de la información, específicamente a los archivos más importantes en función a los atributos e disponibilidad, integridad y confidencialidad.

Tratamiento de riesgos: Respecto al tratamiento de riesgos se va analizar en cada una de las unidades o áreas de la institución edil [redacted] las

normas [redacted] que están aplicando, [redacted] medios tecnológicos [redacted] disponen para enfrentar los riesgos; cómo están utilizando los medios de control de riesgos. También se va a analizar los conocimientos que los empleados usuarios del sistema información dispones [redacted], se va analizar [redacted] dominios sobre uso [redacted] hardware, software, [redacted] e [redacted], etc.

Selección de salvaguardas: En este proceso se va analizar los mecanismos de control que están realizando los empleados de la municipalidad, los controles que se van a analizar hacen referencia a los controles en la seguridad de hardware, software y conocimiento de los usuarios aspecto a la [redacted]. Se [redacted] controlar [redacted] seguridad de [redacted] archivos [redacted] alta confidencialidad, específicamente en el cuidado de sus tres principales atributos: confidencialidad, integración y disponibilidad.

Metodología del estudio: Se va a utilizar la metodología de la mejora continua o Ciclo PDCA o ciclo PHVA que consiste en **planificar** y que consiste en planificación [redacted], se va a analizar el contexto institucional, definir metas, objetivos, así como también las políticas que van a contribuir lograr dichos objetivos. en la planificación se identifican las actividades o tareas a realizar en la implementación del sistema de [redacted]. **Hacer.** [redacted] segunda etapa de esta metodología va a consistir en poner en funcionamiento el plan [redacted], estos significa que [redacted] va a poner [redacted] práctica [redacted] las políticas relacionados con el análisis de riesgos encontrar, en esta fase se busca disponer y aplicar los procesos y actividades que van a permitir la identificación de las actividades que se debe realizar con la finalidad de asegurar un control adecuado y garantizar la seguridad de la información y todo el sistema. **Verificar.** En esta fase se va a desarrollar el monitoreo y fiscalización sobre cómo se está llevando a cabo [redacted]

[redacted], consiste [redacted] controlar [redacted] procesos para que [redacted] apliquen en la forma indicada y que se estén cumpliendo las metas y objetivos establecidos dentro de un marco de eficacia y eficiencia. **Actuar.** En esta etapa se va a tratar de [redacted], para ello va a definir y ejecutar acciones correctivas que se han encontrado y diseñado con el propósito de rectificar las vulnerabilidades o fallos encontrados en las etapas anteriores.

RESULTADOS

plan seguridad de la la seguridad los recursos software.

Tabla 4

Correlación entre con la Seguridad software

		Plan de seguridad	software
Plan de seguridad			
Seguridad software			

).

Plan de seguridad seguridad software encontrada fue 0.745, este resultado existió positiva Plan seguridad dimensión seguridad software. El p valor fue de 0.000, lo cual es menor a 0.05, lo cual confirma que los datos no correspondieron a una curva normal.

objetivo específico 2

Establecer la relación del plan con recursos hardware Municipalidad Provincial de Huari, 2022.

Tabla 5

Correlación entre [redacted] *con la* [redacted] *Seguridad* [redacted] *hardware*

			Plan de seguridad	Seguridad de hardware
[redacted]	Plan [redacted] seguridad	[redacted]	1,000	,763**
		[redacted]	.	,000
		N	24	24
	Seguridad [redacted] hardware	Coeficiente de [redacted]	,763**	1,000
		[redacted]	,000	.
		[redacted]	24	24

**. [redacted] en el [redacted]

[redacted] Plan de seguridad [redacted] seguridad [redacted] hardware encontrada fue 0.763, este resultado [redacted] existió [redacted] positiva [redacted] Plan [redacted] seguridad [redacted] dimensión seguridad [redacted] hardware. El p valor fue de 0.000, lo cual es menor a 0.05, lo cual confirma que los datos no correspondieron a una curva normal.

Objetivo específico 6

Determinar la relación [redacted] los conocimientos [redacted] informática de [redacted] Municipalidad Provincial de Huari, [redacted]

[redacted] 7 [redacted] *variable Plan* [redacted] *con* [redacted] *dimensión Conocimiento personal*

			Plan de [redacted]	Conocimiento del personal
[redacted]	Plan [redacted]	[redacted]	[redacted]	,794**
		[redacted]	.	,000
		[redacted]	24	24
[redacted]	Conocimiento del personal	[redacted]	,794**	1,000
		[redacted]	,000	.
		[redacted]	24	24

[redacted]).

La relación entre la variable Plan de seguridad y la dimensión conocimiento del personal encontrada fue 0.794, este resultado existió positiva Plan seguridad dimensión Conocimiento del personal. El p valor fue de 0.000, lo cual es menor a 0.05, lo cual confirma que los datos no correspondieron a una curva normal.

Objetivo general

Determinar la relación del plan con seguridad Municipalidad Provincial Huari, 2022.

Tabla 8

Correlación entre la variable Plan de Seguridad con la variable Seguridad de los activos informáticos

		Plan de seguridad	Seguridad de los activos informáticos
Plan de seguridad			,788**
	N	24	24
Seguridad de los activos informáticos		,788**	1,000
		,000	.

).

Plan de seguridad variable Seguridad la información encontrada fue 0.788, este resultado existió positiva Plan seguridad variable Seguridad los activos informáticos. El p valor fue de 0.000, lo cual es menor a 0.05, lo cual confirma que los datos no correspondieron a una curva normal.

ANÁLISIS Y DISCUSIÓN

En este estudio se encontró que existió relación positiva alta de 0.788 entre la variable Plan de seguridad y la variable Seguridad de los activos informáticos, los cuales coinciden parcialmente con los resultados de la investigación de Huacón (2022) quien tuvo el resultado de que las empresas adquieren fragilidad cuando crecen y tienden a ser atacados generalmente por agentes externos para extorsionar y robar activos informáticos, etc., que las herramientas informáticas se seleccionan en función a las necesidades de obtención de los datos, el cual debe cumplir con parámetros alcanzados para su gestión. Que se encontraron conductas e información de vulnerabilidades que puede estar expuestos y que los datos permitieron realizar un estudio riguroso sobre seguridad informática institucional.

En el presente estudio se encontró que 11 seguridad mejoró informáticos una institución edil con un valor de relación positiva alta de 0.788, estos resultados coinciden parcialmente con los obtenidos por Ramírez (2020) en donde se tuvo que las empresas a están expuestas a ataques informáticos a medida que crecen, que los datos se vuelven vulnerables, aunque la investigación antecedente no mostró resultados de correlación, mostraron conductas e información de vulnerabilidades en donde se expuso a la institución, los datos permitieron llevar a cabo un estudio profundo y sistemático de la elaboración de probables resultados fundamentados en normas de seguridad.

En este estudio se tuvo que 11 seguridad mejoró informáticos una institución edil con un valor de relación positiva alta de 0.788, estos resultados coinciden parcialmente y también difieren parcialmente con los resultados de la investigación antecedente de Zapata (2020) quién encontró que en el espacio estudiado no tuvieron 6 los procesos realizados fundamentaron en políticas establecidas, que aplicaron ciertas normas de manera general y aislada, por tanto, no garantizaron la seguridad del sistema de información a nivel de software y hardware, existieron deficiencias y errores adminsitrativos y gestión relacionados con la seguridad de la información,

especialmente en los servidores debido a que procesaran datos importantes y estuvieron .

Las conclusiones de la presente investigación indicaron que seguridad mejoró informáticos una institución edil con un valor de relación positiva alta de 0.788, estos resultados coinciden parcialmente y también difieren parcialmente con los resultados del antecedente de Vargas (2019) quien encontró que los procesos fueron evaluados por distintas personas, no hubo capacitación, tampoco información relacionados con los procesos y métodos utilizados, existió considerable nivel de confianza en las habilidades, capacidades y competencias del personal, no existió , tampoco privacidad conocimientos del personal sobre seguridad informática estuvieron bastante bajos, esto difirió significativamente con los resultados presente

encontró que plan seguridad mejoró la seguridad de los activos informáticos de una institución edil con un valor de relación positiva alta de 0.788, estos resultados coinciden parcialmente y también difieren parcialmente con los resultados de la investigación antecedente de Pacheco (2018) quien concluyó que Plan Políticas se constituyó alternativa solución que protegió administró de manera eficiente los procesos de control, pudo prevenir las ocurrencias generados por riesgos a la información.

Los resultados del presente estudio indicaron que seguridad mejoró informáticos una institución edil con un valor de relación positiva alta de 0.788, parcialmente Camapaza (2019) en donde se encontró que el 100% indicaron divulgó información sensible, para el 75% nunca se realizó evaluación de riesgos, el 50% no realizó copia de seguridad, el 75% señala que su oficina no estuvo protegida contra ataques informáticos, que MARGERIT v.3 contribuyó en el dimensionamiento de posibles ocurrencias del

riesgo, elaboraron [redacted] con la cual se pudo minimizar los riesgos de diferentes niveles establecidos para el diseño [redacted].

Se tuvo [redacted] encontró que [redacted] mejoró [redacted] seguridad [redacted] una [redacted] edil con un valor de relación positiva alta de 0.788, estos resultados coinciden parcialmente y también difieren parcialmente con los resultados de la investigación antecedente de Monteza (2019) quién encontró que el 34% de los empleados fueron descuidados o inconscientes, el 26% indicaron que los controles de seguridad estuvieron obsoletos, para el 13% pueden ingresar al sistema sin autorización, que se encontraron 72% de activos de información con grado de alta criticidad, que existieron 44% de activos de información con alto riesgo alto y medio con un 44%.

En los resultados del presente estudio se encontró que [redacted] seguridad mejoró [redacted] informáticos [redacted] una institución edil con un valor de relación positiva alta de 0.788, estos resultados coinciden parcialmente y también difieren con la investigación de Poicon y Ramírez (2020) quienes tuvieron que el [redacted] fue [redacted] con [redacted] impacto del riesgo fueron bajo y medio en los activos de la información; y el nivel de los riesgos fue 30%, en riesgo de daños fue 15% y para un riesgo serio fue del 4%, que de 114 controles, 63 de estos no se cumplieron alguna evidencia, la cual no se encontró sistematizada, estuvo en directivas que todavía fueron aprobadas institucionalmente, por lo tanto, no se registraron indicadores relacionados con el diagnóstico antes de [redacted].

En [redacted] investigación [redacted] tuvo que [redacted] plan [redacted] mejoró [redacted] seguridad [redacted] una [redacted] edil con un valor de relación positiva alta de 0.788, estos resultados coinciden parcialmente y también difieren parcialmente con los resultados de la investigación antecedente de Vásquez y Rengifo (2019) quien concluyó que mediante análisis de riesgo determinaron los temas más importantes del cuidado y seguridad de los equipos, en función a presencia de vulnerabilidad con el propósito de dar protección y gestión de información, manteniendo [redacted] la [redacted]

edil, que plan acción y emergencia procedimientos fue satisfactorio porque permitió conocer las deficiencias ediles, en base a la cual se logró alcanzar la mejora con el propósito de contrarrestar dicha problemática.

Se tuvo en la investigación se encontró que seguridad mejoró informáticos una institución edil con un valor de relación positiva alta de 0.788, estos resultados coinciden parcialmente y también difieren parcialmente con los resultados de la investigación antecedente de Armas y Pérez (2018) debido a que aplicaron la misma metodología MAGERIT, la cual permitió identificar los puntos importantes en el poseso de , permitió logar resultados estado riesgo.

CONCLUSIONES RECOMENDACIONES

Conclusiones

Se concluyó a nivel general que existió relación positiva alta de 0.788 entre la variable Plan de seguridad y la variable Seguridad de los activos informáticos, el p valor fue de 0.000, esto indicó que los datos no correspondieron a una curva normal.

Existió relación positiva alta de 0.745 entre la variable Plan de seguridad y la dimensión seguridad de software, el p valor fue de 0.000, lo cual confirmó que los datos no correspondieron a una curva normal.

Existió relación positiva alta de 0.763 entre la variable Plan de seguridad y la dimensión seguridad de hardware el p valor fue de 0.000, lo cual indicó que los datos no correspondieron a una curva normal.

Existió relación positiva alta de 0.794 entre la variable Plan de seguridad y la dimensión conocimiento del personal el p valor fue de 0.000, lo cual indicó que los datos no correspondieron a una curva normal.

RECOMENDACIONES

La Gerencia Municipal y [redacted] Municipalidad Provincial [redacted] Huari deben tomar decisiones respecto a los resultados de [redacted] Plan [redacted] seguridad [redacted] Seguridad [redacted] los activos informáticos, estas decisiones deben enfocarse en la mejora de ambas variables, pero con la participación activa y decidida de la parte administrativa y operativa, específicamente de los empleados que utilizan cotidianamente el sistema de información edil.

La Gerencia Municipal y [redacted] Municipalidad Provincial [redacted] Huari deben seguir o continuar con la capacitación a los empleados ediles en las actualizaciones sobre la seguridad de software, específicamente en seguridad del sistema operativos, seguridad de base de datos, uso e instalación de programas antivirus, to ello dentro de las políticas del plan de seguridad, para ello deben contar con la participación de especialistas.

La Gerencia Municipal y [redacted] Municipalidad Provincial [redacted] Huari deben seguir o continuar con la capacitación a los empleados ediles en las actualizaciones sobre la seguridad de hardware, especialmente en el uso adecuado de la computadora y sus periféricos, así como, la adopción de conductas en el manejo de claves y acceso a los sistemas.

La Gerencia Municipal y [redacted] Municipalidad Provincial [redacted] Huari deben continuar con las capacitaciones en el conocimiento del personal en los temas de la seguridad de hardware y software, así como también en la [redacted] activos informáticos de la institución edil.

AGRADECIMIENTOS

A Dios por permitirme el objetivo de ser profesional, a la Municipalidad Provincial de Huari 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.

Maritza

REFERENCIAS BIBLIOGRÁFICAS

Abril, A., Pulido, J., & Bohada, J. A. (2013). *Análisis de Riesgos en Seguridad de la Información,* Recuperado de https://www.jdc.edu.co/revistas/index.php/rciyt/article/view/121/113

Andress, J. (2015). *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*. Massachusetts, Estados: Elsevier, 2015.

Areitio, J. (2008). *Seguridad de la Información, Redes, Informática y Sistemas de Información*. Madrid: Paraninfo.

Armas, Angélica Madeleine y Pérez, Flor Rosmery (2018). *Desarrollo de un sistema de gestión de seguridad de la información para minimizar riesgos en los activos de información en la sub gerencia de informática y telecomunicaciones de la Municipalidad Distrital de Independencia 2016*. Universidad Nacional Santiago Antúnez de Mayolo. Huaraz Perú.

Bernal, C. (2010). *Metodología de la Investigación*. Tercera edición. Bogotá: Editorial Pearson Educación de Colombia Ltda.

Camapaza, Abdon Anders (2019) *Diseño del plan de seguridad informática basado en la NTP ISO/IEC 27001:2014 para la municipalidad del centro poblado de Salcedo – Puno*. Tesis de grado. Universidad Andina de Cusco. Perú.

CISCO. (2018). *Lo que usted necesita saber sobre seguridad de la red*. Obtenido de http://www.cisco.com/web/LA/soluciones/la/information_security/index.h

Cocho, J., & Romo, M. (2012). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*.

De Freitas, Vidalina (2012). *Sistema de Gestión de Seguridad de la Información*. Primera ed. Venezuela: EAE.

Deming, W. E. (1982). *Quality, productivity, and competitive position* (Vol. 183): Massachusetts Institute of Technology, Center for advanced engineering study.

Dussan, C. (2006). *Políticas de Seguridad Informática*. *Entramado*, *2*(1), 86–92.

Endler, D. (2007). *Hacking Exposed VoIP: Voice Over IP Security Secret & S*olutions. Osborne: Mc Graw-Hill.

Farias, M., Mendoza, M., & Gómez, L. (2003). Las Políticas de Seguridad como Apoyo a la Falta de Legislación Informática. *Techno-legal Aspects of Information Society and New Economy: An Overview*, *I*, 185–191.

Fitzgerald, T. (2007). *Information Security Governance*. En H. Tipton, & M. Krause, Information Security Management Handbook (págs. 15-34). USA: Auerbach.

Garre, S.; Tortajada, S. H. y Cruz, A. (2018). *Sistema de gestión de la seguridad de la información.* Primera ed. España: Editorial UOC.

Halvorson, N. (2008). *Information Risk Management: A Process Approach to Risk Diagnosis and Treatment*. *Information Security Management Handbook*. USA: Auerbach Publications.

Harold, F & Tipton, M. K. (2008). *Information security management handbook*. Sexto ed. Tipton HF, editor. Nueva York: Auerbach.

Hernández, R.; Fernández, C. y Baptista, P. (2010). *Metodología de la investigación*. Quinta edición. México: Mc Graw Hill. ISBN: 978-607-15-0291-9

Huacón (2022) *Vulnerabilidades de la seguridad de la información y su incidencia en el departamento de sistemas del Municipio de Babahoyo*. Tesis de grado. Universidad Estatal Península de Santa Elena, La Libertad, Ecuador.

INDECOPI. (2014*). Norma Técnica Peruana NTP-ISO/IEC 27001:2014. Tecnología de la información. Técnicas de seguridad. Sistema de gestión de seguridad de la información. Requisito*.". Lima: Segunda Edición.

ISO 27000. (2018). ISO 27000.es. Obtenido de El Portal de ISO 27001 en español: http://www.iso27000.es/iso27000.html

MARGERIT. (2012). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Madrid: Ministerio de Hacienda y Administración Pública.

Miguel, C. (2015). *Protección de datos y seguridad de la información*. Cuarta ed. España: Ra-Ma; 2015.

Monteza Mera, Lisbet Odelly (2019). *Diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2013 para la Municipalidad Distrital de El Agustino*. Tesis de grado. Universidad Peruana de Ciencias Aplicadas. Lima. Perú.

Mujica, M., & Álvarez, J. (2009). *El Análisis de Riesgo en la seguridad de la* información, *4*, .33–37.

Pacheco, L. A. (2018). *Políticas de seguridad de la información de aprovechamiento estudiantil en la educación general básica basado en la norma ISO 27002*. Tesis de maestría. Universidad Espíritu Santo. Ecuador.

Peltier, T., Peltier, J., & Blackley, J. (2005). *Information Security Fundamentals*. USA: Auerbach Publications.

Poicon, Junior Miguel Ángel y Ramírez, Oscar (2020). *Propuesta de un sistema de gestión de seguridad de la información para la Municipalidad Distrital de Marcavelica, mediante la NTP- ISO/IEC 27001:2014*. Tesis de grado. Universidad César Vallejo. Piura. Perú.

Ramírez, A. F. (2020). *Análisis proactivo de amenazas de la seguridad informática y de la información para la infraestructura de servidores y red de la dirección de tic de un GAD municipal*. Universidad Estatal Península de Santa Elena, La Libertad, Ecuador.

Rodríguez, J. M., & Peralta, I. (2013). *Gestión de Riesgos*. tiThink Consultoría. Recuperado de https://www.tithink.com/publicacion/MAGERIT.pdf

Santana, C. (2012). Seguridad Informática: ¿Qué es una vulnerabilidad, una amenaza y un riesgo? Recuperado de https://www.codejobs.com/es/blog/2012/09/07/seguridad-informatica-que-es-una-vulnerabilidad-una-amenaza-y-un-riesgo

Sotelo, M., Torres, J., & Rivera, J. (2012). *Un Proceso Práctico de Análisis de Riesgos de Activos de Información*. Recuperado de http://www.comtel.pe/comtel2012/callforpaper2012/P26C.pdf

Stair, R., & Reynolds, G. (2017). *Fundamentals of information systems. Cengage Learning*. https://books.google.es/books?hl=es&lr=&id=GtVBDgAAQBAJ&oi=fnd&pg=PP1&dq=information+systems&ots=k24BRDcXuB&sig=xyQYIakwCMLuoVoYjhU96JYjOXY#v=onepage&q=information%20systems&f=false

Stallings, W. (2004). *Fundamentos de Seguridad en Redes*. Madrid: Pearson Prentice Hall.

Valarino, E. (2010). *Metodología de la Inves*tigación. Paso a Paso. México DF: Trillas.

Vargas, H. (2019). *Plan de gestión de seguridad de la información para la secretaría de educación del municipio de yumbo, en cumplimiento de la estrategia de gobierno en línea de Colombia*. Tesis de maestría. Universidad Santiago de Cali, Colombia.

Vásquez, Dennis Alberto y Rengifo, Paulo Manuel (2019). *Propuesta de plan de seguridad informática para la sub gerencia de tecnología de la información de la municipalidad provincial de requena, en el año 2019*. Tesis de grado. Universidad Científica del Perú. Loreto.

Vega, L.; López, F.; Ramírez, J. F. y Orellana, A. (2020). *Impacto de las aplicaciones y servicios informáticos desarrollados por la Universidad de las Ciencias Informáticas para el sector de la salud. Artículo científico. Universidad de las Ciencias Informáticas, Cuba*. Revista Cubana de Informática Médica 2020:12(1)58-75.

Voutssas, J. (2010). Preservación documental digital y seguridad informática. Recuperado de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2010000100008

Yañez, N. A. (2017). *Sistema de gestión de seguridad de la información para la subsecretaria de economía y empresas de menor tamaño*. Santiago de Chile: Universidad de Chile, 2017.

Zapata, K. B. (2020). *Sistema de gestión de seguridad de la información basado en las normas ISO/IEC 27001, en el departamento de tecnologías de la información del gobierno autónomo descentralizado de la municipalidad de Ambato*. Tesis de grado. Universidad Técnica de Ambato. Ecuador.

USP
UNIVERSIDAD SAN PEDRO

REPOSITORIO INSTITUCIONAL DIGITAL

FORMULARIO DE AUTORIZACIÓN PARA LA PUBLICACIÓN DE DOCUMENTOS DE INVESTIGACIÓN

1. Información del Autor

Apellidos y Nombres	DNI	Correo Electrónico
CHIQUIAN CRISPIN EDA MARITZA	44620400	chiquian18@gmail.com

2. Tipo de Documento de Investigación

Tesis	Trabajo de Suficiencia Profesional	Trabajo Académico	Trabajo de Investigación
X			

3. Grado Académico o Título Profesional [1]

Bachiller	Título Profesional	Título Segunda Especialidad	Maestría	Doctorado
	X			

4. Título del Documento de Investigación

PLAN DE SEGURIDAD DE LA INFORMACION EN LA SEGURIDAD DE LOS ACTIVOS INFORMATICOS DE LA MUNICIPALIDAD PROVINCIAL DE HUARI, 2022.

5. Programa Académico

INGENIERIA INFORMATICA Y DE SISTEMAS.

6. Tipo de Acceso al Documento

Abierto o Público [2] (info:eu-repo/semantics/openAccess)	Acceso restringido [3] (info:eu-repo/semantics/restrictedAccess) (*)
X	

(*) 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	26	01	2024

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. X, inciso 10.2
2. Ley N° 30035. Ley que regula el Repositorio Nacional Digital de Ciencia, Tecnología e Innovación de Acceso Abierto y D.S. 006 -2017-PCM.
3. Si el autor eligió el tipo de acceso abierto o público, otorga a la Universidad una licencia no exclusiva, para que se pueda hacer acopios de datos en la obra y difundir en el Repositorio Institucional Digital. Sin perjuicio 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, deberá retirar los datos del autor y revisores de la obra, de acuerdo a la directiva N° 004-2016-CONCYTEC-DRDC (Numerales 5.2 y 6.1) 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 permiten garantizar 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, las Escuelas y demás instituciones de educación superior tienen como obligación registrar todos los trabajos de investigación y proyectos, incluyendo los metadatos en sus repositorios institucionales promoviendo el acceso 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, inc. 32.3)

Plan de seguridad de la información en la seguridad de los activos informáticos de la Municipalidad Provincial de Huari, 2022

INFORME DE ORIGINALIDAD

INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE
21%	20%	4%	9%

FUENTES PRIMARIAS

1	repositorio.ucv.edu.pe Fuente de Internet	3%
2	Submitted to Universidad Cesar Vallejo Trabajo del estudiante	2%
3	hdl.handle.net Fuente de Internet	1%
4	repositorio.uta.edu.ec Fuente de Internet	1%
5	repositorio.uladech.edu.pe Fuente de Internet	1%
6	repositorio.undac.edu.pe Fuente de Internet	1%

7	repositorio.usanpedro.edu.pe Fuente de Internet	1%
8	repositorioacademico.upc.edu.pe Fuente de Internet	1%
9	repositorio.unsm.edu.pe Fuente de Internet	1%
10	docplayer.es Fuente de Internet	1%
11	repositorio.unp.edu.pe Fuente de Internet	1%
12	repositorio.upci.edu.pe Fuente de Internet	<1%
13	repositorio.uwiener.edu.pe Fuente de Internet	<1%
14	es.slideshare.net Fuente de Internet	<1%
15	Submitted to Escuela Politecnica Nacional Trabajo del estudiante	<1%

16	repositorio.unheval.edu.pe Fuente de Internet	<1%
17	repositorio.upt.edu.pe Fuente de Internet	<1%
18	"Information and Communication Technologies of Ecuador (TIC.EC)", Springer Science and Business Media LLC, 2019 Publicación	<1%
19	Submitted to Universidad Nacional del Centro del Peru Trabajo del estudiante	<1%
20	prezi.com Fuente de Internet	<1%
21	repositorio.unprg.edu.pe Fuente de Internet	<1%
22	rraae.cedia.edu.ec Fuente de Internet	<1%
23	repositorio.uisek.edu.ec Fuente de Internet	<1%
24	Submitted to Universidad Privada San Pedro Trabajo del estudiante	<1%

25	repositorio.uees.edu.ec Fuente de Internet	<1%
26	repositorio.espam.edu.ec Fuente de Internet	<1%
27	repositorio.sibdi.ucr.ac.cr:8080 Fuente de Internet	<1%
28	repositorio.ug.edu.ec Fuente de Internet	<1%
29	alejandria.poligran.edu.co Fuente de Internet	<1%
30	repositorio.usmp.edu.pe Fuente de Internet	<1%
31	repositorio.escuelamilitar.edu.pe Fuente de Internet	<1%
32	repositorio.ucp.edu.pe Fuente de Internet	<1%
33	dspace.concytec.gob.pe Fuente de Internet	<1%
34	estrategia.gobiernoenlinea.gov.co Fuente de Internet	<1%

35	Submitted to Universidad Continental Trabajo del estudiante	<1%
36	idoc.pub Fuente de Internet	<1%
37	Submitted to Universidad Anahuac México Sur Trabajo del estudiante	<1%
38	Submitted to Universidad Andina Nestor Caceres Velasquez Trabajo del estudiante	<1%
39	Submitted to Universidad Internacional de la Rioja Trabajo del estudiante	<1%
40	www.cartagena.gov.co Fuente de Internet	<1%
41	Submitted to Centro Europeo de Postgrado CEUPE Trabajo del estudiante	<1%
42	Submitted to Universidad Nacional Abierta y a Distancia Trabajo del estudiante	<1%

43	cdn.www.gob.pe Fuente de Internet	<1%
44	pt.scribd.com Fuente de Internet	<1%
45	moam.info Fuente de Internet	<1%
46	repositorio.autonoma.edu.pe Fuente de Internet	<1%
47	repository.unad.edu.co Fuente de Internet	<1%
48	www.coursehero.com Fuente de Internet	<1%
49	www.map.es Fuente de Internet	<1%
50	cia.uagraria.edu.ec Fuente de Internet	<1%
51	publicaciones.usanpedro.edu.pe Fuente de Internet	<1%
52	repositorio.ecci.edu.co Fuente de Internet	<1%

53 www.amazoniainvestiga.info

Fuente de Internet <1%

---

www.g2security.com

54 Fuente de Internet <1%

---

www.revistaespacios.com

55 Fuente de Internet <1%

Excluir citas	Apagado	Excluir coincidencias	< 10 words
Excluir bibliografía	Activo		

Plan de seguridad de la información en la seguridad de los activos informáticos de la Municipalidad Provincial de Huari, 2022

INFORME DE GRADEMARK

NOTA FINAL /0

COMENTARIOS GENERALES

Instructor

PÁGINA 1

PÁGINA 2

PÁGINA 3

PÁGINA 4

PÁGINA 5

PÁGINA 6

PÁGINA 7

PÁGINA 8

PÁGINA 9

PÁGINA 10

PÁGINA 11

PÁGINA 12

PÁGINA 13

PÁGINA 14

PÁGINA 15

PÁGINA 16

PÁGINA 17

PÁGINA 18

PÁGINA 19

PÁGINA 20

PÁGINA 21

PÁGINA 22

PÁGINA 23

PÁGINA 24

PÁGINA 25

PÁGINA 26

PÁGINA 27

PÁGINA 28

PÁGINA 29

PÁGINA 30

PÁGINA 31

PÁGINA 32

PÁGINA 33

PÁGINA 34

PÁGINA 35

PÁGINA 36

PÁGINA 37

PÁGINA 38

PÁGINA 39

PÁGINA 40

PÁGINA 41

PÁGINA 42

PÁGINA 43

PÁGINA 44

PÁGINA 45

PÁGINA 46