UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN

FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

CARRERA PROFESIONAL DE INGENIERÍA DE SISTEMAS

"METODOLOGIA OCTAVE Y SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN DE LA UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN, HUÁNUCO, 2023"

LÍNEA DE INVESTIGACIÓN:

INGENIERÍA DE SISTEMAS

SUBLÍNEA DE INVESTIGACIÓN:

INGENIERÍA DE SISTEMAS Y COMUNICACIONES

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS.

TESISTA:

BACH. GALLARDO VALVERDE, FREDY

ASESORA:

DRA. RIVERA VIDAL DE SANCHEZ, HEIDY VELSY

HUÁNUCO - PERÚ

2024

Dedicatoria

Mi investigación está dedicada principalmente a Dios, a quien agradezco por darme la fuerza necesaria para completar este objetivo.

A mis padres por su amor incondicional y por ser mi mayor fuente de inspiración para lograr mis metas. El sacrificio que realizan diariamente es la luz que guía mi camino profesional.

A mis maestros, cuya guía experta orientación ha sido crucial en mi desarrollo profesional, les agradezco sinceramente por su paciencia, sabiduría y compromiso con mi crecimiento intelectual.

Este trabajo no solo refleja mi esfuerzo personal, sino también la valiosa contribución de quienes han creído en mí. A todos ustedes les dedico este logro con profundo gratitud. Celebramos juntos cada paso de este proyecto de tesis, sabiendo que los hemos logrado gracias a su apoyo.

Agradecimiento

En estas líneas, deseo expresar mi sincero agradecimiento a aquellos que desempeñaron un rol crucial en mi evolución como Ingeniero de Sistemas y en la finalización de mi tesis.

Quiero reconocer el invaluable aporte de la Dra. Heidy Velsy Rivera Vidal de Sanchez, mi asesora, cuya experta guía y dedicación han sido fundamentales para dar forma y orientación a este proyecto. Su respaldo, dirección y estímulo fueron elementos clave para alcanzar este hito en mi vida.

A mi familia, les doy gracias por su incansable apoyo y comprensión a lo largo del arduo proceso. Su amor y respaldo moral han sido la motivación que me impulsó a lograr este éxito académico.

Resumen

El objetivo de la investigación fue determinar la relación que existe entre la Metodología Octave y la seguridad de los sistemas de información de la Universidad Nacional Hermilio Valdizán, Huánuco, 2023. La metodología fue de tipo aplicada, nivel explicativo y diseño correlacional transversal. La muestra estuvo conformada por 91 administrativos de la UNHEVAL. Los resultados indicaron que el 84.6% casi nunca identifica activos de los sistemas de información; el 50.5% casi nunca clasifican los activos de los sistemas de información; el 50.5% casi nunca identifican los riesgos de los sistemas de información; el 83.5% casi nunca identifican las defensas de los sistemas de información; el 52.7% casi nunca realizan controles de acceso en el sistema de información; el 50.5% casi nunca realizan encriptaciones a la información; el 61.5% casi nunca realizan controles de cambios en el sistema de información; el 50.5% casi nunca validan la información mediante firmas digitales; el 51.6% casi nunca realizan una preparación en la gestión de incidentes; estos resultados indican que la seguridad de los sistemas de información no están implementadas adecuadamente; ello indica que existe una relación entre el uso de la metodología OCTAVE y la seguridad de los sistemas de información. La conclusión fue que, se determinó la relación que existe entre la Metodología Octave y la seguridad de los sistemas de información de la Universidad Nacional Hermilio Valdizán, Huánuco, 2023. Se obtuvo un coeficiente de correlación de 0,979, la cual indica que existe una relación positiva muy fuerte; además el sig. obtenido fue de 0.000 menor al error permitido de 0.05, la cual establece que la relación encontrada es significativa.

Palabras clave. Metodología Octave, seguridad de los sistemas de información y activos de los sistemas de información.

Abstract

The objective of the research was to determine the relationship between the Octave Methodology and the security of the information systems of the Hermilio Valdizán National University, Huánuco, 2023. The methodology was applied, explanatory level and cross-sectional correlational design. The sample consisted of 91 UNHEVAL administrators. The results indicated that 84.6% almost never identify information systems assets; 50.5% almost never classify information system assets; 50.5% almost never identify information systems risks; 83.5% almost never identify the defenses of information systems; 52.7% almost never perform access controls on the information system; 50.5% almost never encrypt information; 61.5% almost never perform change controls in the information system; 50.5% almost never validate information using digital signatures; 51.6% almost never prepare for incident management; These results indicate that the security of information systems is not adequately implemented; this indicates that there is a relationship between the use of the OCTAVE methodology and the security of information systems. The conclusion was that the relationship between the Octave Methodology and the security of the information systems of the Hermilio Valdizán National University, Huánuco, 2023, was determined. A correlation coefficient of 0.979 was obtained, which indicates that there is a very strong positive relationship; In addition, the GSI obtained was 0.000 lower than the allowed error of 0.05, which establishes that the relationship found is significant.

Keywords. Octave methodology, information systems security and information systems assets.

Índice

Introducción

La metodología OCTAVE desempeña un papel fundamental en la seguridad de los sistemas de información al proporcionar un enfoque estructurado y holístico para evaluar y gestionar los riesgos. Al centrarse en activos críticos y considerar amenazas tanto internas como externas, OCTAVE permite a las organizaciones identificar vulnerabilidades específicas y desarrollar estrategias de mitigación adaptadas a sus necesidades. Su enfoque participativo, orientado a la acción y adaptable a diversos contextos, facilita la colaboración de stakeholders clave y la implementación efectiva de medidas de seguridad. Además, OCTAVE promueve una cultura de concientización en seguridad al abordar prácticas inseguras y proporcionar directrices claras para la mejora continua. Por ello la investigación tiene como objetivo determinar la relación que existe entre la Metodología Octave y la seguridad de los sistemas de información de la Universidad Nacional Hermilio Valdizán, Huánuco, 2023. Para contestar el objetivo la investigación se dividió en 5 capítulos las cuales se dividen en:

El primer capítulo presenta la descripción del problema y se detalla la situación problémica tomando desde lo general a la especificación en la institución educativa, se presentan los objetivos, la justificación, limitaciones, las hipótesis y la definición operacional de variables.

En el segundo capítulo se presenta el marco teórico, se detalla los antecedentes que sirven de referencia para la ejecución de la investigación, se muestran bases teóricas, conceptuales y bases epistemológicas.

El tercer capítulo muestra la metodología aplicada en la investigación, donde especifica el ámbito de estudio, la población, muestra, nivel y tipo de investigación. Se describe el método, las técnicas y el instrumento aplicado, la forma como se validó los instrumentos, y el cálculo de confiabilidad.

El cuarto capítulo presenta los resultados obtenidos en la investigación, describiéndose las tablas y figuras que se generaron con los datos obtenidos. Asimismo, se contrastan las hipótesis.

En el quinto capítulo se realizó la discusión de resultados que permitió contrastar los resultados obtenidos con los antecedentes que sustentan la investigación.

Finalmente se presentan las conclusiones e inferencias como resultados que se relacionan con los objetivos planteados en la investigación; y se complementa con las sugerencias y conclusiones, las referencias bibliográficas y anexos.

CAPÍTULO I. PROBLEMA DE INVESTIGACIÓN

1.1 Fundamentación del problema de investigación

La seguridad en los sistemas de información es un aspecto crítico en la actualidad debido a la creciente dependencia de la tecnología y la información digital en diversas áreas de la sociedad. Arévalo et al. (2020) mencionan que en la actualidad, empresas e instituciones interactúan a través de dispositivos inteligentes, que permiten acceder a una gran variedad de información desde diversos indoles; por ello, es crucial mantener la seguridad de los sistemas de información, ya que cada vez son más frecuentes los robos de secretos empresariales, el pirateo de cuentas en redes sociales y los ciber robos en cuentas bancarias.

Hoy en día, la información manejada por instituciones son un activo muy valioso; no obstante, los sistemas donde se resguarda la información son vulnerables a multitud de riesgos. Así mismo, la información recolectada por las instituciones se ha convertido en la columna vertebral sobre la que se construyen sus objetivos. Gutiérrez (2022) indica que según el Informe sobre Riesgos Mundiales 2022 del Foro Económico Mundial, en diciembre de 2021 se descubrió una vulnerabilidad de seguridad crítica en un software muy utilizado. Según los datos, se detectaron más de 100 intentos de explotar la vulnerabilidad cada minuto, lo que ilustra la vulnerabilidad de los sistemas informáticos. Como consecuencia de la pandemia COVID 19, la ciberdelincuencia aumentó un 600%, desde el hurto y la malversación hasta la piratería informática y la corrupción de datos.

En el contexto mundial, el 78% de los ejecutivos de seguridad informática afirman que sus empresas no están adecuadamente protegidas frente a los ciberataques. El 90% o más de las instituciones han sufrido un ataque a su ciberseguridad en los últimos tres años. El 62,7% de las empresas achaca a la pandemia COVID-19 un aumento de los ciberataques a partir de 2020 (Gutiérrez, 2022).

En consecuencia, se llega a provocar la eliminación de documentos relevantes, así como compartir contraseñas y datos personales de la institución. Rubiano (2018) menciona que las mayores preocupaciones del sistema de información son que el

40,48% se debe a fraudes internos generando el 60,88% de pérdidas de datos. Afirma también que las repercusiones de las violaciones de datos pueden ser bastante caras. Por ello, el 86% de los directores generales afirman estar muy preocupados por los riesgos cibernéticos, incluida la insuficiente protección de datos.

La ineficiencia de las metodologías utilizadas actualmente para el cuidado de la información es una problemática relevante en el campo de la seguridad de la información; la mala elección de metodologías adecuadas vulnera la seguridad de la información de empresas e instituciones. Esteban y Pacienzia (2015) indica que muchas metodologías de seguridad se basan en enfoques tradicionales que no están al día con las últimas amenazas y técnicas de ataque utilizadas por los ciberdelincuentes.

Las instituciones a menudo utilizan una variedad de soluciones de seguridad independientes que no se integran bien entre sí. Esto conduce a una falta de visibilidad completa y cohesión en la estrategia de seguridad, lo que los atacantes pueden aprovechar para evadir medidas de seguridad. También los errores en los sistemas generan fallos en la seguridad de la información, como lentitud del software generando un ineficiente proceso de datos. Rubiano (2018) informa que el 47,54% de los errores en los sistemas de información se deben a las vulneraciones del software. Esta insuficiencia de administración de riesgos ocasiona grandes pérdidas a la institución.

No podemos dejar de lado al robo de información a las instituciones que son generadas por virus informáticos que atacan el sistema debido a que los antivirus están desactualizados. ¿Por qué tendríamos los antivirus desactualizados? La falta de compromiso de la gerencia institucional por disminuir gastos no destina los fondos suficientes al mantenimiento de los sistemas de seguridad de la institución. Como consecuencia se debilita la confianza en la institución, genera pérdidas informáticas hasta incluso económicas. Rubiano (2018) menciona que en Colombia el 55,52% de los fallos en los sistemas de seguridad se deben a los Malwares, que pueden descargarse junto con software legítimo y datos de sitios web pirateados. De este modo, los delincuentes pueden acceder a los dispositivos y robar información.

El gobierno peruano ha establecido como objetivo principal de su estrategia de ciberseguridad: proteger la privacidad, integridad, disponibilidad, legalidad y confiabilidad de la información; proteger la infraestructura de información, datos e información del Estado; y proteger la tecnología utilizada para procesar esta información de intrusiones maliciosas o accidentales.

Así mismo, el Perú se mantiene entre los países que registran más incidencias en la vulneración de información y venta de información personal por parte de los ciber delincuentes. Terrell (2022) indica que aproximadamente 42 millones de ciudadanos fueron víctimas de fraude de identidad en el 2021, lo que les costó a los consumidores $52,000 millones en pérdidas totales.

García y Huamani (2019) en su investigación sobre la Evolución de la gestión de ciber riesgo y Seguridad de la información, encontró que 4 de cada 10 instituciones han sufrido una brecha de seguridad en los últimos 24 meses, refiriéndose al 2016 y menos del 1% cuenta con indicadores que evalúen la gestión de ciber riesgos y de seguridad de la información. La pérdida de información en su mayoría se debe a la mala manipulación humana de los sistemas de información que pueden compartir contraseñas y otros datos personales de la institución o hasta la eliminación de información.

El robo de información en las instituciones, en su mayoría se deben a los fallos informáticos ocasionados por la infección de virus que ingresan por descargas piratas que se realicen además del antivirus desactualizado, generando desconfianza de las instituciones respecto al manejo de información. Inoguchi y Macha (2017) afirman que el desconocimiento de la noción de seguridad de la información y de los niveles de confidencialidad, integridad y disponibilidad de la información que se maneja son las principales amenazas que influyen en la seguridad de la información de una institución. Registró que el 80% del personal en una institución manifestó que carecen de herramientas que aseguren la información digital de la institución.

En la región de Huánuco las instituciones no son ajenas a los problemas de seguridad de información por la mala manipulación humana que son producto de la

inexperiencia por parte de los operadores informáticos; errores en los sistemas de información producto de los fallos del sistema operativo interno, lentitud de procesamiento del software e incluso el robo de información producto de la infección de virus que debilita la seguridad y confiabilidad de la institución generando pérdidas informáticas o inclusive económicas. En tal sentido Villadeza y Condor (2022) mencionan que, en Huánuco en el distrito de Huácar, la seguridad informática se encuentra en un 2%, inconclusa y con falta de predisposición de los encargados en terminar los requisitos de seguridad en sus instituciones.

En tal sentido se propone emplear la Tecnología Octave para cubrir los riesgos de seguridad informática en las instituciones, en este caso en la Universidad Nacional Hermilio Valdizán.

1.2 Formulación del problema de investigación general y específicos

1.2.1 Problema general

¿Cuál es la relación entre la Metodología Octave y la seguridad de los sistemas de información de la Universidad Nacional Hermilio Valdizán, Huánuco, 2023?

1.2.2 Problemas específicos

- ¿De qué manera se establecerán los requerimientos de seguridad con la metodología Octave y su relación con la seguridad de los sistemas de información de la UNHEVAL, Huánuco, 2023?
- ¿De qué manera se identificará las vulnerabilidades de la infraestructura con la metodología Octave y su relación con la seguridad de los sistemas de información de la UNHEVAL, Huánuco, 2023?
- ¿De qué manera se establecerá un plan y estrategia de mejora para la seguridad de los sistemas de información de la UNHEVAL, Huánuco, 2023?

1.3 Formulación de objetivos generales y específicos

1.3.1 Objetivo general

Determinar la relación que existe entre la Metodología Octave y la seguridad de los sistemas de información de la Universidad Nacional Hermilio Valdizán, Huánuco, 2023.

1.3.2 Objetivos específicos

- Establecer los requerimientos de seguridad con la metodología Octave y su relación con la seguridad de los sistemas de información de la UNHEVAL, Huánuco, 2023.
- Identificar las vulnerabilidades de la infraestructura con la metodología Octave y su relación con la seguridad de los sistemas de información de la UNHEVAL, Huánuco, 2023.
- Establecer un plan y estrategia de mejora para la seguridad de los sistemas de información de la UNHEVAL, Huánuco, 2023.

1.4 Justificación

Justificación práctica: Porque los resultados permitirán evidenciar la forma que se viene aplicando la metodología Octave en favor de la seguridad de los sistemas, en lo cual se establecerá un plan de mejora mediante la metodología Octave, esto servirá de aporte a los administrativos de la Universidad Hermilio Valdizán, para corregir puntos débiles de seguridad, restablecer y mejorar algunos procesos en la seguridad de los sistemas, ya que, la metodología Octave es altamente adaptable y puede personalizarse para satisfacer las necesidades y características específicas de seguridad. Esto es crucial en un entorno donde las amenazas y los riesgos varían ampliamente según la ubicación y otros factores.

Justificación metodológica: Porque la metodología abordará un nivel descriptivo correlacional de tipo básica y diseño no experimental correlacional transversal, además, mediante el empleo del método científico, la técnica encuesta e

instrumento cuestionario, que será dirigido a una muestra representativa de 91 administrativos permitirá direccionar la recolección de datos para hallar los resultados, que serán de vital importancia para responder las incógnitas del problema y alcanzar el objetivo de determinar la relación que existe entre la Metodología Octave y la seguridad de los sistemas de información de la Universidad Nacional Hermilio Valdizán, Huánuco.

Justificación teórica: Porque las teorías y definiciones abordadas en el estudio son de fuentes confiables y de periodos actuales, es por ello que las definiciones establecidas en el estudio servirán para incrementar o reforzar los conocimientos respecto a la metodología Octave, lo cual se basa en la identificación y gestión de riesgos y la variable sistemas de seguridad, los cuales están inmersos a las amenazas y riesgos, siendo los principales beneficiarios los administrativos que se relacionan con los sistemas de información de la UNHEVAL, ya que al estar informados, existe la predisposición de aplicar la metodología Octave como medio de prevención para disminuir los riesgos y amenazas de los sistemas de información.

1.5 Limitaciones

La investigación presente se limita por los siguientes aspectos:

a) La investigación se realizará con los con los propios recursos económicos del investigador.
b) La accesibilidad de cierta información en la seguridad de información es limitada.
c) El personal administrativo no cuenta con el conocimiento sobre la seguridad de la información.
d) La disponibilidad de tiempo para la recolección datos es limitada por la el trabajo.

1.6 Formulación de hipótesis generales y específicas

2.1.1 Hipótesis general

Hi: Existe relación estadísticamente significativa entre la Metodología Octave y la seguridad de los Sistemas de Información de la Universidad Nacional Hermilio Valdizán, Huánuco, 2023.

Ho: No existe relación estadísticamente significativa entre la Metodología Octave y la seguridad de los Sistemas de Información de la Universidad Nacional Hermilio Valdizán, Huánuco, 2023.

2.1.2 Hipótesis específicas

Hi1: Los requerimientos de seguridad con la metodología Octave se relacionan significativamente con la seguridad de los sistemas de información de la UNHEVAL, Huánuco, 2023.

Ho1: Los requerimientos de seguridad con la metodología Octave no se relacionan significativamente con la seguridad de los sistemas de información de la UNHEVAL, Huánuco, 2023.

Hi2: La identificación de las vulnerabilidades de la infraestructura con la metodología Octave se relacionan significativamente con la seguridad de los sistemas de información de la UNHEVAL, Huánuco, 2023.

Ho2: La identificación de las vulnerabilidades de la infraestructura con la metodología Octave no se relacionan significativamente con la seguridad de los sistemas de información de la UNHEVAL, Huánuco, 2023.

Hi3: El establecimiento de un plan y estrategia mejora significativamente la seguridad de los sistemas de información de la UNHEVAL, Huánuco, 2023.

Ho3: El establecimiento de un plan y estrategia no mejora significativamente la seguridad de los sistemas de información de la UNHEVAL, Huánuco, 2023.

1.7 Variables

2.2.1 Variable 1

Metodología Octave

2.2.2 Variable 2

Seguridad de los sistemas de información

1.8 Definición teórica y operacionalización de variables

VARIABLES	DEFINICIÓN TEÓRICA	DEFINICIÓN OPERACIONAL	DIMENSIONES	INDICADORES	INSTRUMENTO
Metodología Octave	Es un enfoque estructurado y sistemático diseñado para evaluar y mejorar la seguridad de los sistemas de información en organizaciones (Pacheco et al., 2021).	Se desarrolla en 3 fases, en los cuales se identifica activos críticos, amenazas y vulnerabilidades asociadas a los activos, y la formulación de estrategias para mitigar los riesgos.	Requerimientos de seguridad	Identificación de activos	Cuestionario
				Clasificación de activos	
				Identificación de riesgos	
				Identificación de defensas	
				Necesidades de seguridad	
			Vulnerabilidades de la infraestructura	Identificación de vulnerabilidades	
				Evaluación de vulnerabilidades	
				Análisis de vulnerabilidades	
				Priorización de atención de vulnerabilidades	
			Plan y estrategia de seguridad	Identificación de riesgos de información.	
				Control de seguridad	

				Integración de los controles	
Seguridad de los Sistemas de Información	Se refiere a la práctica de proteger la información y los sistemas informáticos contra amenazas y riesgos con el objetivo de garantizar su confidencialidad, integridad y disponibilidad para lo cual se emplea una gestión de incidentes y vulnerabilidades; siguiendo normas legales que regulan los procedimientos en la seguridad de los sistemas (Martinez, 2020).	Abarca una amplia gama de medidas técnicas, administrativas y físicas diseñadas para minimizar los riesgos y asegurar que la información esté protegida de manera adecuada.	Confidencialidad e integridad	Control de acceso	Cuestionario
				Encriptación	
				Control de cambios	
				Firmas digitales	
			Gestión de incidentes	Preparación	
				Análisis y detección	
				Contención, erradicación y recuperación	
				Actividades después de incidentes	
			Gestión de vulnerabilidades	Escaneo de vulnerabilidades	
				Parches y actualizaciones	
			Cumplimiento legal y regulatorio	Evaluación y conformidad	
				Auditorías y revisiones externas	

CAPÍTULO II. MARCO TEÓRICO

2.1 Antecedentes

2.1.1 Antecedentes internacionales

Rodríguez (2023) en su investigación titulada *"Propuesta de un modelo de mejora continua para la gestión de riesgos de la seguridad de la información a una institución educativa privada mediante el ciclo CAP-DO"*, para optar el título profesional de Ingeniero en Tecnología de la Información en la Universidad Estatal Península de Santa Elena. Planteó como objetivo general: "Realizar un análisis de riesgos mediante un estudio comparativo para gestionar la toma de decisiones de políticas de seguridad de la información en una institución educativa privada". La metodología empleada fue de tipo cuantitativo, nivel exploratorio, diseño pre experimental. La población muestral fue de 688 beneficiarios. Las técnicas empleadas fueron la observación y la entrevista, como instrumento la guía de observación y el cuestionario. El autor concluyó que, las mejores prácticas en materia de seguridad de la información se identificaron a través de la investigación sobre marcos de gestión de riesgos, entre ellos ISO 31000:2018, CRAMM, Magerit y OCTAVE. Esto nos permitió examinar las similitudes y diferencias entre los marcos de los distintos enfoques e inspirarnos en diversas fuentes para los principios rectores de la propuesta. Era necesario gestionar las decisiones en materia de política de seguridad de la información en una escuela privada, por lo que se elaboró una guía de análisis de riesgos mediante una investigación comparativa. Empezando por la identificación y valoración de los activos, esta guía avanza hacia un examen exhaustivo de los indicadores de riesgo. Como resultado, la institución pudo identificar las amenazas, vulnerabilidades y peligros específicos a los que estaban expuestos sus activos de información, y tomar las medidas oportunas.

Barraza (2021) en su investigación titulada "*Sistema de gestión de la seguridad de la información en las pequeñas y medianas empresas",* para optar el título profesional de Ingeniero de Sistemas en la Universidad de Cartagena. Planteó como objetivo general: "Eliminar, o al menos reducir los inconvenientes y ayudar a las

PYMES a evaluar los riesgos a los que sus activos están expuestos, y a establecer los controles de seguridad adecuados con los estándares de seguridad aprobados internacionalmente". La metodología empleada fue de tipo aplicada, nivel explicativo, diseño cuasi experimental. La técnica empleada fue la entrevista y como instrumento el cuestionario. El autor concluyó que: Cuando las empresas disponen de sistemas eficaces de gestión de la seguridad de la información, pueden proteger mejor sus activos. Muchas empresas, sobre todo las más pequeñas, carecen de uno. Dado que más del 90% de las empresas colombianas son pymes y deben garantizar que sus activos estén lo más seguros posible, es crucial que los especialistas en seguridad informática del país estén familiarizados con este enfoque o uno similar.

Guerra (2020) en su tesis titulada *"Sistema de gestión para la seguridad de la información basado en metodología de identificación y análisis de riesgo en la Biblioteca de la Universidad de la Costa"*, para optar el grado académico de Maestro en Gestión Tecnológica de la Información y Comunicación en la Universidad de la Costa. Planteó como objetivo general: "Desarrollar un SGSI basado en una metodología de identificación y análisis de riesgos para los procesos de la biblioteca de la Universidad de la Costa (CUC)". La metodología empleada fue de tipo cualitativa, nivel explicativo, diseño pre experimental. La técnica empleada fue la revisión bibliográfica. El autor concluyó que: Con el paso del tiempo, el Sistema de Gestión de la Calidad se ha convertido en una herramienta para la certificación internacional y la organización de procesos con el objetivo de planificar, controlar y mejorar dichas operaciones. Para cada riesgo identificado, el enfoque afirma que ni las amenazas ni las vulnerabilidades han sido detectadas por el sistema de gestión de la calidad. También debe evaluarse la gravedad de las consecuencias en función de los riesgos. Sin embargo, el SGC existente revela una falta de protecciones para cada peligro y vulnerabilidad identificados, por lo que las medidas para disminuir o mitigar los riesgos tienen un alcance bastante amplio.

Álvarez y Silva (2019) en su tesis titulada *"Auditoría Informática aplicando la metodología OCTAVE de los procesos de recaudaciones y permisos en el Gobierno Autónomo Descentralizado (GAD) de San Pedro de Pelileo"*, tuvo como objetivo

general realizar una Auditoría Informática de procesos de recaudaciones y permisos en el Gobierno Autónomo Descentralizado de San Pedro de Pelileo aplicando la metodología OCTAVE. La metodología fue de tipo aplicada, nivel explicativo y diseño experimental. La técnica fue la encuesta e instrumento el cuestionario. Las conclusiones fueron: La aplicación de la Auditoria Informática bajo la metodología OCTAVE fue de gran utilidad, ya que permitió enfocarse en los activos de información que intervenían en los procesos, contemplando varios escenarios de amenazas y así tener un mayor alcance en la identificación e evaluación de los riesgos. Las instalaciones físicas no cuentan con seguridad de registro de acceso al lugar o cámaras de vigilancia, lo que pone en riesgo a departamento tecnológico donde se encuentra el centro de procesamiento de datos. Al realizar la auditoria se identificó que el GAD municipal actualmente utiliza una versión de prueba de Oracle lo que limita funciones y espacio de almacenamiento, que en un futuro sería necesario por la cantidad de información que se maneja en la entidad. Al realizar la mitigación de riesgos se procedió a dar recomendaciones entre ellas los controles que se deben realizar para evitar que un riesgo se materialice, siempre contemplando que vaya encaminado a tener una mayor seguridad e integridad de la información.

2.1.2 Antecedentes nacionales

Campos y León (2020) en su trabajo de investigación titulado *"Comparativa de las metodologías Magerit y Octave, para determinar la más adecuada en la gestión de riesgos de tecnologías de información en la Unidad de Red Telemática de la Universidad Nacional Pedro Ruiz Gallo"* para optar el título profesional de Ingeniero de sistemas en la Universidad Nacional Pedro Ruiz Gallo. Planteó el siguiente objetivo general: "Desarrollar una evaluación comparativa de las metodologías MAGERIT y OCTAVE, para determinar el nivel de adecuación de cada una de ellas al proceso de gestión de riesgos de TI en la Unidad de Red Telemática de la Universidad Nacional Pedro Ruiz Gallo". La metodología empleada fue de tipo cuantitativa, nivel explicativo, diseño cuasi experimental. La técnica utilizada fue la entrevista y como instrumento el cuestionario. El autor concluye que: La técnica OCTAVE adopta un enfoque de nivel corporativo para su proceso, que evalúa las numerosas Fases, Procedimientos y Actividades que componen un Sistema de Gestión de Riesgos

Informáticos. La primera etapa, "construcción del perfil de amenazas basado en los activos", implica establecer criterios de evaluación del impacto, identificar los activos de la organización y evaluar las prácticas de seguridad de la organización, entre otras cosas; y seleccionar los activos críticos, identificar los requisitos de seguridad para los activos críticos e identificar las amenazas a los activos críticos, entre otras cosas, para crear el perfil de amenazas. En la segunda fase, se buscarán puntos débiles en la infraestructura informática, revisando las operaciones relacionadas con la tecnología y estudiando las vías de acceso a los recursos críticos. En la tercera y última etapa, desarrollará estrategias y planes de seguridad, incluyendo pasos como: identificar y analizar los riesgos mediante acciones como: determinar la gravedad de las amenazas; crear criterios para evaluar la probabilidad de eventos adversos; y sopesar los riesgos relativos de varios escenarios. Planifique los peligros potenciales mediante acciones como la descripción de su estrategia de protección actual y la elección de métodos de mitigación.

Llauce (2022) en su tesis titulada *"Análisis comparativo de metodologías de gestión de riesgos de tecnologías de la Información en el marco de la NTP - ISO/IEC 27001:2014"*, para optar el grado académico de Maestro en Ingeniería de Sistemas con mención en Gerencia de Tecnologías de la Información de la Universidad Nacional Pedro Ruiz Gallo. Planteó el siguiente objetivo general: "Realizar un estudio analítico y crítico desde el punto de vista de la gestión de riesgos de tecnologías de la información en el marco de la NTP - ISO/IEC 27001:2014". La metodología empleada fue de tipo aplicado, nivel descriptivo, diseño cuasi experimental. Las técnicas empleadas fueron la observación y la entrevista, para los instrumentos se empleó la guía de observación y el cuestionario. El autor concluye que: Se encontró que la metodología Magerit V3 es la más similar a la Norma Técnica Peruana NTP-ISO/IEC 27001:2014, con un puntaje de similitud de 96%; en este sentido, se descubrió que esta metodología tiene un alto grado de similitud con los aspectos y características definidos en la NTPISO/IEC 27001: 2014 vinculados a la gestión de riesgos, de tal manera que se reduce la incertidumbre en la selección de la metodología a utilizar en la implementación de la norma.

Segura (2022) en su tesis titulada *"Diseño de un sistema de gestión de seguridad de la información: Caso de estudio Universidad Nacional Intercultural Fabiola Salazar Leguía"*, para optar el título profesional de Ingeniero de Sistemas de la Universidad Señor de Sipán. Planteó el siguiente objetivo general: "Diseñar una propuesta de un Sistema de Gestión de Seguridad de la información para la Universidad Nacional Intercultural Fabiola Salazar Leguía". La metodología empleada fue de tipo cuantitativo, nivel explicativo, diseño cuasi experimental. La técnica utilizada fue la entrevista y la observación, para el instrumento se usó el cuestionario y la guía de observación. El autor concluyó que: A través de las directrices de esta norma internacional de seguridad de la información ISO/IEC 27001, y con el apoyo de las directrices de COBIT 5, ITIL, y PMBOK, se considera que son herramientas de gran beneficio en la toma de decisiones necesarias para implantar y constituir un modelo de seguridad de la información. Una de las ventajas fundamentales que plantea es que las directrices se pueden adaptar a metodologías de evaluación de análisis de riesgos.

Villaverde (2021) en su tesis titulada *"Implementación de una gestión de riesgos de TI para mejorar la seguridad de la información de una empresa de agencia publicitaria - 2021"*, tuvo como objetivo general implementar una gestión de riesgo de TI para mejorar la seguridad de la información en una empresa de agencia publicitaria. La metodología fue de tipo aplicada, nivel explicativo y diseño experimental. La técnica fue la encuesta e instrumento el cuestionario. Las conclusiones fueron: La Empresa de Agencia Publicitaria no tenía un inventario de activos posteriormente luego de aplicar la metodología Octave se identificó los activos y se realizó una valoración de los activos. La empresa de Agencia Publicitaria al implementar la metodología Octave pudo identificar los riesgos que estaban expuestos los activos y posteriormente se realizó una valoración de los riesgos. La empresa de Agencia Publicitaria al implementar la metodología Octave estableció planes de acción y controles que no tenían identificados, con el fin de mitigar los riesgos.

2.1.3 Antecedentes locales

Villadeza y Condor (2022) en su trabajo de investigación titulado *"Diseño de un sistema de gestión de seguridad de la información basado en la norma técnica peruana -ISO/IEC 27001:2014 para la Municipalidad Distrital de Huácar 2022"*, para optar el título profesional de Ingeniero de Sistemas en la Universidad Nacional Hermilio Valdizán. Planteó como objetivo general: "Proponer el diseño de un Sistema de Gestión de Seguridad de la Información basado en la NTP ISO/IEC 27001:2014, para mejorar la seguridad de la información de la Municipalidad Distrital de Huácar 2022". La metodología empleada fue de tipo aplicada, nivel explicativo, diseño no experimental. La población muestral fue constituida por 47 personas. La técnica empleada fue la observación y como instrumento la guía de observación. Los autores concluyeron que: El uso de la metodología MAGERIT para el análisis y gestión de riesgos en su versión 3 permitió observar los peligros internos y externos a los que está sometida la municipalidad, así como sus efectos y peligros asociados. La investigación determinó que la municipalidad del distrito de Huácar había alcanzado un nivel intolerable, ya que la mayoría de sus activos estaban fuera de la tolerancia al riesgo.

Abanto y Rivera (2022) en su trabajo de investigación titulado *"Propuesta de un modelo de sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 para la Sede Central del Gobierno Regional de Huánuco – 2022"* para optar el título profesional de Ingeniero de Sistemas en la Universidad Nacional Hermilio Valdizán. Planteó el siguiente objetivo general: "Proponer un modelo de sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 para mejorar la seguridad de la información en la sede central del Gobierno Regional de Huánuco, 2022". La metodología empleada fue de tipo aplicado, nivel explicativo, diseño cuasi experimental. La población fue constituida por 5000 activos físicos y 200 funcionarios públicos. La muestra fue de 1000 activos físicos y 74 funcionarios públicos. La técnica empleada fue la entrevista y como instrumento el cuestionario. Los autores concluyeron que: La situación actual de GOREHCO, donde la institución entendía la importancia y el alcance de un SGSI pero no había establecido estrategias ni metodología alguna para la evaluación de riesgos,

llevó al desarrollo de un modelo de SGSI basado en la NTP ISO/IEC 27001:2014, donde se potencia la gestión de riesgos con sus respectivos controles según la norma. Los valores de los activos se calcularon utilizando medidas relacionadas con la seguridad tanto física como digital.

Rivera y Valdivia (2021) en su tesis titulada *"Implementación de la metodología Octave para mejorar la gestión de riesgos de Seguridad de la Información y propuesta de políticas de seguridad en la Dirección Regional de Trabajo y Promoción del Empleo"*, tuvo como objetivo general implementar la metodología Octave y la Norma Técnica Peruana ISO 27001-2014 para mejorar la gestión de riesgos de la seguridad de la información en la DRTPE-Hco – 2021. La metodología fue tipo aplicada, nivel explicativo y diseño experimental. La técnica fue la encuesta i instrumento el cuestionario: Las conclusiones fueron: La identificación de las amenazas a los que están expuestos los activos informáticos permite estimar el alcance del daño de la seguridad de la información en la DRTPE-Hco, debido a una mejora en la reducción de Probabilidad de ocurrencia de las amenazas, de los activos informáticos. La verificación del nivel de cumplimiento de las salvaguardas reduce el nivel de impacto de los activos informáticos en la DRTPE-Hco 2021, debido a un incremento de las salvaguardas implantadas actualmente en los activos informáticos de 9% a 33%, por consiguiente, se puede establecer, que, al haber más activos con salvaguardas establecidas, se obtendrá una mejor reducción del nivel de impacto de los activos.

2.2 Bases teóricas

2.2.1 Metodología Octave

La metodología Octave, creado por el Instituto de Ingeniería de Software (SEI) de Estados Unidos, es un enfoque de la evaluación de riesgos basado en procesos y actividades que consta de tres partes y cuyo objetivo es ofrecer una imagen completa de los requisitos de seguridad de una organización abordando tanto los riesgos operativos como las prácticas de seguridad. En resumen, es un enfoque estructurado y

sistemático diseñado para evaluar y mejorar la seguridad de los sistemas de información en organizaciones (Pacheco et al., 2021).

Desde la publicación inicial del enfoque en 2000, el SEI ha distribuido numerosas actualizaciones. Los formularios más comunes ahora disponibles son:

OCTAVE 2.0.: Las empresas con más de 300 personas, infraestructura propia, estructura jerárquica y capacidad para ejecutar herramientas de detección de vulnerabilidades y comprender sus hallazgos son las que más se beneficiarían de esta edición. Para alcanzar los objetivos estratégicos, tácticos y operativos, esta versión define los procesos, reglas, catálogos y formación que se utilizarán en los distintos niveles de la organización. Para identificar las amenazas, vulnerabilidades y riesgos y diseñar una estrategia de mitigación eficaz, esta última parte también abarca la tecnología que soporta los activos que hay que vigilar. Los talleres sirven de base para el proceso de recopilación de información (Pacheco et al., 2021).

OCTAVE – S: Está diseñado para empresas con menos de 100 trabajadores. Está estructurado en tres actos, muy parecido al OCTAVE original. Sin embargo, los talleres no se utilizan como base para la recopilación de datos. Se espera que el equipo que aplica la técnica esté familiarizado con los activos de la organización, las necesidades de seguridad, las amenazas y los procedimientos generales de seguridad (Pacheco et al., 2021).

OCTAVE Allergo: Está diseñado para equipos que necesitan información exhaustiva sobre todos los recursos de una organización, pero que no desean incluir a toda la empresa en una evaluación de riesgos (Pacheco et al., 2021).

OCTAVE FORTE: Esta nueva versión de OCTAVE está pensada para utilizarse como marco de gestión de los riesgos operativos en toda la empresa. Adopta una visión amplia del riesgo y garantiza que las ciber amenazas se evalúen y controlen del mismo modo que el resto de peligros de una organización (Pacheco et al., 2021).

El SEI ha creado una técnica llamada OCTAVE para proporcionar una evaluación exhaustiva de los requisitos de seguridad de una empresa a través de una

amplia gama de riesgos operativos y prácticas de seguridad. Resulta ventajoso ya que un pequeño equipo puede llevarlo a cabo, recopilando datos de varios departamentos para proporcionar una imagen completa de los riesgos de la empresa en todos los ámbitos (estratégico, táctico, operativo y tecnológico). Esto aclara la función prevista de OCTAVE, ya que todos sus componentes encajan para formar el conjunto. Existe un posible inconveniente, ya que para calcular un efecto global se utiliza una matriz de valores de riesgo (alto, medio y bajo) y sus probabilidades asociadas. Sin un valor monetario, es imposible saber si merece la pena o no invertir en técnicas de gestión y mitigación (Hurtado, 2021).

Según, Pacheco et al. (2021) la metodología Octave como técnica de evaluación de riegos se ejecuta en 3 fases, además se subdivide en 8 procesos:

- **Primera fase:** Establecer requerimientos de seguridad a nivel de la organización. Esta fase se subdivide en 4 procesos:

  - Proceso 1: Identificar el conocimiento empresarial
  - Proceso 2: Identificar el conocimiento de las áreas operativas
  - Proceso 3: Identificar el conocimiento del personal
  - Proceso 4: Establecer los requerimientos de seguridad

- **Segunda fase:** Identificar vulnerabilidades de la infraestructura. Esta fase se subdivide en 2 procesos:

  - Proceso 5: Mapeo de los activos de alta prioridad sobre la infraestructura que los soporta
  - Proceso 6: Ejecutar una evaluación de vulnerabilidades en la infraestructura

- **Tercera fase:** Desarrollar un plan y una estrategia de seguridad. Esta fase se subdivide en 2 procesos:

  - Proceso 7: Conducir un análisis de riesgo multidimensional
  - Proceso 8: Desarrollar una estrategia de protección

2.2.1.1 Primera fase: Establecer requerimientos de seguridad a nivel de la organización.

Según, Pacheco et al. (2021) durante esta fase, la organización se somete a examen mediante el acercamiento y la adquisición de información de las personas empleadas dentro de la empresa. Las personas de los distintos niveles jerárquicos de la empresa interactúan con el objetivo principal de aportar sus conocimientos, experiencia y distintas perspectivas a la empresa.

Para Hurtado (2021) en este punto, se realiza una aproximación a la organización y se recaba información de sus empleados. Se habla con personas de toda la empresa y se espera que aporten su experiencia, sus ideas y sus puntos de vista.

Proceso 1: Identificar el conocimiento empresarial

En el primer proceso OCTAVE especifica las acciones que la alta dirección utiliza para identificar los activos, riesgos y defensas más críticos de la organización. Para recopilar datos que ayuden a crear todos los procesos de la metodología, es crucial que el equipo que dirige los talleres conozca a fondo los activos que se van a valorar (López y Vásquez, 2016).

Además, según Pacheco et al. (2021) los talleres deben prepararse bien antes de invitar a los altos cargos, ya que OCTAVE se limita a dar recomendaciones sobre cómo realizarlos. Así pues, la capacidad de los talleres para responder a las siguientes preguntas es crucial:

a. Activos de información más importantes en el área a evaluar.
b. Requerimientos de seguridad asociados a los activos de información.
c. Vulnerabilidades asociadas a los activos de información.
d. Amenazas existentes asociadas a los activos de información.
e. Políticas de protección existentes.

Las personas que realizan la evaluación en esta fase tienen un conocimiento más profundo de los activos, ya que los supervisan de forma continua. Así se obtiene

un análisis en profundidad de los activos, las brechas de seguridad y las posibles lagunas en las operaciones y procedimientos del sistema (López y Vásquez, 2016).

Pero OCTAVE allegro puede utilizarse para complementar la metodología, ya que proporciona una hoja de trabajo de áreas de preocupación en la que se detallan amenazas, vulnerabilidades y riesgos, y también ilustra un árbol de amenazas que resulta muy útil para identificar de forma clara y rápida las amenazas a los activos de información (López y Vásquez, 2016).

Proceso 2: Identificar el conocimiento de las áreas operativas

Definir las actividades para identificar la perspectiva de las áreas operativas con respecto a los activos más significativos, las amenazas y las técnicas de protección accesibles para la empresa; este es el segundo paso del proceso OCTAVE (Torres y Rojas, 2017).

Además, según Pacheco et al. (2021) el proceso 2 investiga las mismas cuestiones que el proceso 1, pero tiene en cuenta las dimensiones tácticas de la organización en su búsqueda de respuestas. Las respuestas a las siguientes preguntas deben proceder de los Talleres:

a. Activos de información más importantes en el área a evaluar.
b. Requerimientos de seguridad asociados a los activos de información.
c. Vulnerabilidades asociadas a los activos de información.
d. Amenazas existentes asociadas a los activos de información.
e. Políticas de protección existentes.

En este escenario, la información procede de la dirección de operaciones, que comparte los conocimientos adquiridos mediante la interacción con clientes internos y externos y la identificación de áreas de preocupación, muchas de las cuales están relacionadas con accidentes pasados. Al igual que en el paso 1, la experiencia del equipo encargado del taller es crucial para guiar a los participantes en la elaboración

de estos requisitos y destacar su experiencia particular con respecto a los activos del taller (Torres y Rojas, 2017).

Proceso 3: Identificar el conocimiento del personal

El tercer proceso OCTAVE, identificar el conocimiento del personal, define las actividades para conocer la perspectiva de las personas que trabajan directamente con estos activos o indirectamente, por ejemplo, en las áreas de apoyo, con el fin de identificar los activos, amenazas y estrategias de protección más importantes de que dispone la organización (Fuentes et al., 2018).

Además, según Pacheco et al. (2021) la tercera fase pretende dar respuesta a las mismas preguntas que las dos primeras, pero esta vez desde el punto de vista de quienes interactúan a diario con el área objeto de revisión, como el equipo informático, el de marketing, el de proyectos, etc. Las respuestas a las siguientes preguntas deben proceder de los Talleres:

a. Activos de información más importantes en el área a evaluar.
b. Requerimientos de seguridad asociados a los activos de información.
c. Vulnerabilidades asociadas a los activos de información.
d. Amenazas existentes asociadas a los activos de información.
e. Políticas de protección existentes.

Las personas que realizan la evaluación en esta fase tienen un conocimiento más profundo de los activos, ya que los supervisan de forma continua. Así se obtiene un análisis en profundidad de los activos, las brechas de seguridad y las posibles lagunas en las operaciones y procedimientos del sistema (Fuentes et al., 2018).

Proceso 4: Establecer los requerimientos de seguridad

Los conocimientos adquiridos en los tres primeros pasos de OCTAVE se utilizan como base para el cuarto paso, que consiste en establecer las necesidades de seguridad. Se reúnen y analizan conjuntamente las amenazas, las operaciones de protección, los indicadores de riesgo y los activos, y a continuación se establecen las

necesidades de seguridad para los activos identificados (Pacheco, Suarez, & Gonzáles, 2021).

Este procedimiento arroja datos suficientes para servir de base a la formulación del plan de seguridad de la empresa. El propósito de este paso es consolidar la información recopilada hasta el momento en una imagen cohesionada de los activos de la organización, las amenazas y los indicadores de riesgo en los que basar un plan de seguridad integral (Díaz, 2018).

2.2.1.2 Segunda fase: Identificar vulnerabilidades de la infraestructura

Según, Pacheco et al. (2021) la fase actual de OCTAVE aprovecha los datos recogidos en las actividades de la fase 1 precedente. Basándose en la información proporcionada, el objetivo principal es determinar los elementos más críticos de la infraestructura, incluidos los componentes tanto físicos como informáticos. El objetivo de esta evaluación es identificar las vulnerabilidades de estos componentes, lo que conduce posteriormente a una evaluación y análisis de la exposición al riesgo asociado para los activos de la organización que dependen de dichos componentes. El objetivo principal de la fase 2 es determinar la ausencia de normas y procesos, así como identificar los componentes de la infraestructura susceptibles de presentar vulnerabilidades para darle prioridad.

Proceso 5: Consiste en identificar los componentes más críticos de la infraestructura de apoyo para los activos de alta prioridad, en función de los activos y amenazas descubiertos en la primera fase. Tanto los sistemas de soporte digitales como físicos se incluyen en el concepto más amplio de infraestructura de la información. El objetivo principal de este procedimiento es determinar qué partes de la infraestructura son las más importantes para analizarlas en profundidad y determinar si son vulnerables o no (Fuentes et al., 2018).

La participación y los conocimientos de los profesionales de la Tecnología de la Información (TI) son cruciales en el paso 5, que consiste en recopilar información sobre:

a) Ubicación física de los activos de información.

b) Rutas de acceso de los activos de información.

c) Arquitectura de red de los activos de información.

d) Flujos de los activos de información.

Proceso 6: Se basa en estos datos para llevar a cabo un examen exhaustivo de los activos de información y la infraestructura de apoyo con el fin de descubrir cualquier fallo (Pacheco et al., 2021).

Además, para llevar a cabo una evaluación de la vulnerabilidad de la infraestructura se especifica los pasos que deben darse para evaluar la seguridad de las partes de la Tecnología de la Información en el paso 5. Además de los activos estudiados y los servicios que los acompañan, estas partes también comprenden infraestructuras de terceros. El objetivo principal es determinar los puntos débiles de la infraestructura actual y descubrir las políticas y procesos que faltan o no se ejecutan adecuadamente (Pacheco et al., 2021).

Los siguientes pasos sirven para identificar posibles puntos débiles en la infraestructura:

a) Identificar políticas y prácticas existentes.

b) Verificar si existen escenarios de intrusión para ser evaluados.

c) Identificar ausencia de políticas y prácticas existentes.

2.2.1.3 Tercera fase: Desarrollar un plan y una estrategia de seguridad

Según Pacheco et al. (2021) en la tercera fase de OCTAVE, se ejecuta la determinación de la estrategia de gestión de riesgos de seguridad, se analizan los datos sobre amenazas y vulnerabilidades de los activos en el contexto de escenarios de intrusión para evaluar la exposición de la empresa a cada escenario y clasificarlos por orden de gravedad. En esta tercera fase, nos centraremos en señalar las amenazas más acuciantes para la banca electrónica y en formular un plan para contrarrestarlas.

Proceso 7: Determinar las acciones para identificar y controlar los riesgos en la organización relacionados con la banca virtual mediante la realización de un análisis

de riesgos multidimensional. Los riesgos se definen en este contexto en función de la familiaridad del equipo con los posibles escenarios de intrusión, los activos expuestos, el impacto en el negocio, las amenazas, las prácticas de protección existentes y ausentes, y la probabilidad de actualización de dichas amenazas, de ahí la naturaleza multidimensional del análisis. El objetivo principal de este procedimiento es compilar una lista de amenazas en orden descendente de gravedad y probabilidad (Hurtado, 2021).

En esta parte de la aplicación de la metodología, los riesgos se definen y priorizan utilizando el enfoque expuesto al principio del documento, en el que se identifican y evalúan los factores más cruciales para la estrategia del banco y se propone un ejercicio estándar de probabilidad frente a un impacto para su evaluación y posterior priorización (Hurtado, 2021).

Proceso 8: Se trata de concebir y ejecutar un plan de protección para disminuir la exposición de la organización a las amenazas de la seguridad de los datos sensibles. El objetivo principal es desarrollar una estrategia de gestión de riesgos y un plan de protección para lo cual se debe integrar las diversas formas de control de seguridad.

Se desarrollan controles para cada uno de los peligros identificados en el paso 7, de modo que puedan crearse planes de mitigación. Tras aplicar cada uno de los controles especificados, se realiza una evaluación del riesgo para valorar su eficacia en la reducción del riesgo (Pacheco et al., 2021).

Las prioridades de aplicación de los controles se establecen asignando un valor numérico a cada ejercicio de riesgo y sumando después los costes de cada aplicación para facilitar la toma de decisiones y la categorización a lo largo de la ejecución. Hacer un cálculo de las pérdidas esperadas es crucial para estimar el coste total del proyecto y decidir qué riesgos se mitigarán y cuáles no. Esto se debe a que revelará qué inversiones son viables e incluso los medios de autofinanciación o mitigación del riesgo, provisión en el cobro de comisiones o seguros contratados (Pacheco et al., 2021).

El despliegue de los controles con mayor impacto positivo sobre el riesgo puede realizarse como parte de la aplicación de estrategias de protección; a continuación, es importante evaluar si los recursos humanos disponibles están o no a la altura de la tarea; por último, es importante calcular cuánto dinero se necesitará para poner en marcha estos planes (Díaz, 2018).

Dado que se descubre que algunos de los riesgos identificados inicialmente pueden ser desencadenados por otros riesgos y, en algunos casos, aumentar la criticidad de otros riesgos, también es importante llevar a cabo una revisión del riesgo impulsor como parte del ejercicio de análisis de riesgos, que no está incluido en la metodología OCTAVE pero que, no obstante, es útil para minimizar los riesgos. En caso de violación de datos, por ejemplo, los delincuentes podrían utilizar la información robada de los clientes para lanzar campañas de vishing o fishing, con el objetivo final de robar el resto de la información de identificación y autenticación necesaria para llevar a cabo su fraude. Estos riesgos están interrelacionados, y debe existir una estrategia minuciosa para hacer frente al riesgo motor si se produce y cuando se produzca (Díaz, 2018).

2.2.2 Seguridad de los sistemas de información

Según, Martinez (2020) la seguridad de los sistemas se refiere a la práctica de proteger la información y los sistemas informáticos contra amenazas y riesgos con el objetivo de garantizar su confidencialidad, integridad y disponibilidad para lo cual se emplea una gestión de incidentes y vulnerabilidades; siguiendo normas legales que regulan los procedimientos en la seguridad de los sistemas.

El término seguridad informática, que es sinónimo de ciberseguridad, se utiliza para describir la práctica de salvaguardar los datos y sistemas para que no sean manipulados por intrusos. Su objetivo principal es evitar daños a las personas, los bienes y los sistemas de información procedentes de fuentes externas. Por eso, el campo de la tecnología de la información que garantiza la seguridad de la información sensible de la empresa dentro de las redes informáticas es esencial para las empresas de hoy en día. Es obvio que no existe un sistema totalmente infalible, por lo que las empresas que dependen de canales electrónicos de comunicación deben tomar medidas

para salvaguardar su información sensible aplicando diversas formas de seguridad informática (Molina, 2000).

2.2.2.1 Confidencialidad e integridad

Según, Martinez (2020) la confidencialidad se rige por la norma ISO 27001 en el cual exige que la información sea accesible exclusivamente a las personas autorizadas. La autorización y la gestión del acceso a la información son cruciales. La confidencialidad se refiere a la necesidad de ocultar o mantener la confidencialidad sobre determinada información o recursos. La confidencialidad, a veces denominada privacidad, sirve como mecanismo fundamental para limitar el acceso a la información exclusivamente a las personas autorizadas, garantizando así que sólo aquellos con la debida autorización tengan visibilidad sobre dicho material. Los datos pueden clasificarse en varias categorías en función de los distintos niveles de seguridad o sensibilidad asociados a la información. Por ejemplo, un desarrollador Java no puede ver los datos personales de todos los trabajadores. Además, es importante proporcionar al personal una formación completa que garantice su comprensión de las estrategias óptimas para proteger los datos sensibles. Esta medida es crucial para fortificar tanto a los empleados individuales como a la organización en su conjunto contra posibles violaciones de la seguridad. Se pueden utilizar varias estrategias para proteger la confidencialidad, como el uso de técnicas de cifrado de datos, la aplicación de protocolos de nombre de usuario y contraseña, la utilización de mecanismos de autenticación de dos factores y la restricción del grado de exposición de la información sensible.

Así mismo, Martinez (2020) refiere que, la integridad se rige por la norma ISO 27001, en el cual la utilidad de los datos está íntimamente ligada a su capacidad para mantener la corrección, coherencia y fiabilidad a lo largo de todo su ciclo de vida. La integridad de los datos debe preservarse durante todo el proceso de transmisión y no debe ser objeto de modificaciones no autorizadas. La implementación de permisos de archivos y mecanismos de control de acceso de usuarios sirve como medida eficaz para mitigar el riesgo de acceso ilegal. El control de versiones es una herramienta valiosa que puede mitigar eficazmente la aparición de modificaciones involuntarias

realizadas por quienes tienen la debida autorización. La disponibilidad de copias de seguridad para restaurar los datos comprometidos y el uso de sumas de comprobación hash para garantizar la integridad de los datos durante el transporte también son consideraciones importantes.

2.2.2.2 Gestión de incidentes

Según, Molina (2000) la norma ISO 27001 regula la gestión de incidentes, incluidos los procedimientos sistemáticos utilizados por las organizaciones para detectar, gestionar, documentar y analizar los riesgos o incidentes de seguridad. El objetivo de este procedimiento es proporcionar una comprensión completa y exhaustiva de cualquier problema de seguridad de las tecnologías de la información dentro del marco tecnológico.

Además, Molina (2000) refiere que, la gestión de incidentes abarca varias fases, entre las que destacan las siguientes:

Preparación: Las acciones que delinean las tácticas a seguir en caso de incidente incluyen varios componentes, como protocolos, escalada de fallos, formatos y otros factores relevantes.

Análisis y detección: El proceso implica la activación de sistemas de alarma predeterminados y la posterior identificación del tipo específico de suceso.

Contención, erradicación y recuperación: Medidas para mitigar y erradicar las consecuencias del suceso, restaurando así los procesos afectados a su estado regular de funcionamiento.

Actividades después de incidentes: Informes finales, comunicados de prensa y otros documentos similares.

2.2.2.3 Gestión de vulnerabilidades

Según, Saeckel (2023) una estrategia potencial para mejorar la seguridad de la infraestructura de TI es la supervisión proactiva de posibles vulnerabilidades y brechas de seguridad. Esto implica la práctica coherente, metódica y regulada de escanear la

red y realizar pruebas de penetración en todos los sistemas para identificar vulnerabilidades tecnológicas. El sistema de gestión de la seguridad de la información (SGSI), de conformidad con la norma ISO 27001, documenta y registra las vulnerabilidades detectadas.

Así mismo, los escáneres de vulnerabilidades suelen ser utilizados por organizaciones de distintos tamaños para evaluar la eficacia y la seguridad de sus sistemas, redes y aplicaciones en línea. Estas herramientas y aplicaciones están diseñadas para ser fáciles de usar, lo que facilita su utilización por una amplia gama de usuarios. Las herramientas de exploración de vulnerabilidades, también denominadas aplicaciones de evaluación de vulnerabilidades, permiten a los equipos de seguridad identificar lagunas, puntos débiles o vulnerabilidades en diversos componentes de un sistema, red o aplicaciones web. Estos componentes pueden incluir cortafuegos, impresoras, faxes, enrutadores, servidores web, sistemas operativos, infraestructura en la nube, componentes de herramientas de código abierto y pruebas de seguridad de aplicaciones (Molina, 2000).

2.2.2.4 Cumplimiento legal y regulatorio

Según, Molina (2000) las empresas deben cumplir con una variedad de regulaciones, incluidas las relacionadas con la privacidad de datos, la seguridad de la información, la protección del medio ambiente y la igualdad de oportunidades. El cumplimiento normativo ayuda a garantizar que las empresas no solo cumplan con la ley, sino que también sigan las mejores prácticas empresariales. Para garantizar que una empresa cumpla con las regulaciones aplicables, es importante implementar un sistema de gestión de riesgos que incluya una estrategia de cumplimiento normativo. Este sistema debe incluir una evaluación continua del riesgo y una actualización constante de los procedimientos de cumplimiento normativo.

Además, en el proceso de gestión de riesgos, el cumplimiento normativo es esencial para garantizar que la empresa cumpla con las leyes y regulaciones aplicables. Las empresas deben tener una comprensión clara de las regulaciones aplicables y cómo estas regulaciones afectan a sus operaciones. Además, deben tener políticas y procedimientos claramente definidos para garantizar que cumplan con estas

regulaciones. Las empresas también deben ser conscientes de las sanciones que enfrentan en caso de incumplimiento normativo. Las sanciones pueden incluir multas y penalizaciones financieras, así como daño a la reputación y pérdida de confianza del cliente. Es importante que las empresas estén preparadas para mitigar estos riesgos y estén en conformidad con todas las regulaciones aplicables (Molina, 2000).

Según, la publicación oficial del Diario el Peruano (2021) en el Perú las normas en cuanto a los sistemas de información se relacionan en la constitución política del Perú, y se regula mediante decreto legislativo N° 1412-Ley de Gobierno Digital

Artículo 2° del título I; de la constitución política del Perú, refiere que toda persona tiene derecho:

6. A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.

7. Al honor y a la buena reputación, a la intimidad personal y familiar, así como a la voz y a la imagen propias.

9. A la libertad de creación intelectual, artística, técnica y científica, así como a la propiedad sobre dichas creaciones y a su producto. El Estado propicia el acceso a la cultura y fomenta su desarrollo y difusión.

10. Al secreto y a la inviolabilidad de sus comunicaciones y documentos privados.

Las comunicaciones, telecomunicaciones o sus instrumentos solo pueden ser abiertos, incautados, interceptados o intervenidos por mandamiento motivado del juez, con las garantías previstas en la ley. Se guarda secreto de los asuntos ajenos al hecho que motiva su examen.

Los documentos privados obtenidos con violación de este precepto no tienen efecto legal.

Los libros, comprobantes y documentos contables y administrativos están sujetos a inspección o fiscalización de la autoridad competente, de conformidad con la ley. Las acciones que al respecto se tomen no pueden incluir su sustracción o incautación, salvo por orden judicial.

Gobierno digital: Las normas del Gobierno digital - Decreto Legislativo Nº 1412, tienen por objeto, regular las actividades de gobernanza y gestión de las tecnologías digitales en las entidades de la Administración Pública en materia de Gobierno Digital, que comprende la identidad digital, interoperabilidad, servicios digitales, datos, seguridad digital y arquitectura digital, así como establecer el marco jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales en los tres niveles de gobierno, conforme lo señalado en el Decreto Legislativo Nº 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital (en adelante la Ley), con observancia de los deberes y derechos fundamentales previstos en la Constitución Política del Perú y en los tratados internacionales de derechos humanos y otros tratados internacionales ratificados por el Perú (El peruano, 2021).

Así mismo se encarga de establecer las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo, y los criterios, condiciones, mecanismos y plazos de implementación de la casilla única electrónica, conforme lo establecido en los numerales 20.4 del artículo 20 y 30.4 del artículo 30 del Texto Único Ordenado de la Ley Nº 27444, Ley del Procedimiento Administrativo General, aprobado mediante Decreto Supremo Nº 004- 2019-JUS (en adelante el TUO de la Ley Nº 27444) (El peruano, 2021).

2.2.2.5 Seguridad de Hardware

Para Barría (2020), la seguridad informática puede dividirse en muchas categorías diferentes, las más importantes de las cuales son el software, la red y el hardware.

Esta rama de la seguridad se ocupa de salvaguardar el hardware y el software que defiende los ordenadores y las redes contra los intrusos. Las prácticas habituales incluyen la gestión del SAI, la administración del servidor proxy, la administración del cortafuegos, la gestión del HSM y la DLP (protección frente a la pérdida de datos). Esta seguridad también incluye proteger el hardware de daños físicos (Barría, 2020).

Cuando hablamos de seguridad informática, el término *hardware* se refiere a los propios dispositivos. Es decir, son el tipo de cosas que se conectan al ordenador o a otros aparatos electrónicos para hacerlos más seguros. A menudo se utiliza para complementar la seguridad del software y es una de las formas más cruciales de seguridad informática. Prepara el camino para una estrategia de seguridad informática que tenga en cuenta no sólo la seguridad del software, sino también la de los componentes físicos del sistema (Barría, 2020).

Las medidas de seguridad del hardware pueden adoptar la forma de firewalls, un servidor proxy o un módulo de seguridad. También es norma de este departamento identificar y evaluar los fallos de seguridad en hardware y software, y concebir soluciones preventivas. Este tipo de seguridad ofrece probablemente el mayor nivel de protección para los sistemas informáticos, pero suele ser el más difícil y costoso de implantar debido a la necesidad de hardware adicional (Hincapie, 2018).

Cuando se habla de seguridad informática, el término *hardware* se utiliza para referirse a los propios dispositivos. Los periféricos de seguridad son componentes añadidos que protegen un ordenador u otro equipo electrónico. Cuando hablamos de ordenadores, seguridad física del hardware, significa tomar precauciones para evitar que el hardware resulte dañado por fuerzas externas. Golpes, caídas, mal tiempo, incendios y otras calamidades cuentan como peligros externos. Hay que formar a los empleados en el uso correcto de los equipos, y también es importante ofrecer componentes de protección adecuados (Hincapie, 2018).

La manipulación de aparatos o el robo de equipos informáticos son dos ejemplos de peligros externos que hay que tener en cuenta. Los equipos deben colocarse en zonas seguras a las que no pueda acceder nadie no autorizado. Además,

podemos tratar el tema de la seguridad física de la radiodifusión. El tema que nos ocupa es la protección de la emisión de señales por hardware. Hay varias formas de que los datos sensibles caigan en malas manos, como la transmisión de pantallas de ordenador a través de ventanas o la captación de ondas electromagnéticas radiadas por dispositivos (Hincapie, 2018).

2.2.2.6 Seguridad de software

Se utiliza para prevenir los ataques de piratas informáticos y otras amenazas asociadas a fallos del software. Los intrusos pueden aprovechar estos "puntos débiles" para acceder a los sistemas, de ahí que se necesiten soluciones basadas en modelos de autenticación (Hernández M. , 2020).

Todo desarrollador se preocupa por la solidez de las medidas de seguridad de su software. Es un hecho innegable. Sin embargo, garantizar que el software es realmente seguro puede resultar difícil en el complicado entorno informático actual, con empresas que utilizan más software que nunca y ciberataques persistentes. La amplia disponibilidad de programas informáticos de seguridad en la actualidad permite tanto a las empresas como a los usuarios particulares comprobar que disponen de las protecciones adecuadas (Hernández M. , 2020).

Para garantizar que el software siga funcionando (o sea resistente a los ataques), la seguridad del software es la práctica de incorporar medidas de protección en su diseño y construcción. Esto implica que antes de que un software se ponga a disposición del público, se somete a pruebas de seguridad para garantizar que puede resistir los ataques de los ciberdelincuentes. El objetivo de la seguridad del software es garantizar que los programas se construyen pensando en la seguridad desde el principio, eliminando la necesidad de medidas de seguridad adicionales (que, por desgracia, se aplican a menudo). La instrucción en el uso correcto del software es la siguiente etapa para reducir la vulnerabilidad a las intrusiones (Hernández M. , 2020).

Los ataques de malware son muy peligrosos, ya que comprometen la integridad, autenticación y disponibilidad de cualquier programa que infecten. Los

daños pueden evitarse en seco si los desarrolladores piensan en ello a lo largo de la fase de codificación y no después (Hernández M. , 2020).

2.2.2.7 Seguridad de la red

El objetivo principal es la planificación de medidas para salvaguardar los datos a los que se puede acceder a través de la red, pero que corren el riesgo de ser corrompidos, robados o utilizados indebidamente. Virus, troyanos, phishing, spyware, robo de datos y usurpación de identidad son los principales peligros en este campo (Alzórriz, 2014).

El término seguridad de la red se refiere a las medidas adoptadas para evitar daños o accesos no autorizados a la red interna de una empresa. Los hackers, el malware y los virus son los culpables habituales de los ataques a las redes informáticas y a los datos que contienen. Impedir que estos ataques entren y se propaguen por la red es una cuestión de primer orden para la seguridad de la red (Alzórriz, 2014).

La seguridad de una red depende de varias capas de protección, tanto externas como internas. La base de la seguridad de la red es el control de acceso, o el conjunto de normas y procedimientos utilizados para admitir personas, dispositivos y datos en la red de forma segura. Un firewall, que puede ser de hardware o de software, es otra barrera fundamental que impide el acceso no autorizado desde Internet y otras redes no fiables. Los firewalls se utilizan para controlar y restringir el tráfico de red. Los sistemas de detección y prevención de intrusiones también se utilizan para la seguridad de la red; estos sistemas supervisan el tráfico de la red en busca de actividades sospechosas y toman las medidas oportunas. La seguridad de las aplicaciones es un tipo de seguridad de red que se centra en proteger el software y las aplicaciones en línea frente a posibles amenazas. Los centros de datos y las nubes públicas, entre otros lugares, utilizan diversas tácticas y tecnologías para garantizar la seguridad de los usuarios (Gigant, 2016).

La llegada de la tecnología digital ha provocado un enorme cambio global. Ha alterado nuestros métodos de transporte, comunicación, educación y ocio. Una red segura es esencial para toda empresa que quiera satisfacer las necesidades de sus

clientes y trabajadores. Proteger los datos sensibles de intrusiones es otra de las ventajas de la seguridad de la red. En definitiva, salvaguarda su buen nombre (Gigant, 2016).

2.2.2.8 Políticas de seguridad informática

Las políticas de seguridad de las tecnologías de la información son conjuntos de reglas y normas diseñadas para proteger los datos y reducir la probabilidad de fallos de seguridad. El conjunto de normas que hay que aplicar, son las líneas maestras de una política de seguridad. Los mecanismos, tanto tecnológicos como organizativos, que se ponen en marcha para garantizar el cumplimiento de la política se establecen en una serie de procesos e instrucciones técnicas (Tavosnanska, 2011).

Todos los procedimientos, sistemas y personas de una organización deben tenerse en cuenta a la hora de crear una política de seguridad, teniendo en cuenta los peligros a los que está expuesta la información. También tiene que haber sido divulgada a todos los empleados y autorizada por la dirección de la organización (Tavosnanska, 2011).

En concreto, los siguientes conjuntos de normas y reglamentos conforman el cuerpo normativo de una organización en materia de seguridad de la información:

Buenas prácticas: El documento de buenas prácticas en materia de seguridad de la información -que puede ser un documento independiente o cláusulas anexas a los contratos de los empleados, etc.- debe incluir directrices sobre el uso adecuado de los sistemas y la información por parte de los empleados, normas de limpieza de los puestos de trabajo, el bloqueo de los equipos desatendidos y la protección de las contraseñas (Tavosnanska, 2011).

Procedimiento de control de accesos: El control de acceso es el conjunto de salvaguardias tecnológicas y organizativas establecidas para garantizar que sólo el personal autorizado tenga acceso a los datos y sistemas sensibles dentro de una organización. Los controles de entrada pueden ser físicos o electrónicos (Tavosnanska, 2011).

Control de acceso físico: Tornos, barreras, cámaras, alarmas, sistemas biométricos o de apertura de puertas con tarjeta, etc. son ejemplos de mecanismos y sistemas de control de acceso que pueden utilizarse para supervisar y gestionar quién entra y sale de los edificios de una organización. La información almacenada en armarios con cerradura es otro tipo de control de acceso físico, al igual que cualquier otra barrera física o protección contra el acceso no deseado a los datos (Tavosnanska, 2011).

Control de acceso lógico: Los sistemas de gestión de acceso se configuran para que sólo los usuarios autorizados puedan acceder a los datos o a los numerosos servidores que los almacenan. Implantar un NAC (control de acceso de ordenadores y usuarios a la red), establecer permisos de lectura/escritura en los propios archivos de información, configurar sistemas de login en los distintos sistemas, autorizar a los usuarios a acceder remotamente a la red a través de una VPN, etc. son ejemplos de controles lógicos de acceso (Tavosnanska, 2011).

2.3 Bases conceptuales

Activo: Un activo se refiere a cualquier recurso valioso que posee una organización o entidad. Puede ser físico, digital o intangible, y su valor puede ser económico, operativo o estratégico. Los activos se consideran valiosos porque contribuyen al funcionamiento y al éxito de la organización (Muñoz, 2020).

Vulnerabilidad del sistema: Una vulnerabilidad del sistema se refiere a una debilidad o defecto en un sistema informático, software, red o proceso que podría ser explotado por un atacante o provocar un mal funcionamiento, comprometiendo la seguridad o el rendimiento del sistema. Las vulnerabilidades pueden surgir debido a errores de diseño, programación o configuración, y pueden ser utilizadas por individuos malintencionados para ganar acceso no autorizado, robar información, causar daños o interrumpir el funcionamiento normal del sistema (Santos, 2023).

Plan de mitigación: Un plan de mitigación es un conjunto de acciones y estrategias diseñadas para reducir o minimizar los impactos negativos de un riesgo, amenaza o situación problemática. Estos planes son comunes en contextos de gestión

de riesgos y seguridad, donde se busca anticiparse a posibles problemas y tomar medidas preventivas o correctivas para reducir su probabilidad de ocurrencia o mitigar sus efectos en caso de que ocurran (Enrique, 2023).

Encriptación: La encriptación es un proceso de seguridad que consiste en convertir información legible en un formato ilegible y cifrado, de modo que solo las personas o sistemas con la clave de encriptación adecuada puedan revertir el proceso y descifrar la información (Carvajal, 2019).

Firma digital: Una firma digital es un componente esencial de la seguridad en línea que proporciona autenticación, integridad y no repudio a documentos y mensajes electrónicos. Es similar a una firma manuscrita en documentos físicos, pero se aplica a documentos digitales y electrónicos. La firma digital es una forma de garantizar que el contenido de un mensaje o un documento no haya sido alterado y que el autor del mensaje o el documento sea quien dice ser (RENIEC, 2015).

Actualizaciones: Una actualización se refiere a la acción de modificar, mejorar o corregir un software, aplicación, sistema operativo o cualquier otro tipo de programa o tecnología con el objetivo de implementar mejoras, resolver problemas, agregar nuevas funciones o mantener la seguridad (Gutierrez, 2019) .

Auditorias: Las auditorías son procesos de revisión y evaluación sistemática de actividades, sistemas, registros u operaciones con el objetivo de verificar su precisión, conformidad, eficiencia, legalidad o cumplimiento de estándares establecidos (Pert, 2023).

2.4 Bases epistemológicas, bases filosóficas y/o bases antropológicas

La seguridad informática tiene fundamentos filosóficos que guían su enfoque y comprensión desde una perspectiva ética y conceptual (Voutssas, 2010).

Ética de la información: Esta filosofía se centra en la ética y la moralidad en el uso y el acceso a la información. Reconoce que la información es un recurso valioso y aboga por el respeto a los derechos de propiedad intelectual, la privacidad y la

confidencialidad. También plantea cuestiones sobre cómo se debe recopilar, compartir y proteger la información de manera ética.

Privacidad y autonomía: La filosofía de la privacidad se refiere a la capacidad de las personas para controlar su información personal y ser libres de interferencias no deseadas en sus vidas. La seguridad informática busca preservar la privacidad y la autonomía al proteger la información personal y prevenir el acceso no autorizado a datos sensibles.

Responsabilidad tecnológica: Esta filosofía sostiene que aquellos que crean, implementan y utilizan tecnología tienen la responsabilidad de hacerlo de manera ética y considerada. En el contexto de la seguridad informática, esto implica diseñar sistemas seguros, proteger la integridad de los datos y prevenir daños innecesarios.

Justicia y equidad digital: La seguridad informática también se relaciona con la idea de proporcionar igualdad de acceso y oportunidades en el mundo digital. Esto significa que las medidas de seguridad no deben discriminar ni perjudicar a ciertos grupos o individuos, y que se debe luchar por un entorno digital justo y equitativo.

Filosofía hacker ética: Algunos aspectos de la cultura hacker están basados en valores éticos, como la curiosidad, el aprendizaje constante y el deseo de resolver problemas de manera creativa. La filosofía hacker ética promueve el uso de habilidades técnicas para el bienestar de la sociedad y la protección de sistemas en lugar de su explotación.

Transparencia y responsabilidad corporativa: Las empresas y organizaciones que gestionan y almacenan datos de usuarios tienen la responsabilidad de proteger esos datos y actuar con transparencia sobre cómo se utilizan. La filosofía de la seguridad informática exige que las organizaciones sean responsables en su manejo de la información y estén dispuestas a rendir cuentas por cualquier violación de seguridad.

CAPÍTULO III. METODOLOGÍA

3.1 Ámbito

La presente investigación se desarrolló en la Universidad Nacional Hermilio Valdizán; ubicada en el distrito de Pillco Marca, provincia y departamento de Huánuco.

3.2 Población

Hernández et. al (2017) señala que el término "población" se refiere a la totalidad del fenómeno y es un fenómeno objeto de una investigación, incluyendo todas las unidades de análisis que lo componen y que deben ser cuantificadas respecto a un determinado estudio mediante la integración de un conjunto N de entes que participan en una función determinada.

La población estuvo conformada por 91 administrativos que trabajan con el procesamiento de información de la Universidad Nacional Hermilio Valdizán.

3.3 Muestra

Hernández et. al (2017) menciona “Una muestra es un subconjunto de una población más amplia que está diseñado estadísticamente para reflejar la población en su conjunto”. Como el estudio de la totalidad de la población sería inviable debido a su tamaño o ubicación, los investigadores suelen tener que elegir un subconjunto, o muestra, para analizarla.

La selección de muestra se determinó mediante el muestreo no probabilístico de forma intencionada, es por lo que se eligió el 100% de la población conformado por 91 administrativos que están relacionados con los sistemas de información de la Universidad Nacional Hermilio Valdizán.

3.4 Nivel y tipo de estudio

3.4.1 Nivel

El nivel de la investigación correspondió al nivel descriptivo correlacional; porque se describió las características de ambas variables, para determinar la relación entre la metodología Octave y la seguridad de los sistemas de información.

Al respecto Arias (2006), menciona que "la investigación descriptiva consiste en la caracterización de un hecho, con el fin de establecer su comportamiento, así mismo lo clasifica en correlacional siendo su finalidad determinar el grado de relación (no causal) existente entre dos o más variables" (pp. 24-25).

3.4.2 Tipo

La presente investigación corresponde a la investigación básica o pura; porque los resultados sirvieron de referencia para tomar medidas de seguridad sobre los activos de los sistemas de información, además de determinar la relación entre la Metodología Octave y la seguridad de los sistemas de información.

Sánchez et. al (2015), el tipo de investigación básica, "nos lleva a la búsqueda de nuevos conocimientos y campos de investigación, no tiene objetivos prácticos específicos. Mantiene como propósito recoger información de la realidad para enriquecer el conocimiento científico, está orientando al descubrimiento de principios y leyes" (pp. 47-48).

3.5 Diseño de investigación

La investigación correspondió al diseño no experimental correlacional transversal.

Según, Hernández y Mendoza (2018), "estos diseños son útiles para establecer relaciones entre dos o más categorías, conceptos o variables en un momento determinado sin manipular las variables" (p. 178).

No experimental: Porque no se manipuló las variables, se describió las características de las variables en su estado natural para profundizar el estudio.

Según Hernández y Mendoza (2018), “Los estudios no experimentales no se manipula deliberadamente las variables se estudian en su estado natural” (p. 175).

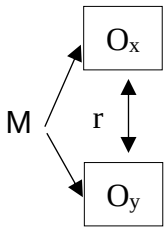
Transversal: Porque la recolección de datos mediante la aplicación de los instrumentos sobre metodología Octave y la seguridad de los sistemas se realizó en un solo momento y en un solo tiempo.

Según Hernández y Mendoza (2018), “los diseños transeccional o transversal recolectan datos en un solo momento, en un tiempo único” (p. 240).

Correlacional: Porque se determinó la relación entre la metodología Octave y la seguridad de los sistemas de información en su estado natural, además se utilizó un método estadístico descriptivo e inferencial para responder las hipótesis de asociación planteadas en el estudio.

Según, Hernández y Mendoza, (2018), “los estudios correlacionales son investigaciones que pretenden asociar conceptos, fenómenos, hechos o variables. Miden las variables y su relación en términos estadísticos” (p. 109).

El diseño se diagrama de la siguiente manera:



Donde:

M = Muestra conformado por 91 administrativos

Ox = Variable 1: Metodología Octave

O2 = Variable 2: Seguridad de los sistemas de información

r = Relación entre las variables

3.6 Métodos, técnicas e instrumentos

3.6.1 Método

De acuerdo a Bunge (2004), “un método es un procedimiento para tratar un conjunto de problemas. Cada clase de problemas requiere un conjunto métodos o técnicas especiales. Los problemas del conocimiento, a diferencia de los del lenguaje o los de la acción, requieren la invención o la aplicación de procedimientos especiales adecuados para los varios estadios del tratamiento de los problemas, desde el mero enunciado de estos hasta el control de las soluciones propuestas” (p. 7).

La presente investigación se realizó mediante el método científico; la cual permitió descubrir las condiciones en que se presentan sucesos específicos, caracterizado generalmente por ser tentativo, verificable, de razonamiento riguroso y observación empírica.

3.6.2 Técnica

Según Hernández et. al (2017), “los métodos y procedimientos de recogida de información se denominan técnicas y varían en función del campo de estudio. Los datos se recogen una vez que se utiliza un procedimiento, entre las técnicas se tiene la encuesta, la observación, etc.” (p. 217).

Para la investigación se utilizó la técnica encuesta, porque permitió recopilar datos de una determinada muestra para presentar los resultados.

3.6.3 Instrumento

Según Vara (2012), “los métodos de investigación que incluyen métodos cuantitativos suelen ser descriptivos, correlacionales o explicativos. Estos instrumentos están bien estructurados, pueden ser modificados para su uso con una amplia gama de pruebas estadísticas y proporcionan una ayuda inestimable para proporcionar descripciones y mediciones precisas de una variedad de factores” (p. 254).

En la investigación se utilizó el cuestionario como instrumento que permitió recopilar información sobre las características de la metodología octave y los sistemas de seguridad de la información, lo cual permitió abordar conocimientos para presentar los resultados que indique la relación de una variable hacia la otra.

3.7 Validación y confiabilidad del instrumento

El cuestionario contó con 12 ítems por cada variable, en escala de Likert, además fue validado por juicio de expertos y fue sometido a un proceso de confiabilidad mediate la vierificación de consistencia con el estadístico Alfa de Cronbach.

3.8 Procedimiento

Para el desarrollo de la presente investigación se realizó los siguientes pasos:

- Se contó con la autorización del decano de la Universidad Nacional Hermilio Valdizán, lo cual sirvió para recopilar información sobre los sistemas de información.
- Para recopilar información primaria se aplicó el cuestionario a 91 administrativos que están relacionados con los sistemas de información de la UNHEVAL, así mismo los participantes previamente han aceptado colaborar con los fines investigativos mediante el consentimiento informado que fueron ser firmado en el momento adecuado.
- Con los datos recopilados se pudo recabar información sobre la clasificación de los activos, evaluación, analices e identificación de riesgos de información, seguidamente se procederá a establecer un plan y una estrategia para mejorar los sistemas de información de la UNHEVAL.
- Finalmente se abordó la conclusiones y recomendaciones.

3.9 Tabulación y análisis de datos

Los datos recopilados del cuestionario se procesarán transformándola en una base de datos. La estadística descriptiva se realizó con el programa Microsoft Excel de

donde se obtuvo las tablas, frecuencias, figuras, gráficos e interpretaciones correspondientes a las preguntas planteadas que responde a los indicadores y dimensiones de las variables. Consecuentemente se realizó la estadística inferencial mediante el programa estadístico SPSS versión 27.0 y el programa Microsoft Excel donde se obtendrá la prueba de normalidad y la prueba de hipótesis.

Para demostrar las hipótesis se utilizó el método estadístico según corresponda si los datos provienen de una distribución paramétrica o no paramétrica para lo cual se realizó la prueba de normalidad y según los resultados se utilizó el estadístico Spearman siempre en cuando los datos tengan una distribución no paramétrica o Pearson si la distribución de los datos es paramétrica.

Además, según el método estadístico que se elija, se pudo determinar la relación que existe entre la metodología Octave y la seguridad de los sistemas de información, así como establecer la aplicación de las fases de la metodología octave en la mejora de la seguridad de los sistemas de información.

3.10 Consideraciones éticas

El presente trabajo empleó los siguientes aspectos éticos:

a) Protección a las personas.

b) Consentimiento informado.

c) Responsabilidad, rigor científico y veracidad.

d) Honestidad.

e) Justicia.

f) Privacidad y confidencialidad.

CAPÍTULO IV. RESULTADOS

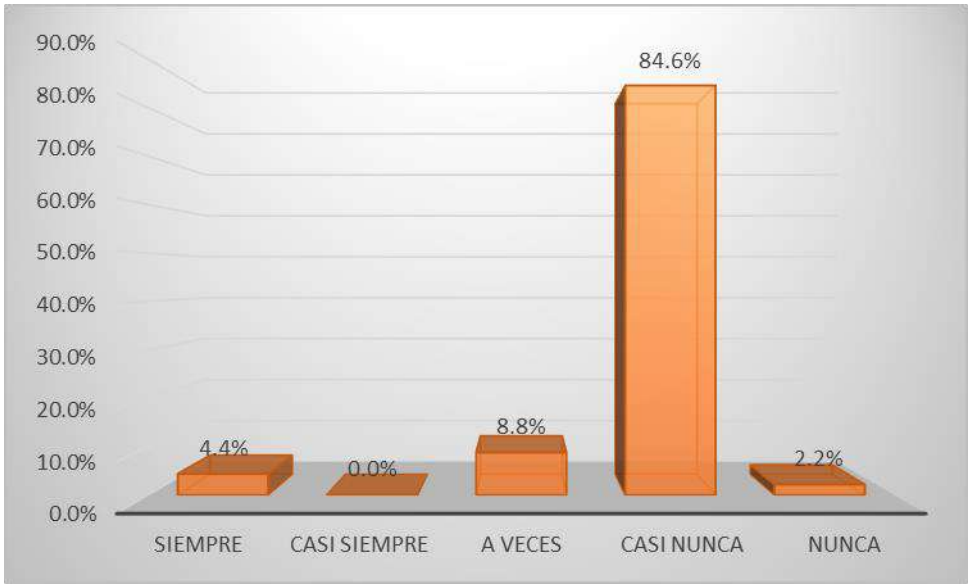
4.1 Resultados descriptivos

Tabla 1. Se identifica los activos de los sistemas de información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Siempre	4	4,4	4,4	4,4
	Casi siempre	0	0,0	0,0	4,4
	A veces	8	8,8	8,8	13,2
	Casi nunca	77	84,6	84,6	97,8
	Nunca	2	2,2	2,2	100,0
	Total	91	100,0	100,0	

Nota. Datos obtenidos del procesamiento en SPSS

Figura 1. Se identifica los activos de los sistemas de información



Nota. Datos obtenidos del procesamiento en SPSS

Interpretación:

En la tabla 1 y figura 1, se observa que de los encuestados, el 84.6% casi nunca identifica activos de los sistemas de información; el 8.8% a veces; el 4.4% siempre; el 2.2% nunca y el 0.0% casi siempre. Estos resultados evidencian que los activos de los sistemas de información de la Universidad Nacional Hermilio Valdizán casi nunca se identifican.

Tabla 2. Se clasifica los activos de los sistemas de información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Siempre	13	14,3	14,3	14,3
	Casi siempre	10	11,0	11,0	25,3
	A veces	20	22,0	22,0	47,3
	Casi nunca	46	50,5	50,5	97,8
	Nunca	2	2,2	2,2	100,0
	Total	91	100,0	100,0	

Nota. Datos obtenidos del procesamiento en SPSS

Figura 2. Se clasifica los activos de los sistemas de información

Nota. Datos obtenidos del procesamiento en SPSS

Interpretación:

En la tabla 2 y figura 2, se observa que, de los encuestados, el 50.5% casi nunca clasifican los activos de los sistemas de información; el 22.0% a veces; el 14.3% siempre; el 11.0% casi siempre y el 2.2% nunca. Estos resultados evidencian que los activos de los sistemas de información de la Universidad Nacional Hermilio Valdizán casi nunca se clasifican.

Tabla 3. Se identifica los riesgos de los sistemas de información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Siempre	13	14,3	14,3	14,3
	Casi siempre	11	12,1	12,1	26,4
	A veces	19	20,9	20,9	47,3
	Casi nunca	46	50,5	50,5	97,8
	Nunca	2	2,2	2,2	100,0
	Total	91	100,0	100,0	

Nota. Datos obtenidos del procesamiento en SPSS

Figura 3. Se identifica los riesgos de los sistemas de información

Nota. Datos obtenidos del procesamiento en SPSS

Interpretación:

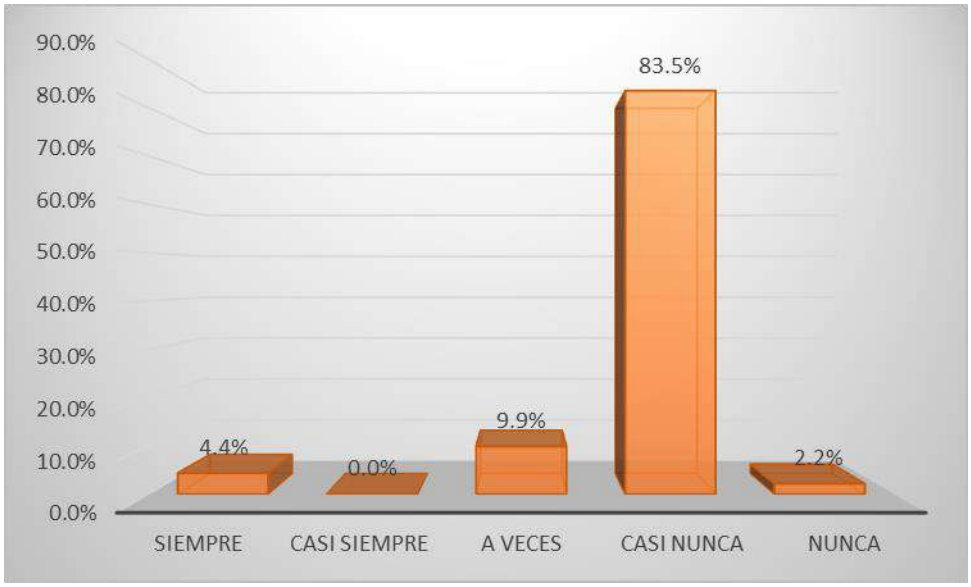
En la tabla 3 y figura 3, se observa que de los encuestados, el 50.5% casi nunca identifican los riesgos de los sistemas de información; el 20.9% a veces; el 14.3% siempre; el 12.1% casi siempre y el 2.2% nunca. Estos resultados evidencian que los riesgos de los sistemas de información de la Universidad Nacional Hermilio Valdizán casi nunca se identifican.

Tabla 4. Se identifica las defensas de los sistemas de información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Siempre	4	4,4	4,4	4,4
	Casi siempre	0	0,0	0,0	4,4
	A veces	9	9,9	9,9	14,3
	Casi nunca	76	83,5	83,5	97,8
	Nunca	2	2,2	2,2	100,0
	Total	91	100,0	100,0	

Nota. Datos obtenidos del procesamiento en SPSS

Figura 4. Se identifica las defensas de los sistemas de información



Nota. Datos obtenidos del procesamiento en SPSS

Interpretación:

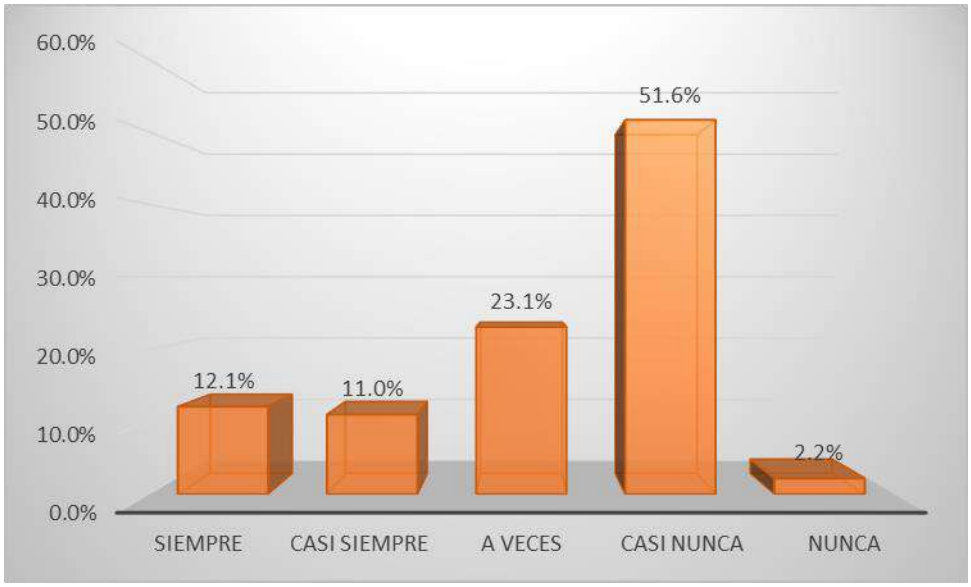
En la tabla 4 y figura 4, se observa que de los encuestados, el 83.5% casi nunca identifican las defensas de los sistemas de información; el 9.9% a veces; el 4.4% siempre; el 2.2% nunca y el 0.0% casi siempre. Estos resultados evidencian que las defensas de los sistemas de información de la Universidad Nacional Hermilio Valdizán casi nunca se identifican.

Tabla 5. Se identifica las necesidades de seguridad

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Siempre	11	12,1	12,1	12,1
	Casi siempre	10	11,0	11,0	23,1
	A veces	21	23,1	23,1	46,2
	Casi nunca	47	51,6	51,6	97,8
	Nunca	2	2,2	2,2	100,0
	Total	91	100,0	100,0	

Nota. Datos obtenidos del procesamiento en SPSS

Figura 5. Se identifica las necesidades de seguridad



Nota. Datos obtenidos del procesamiento en SPSS

Interpretación:

En la tabla 5 y figura 5, se observa que de los encuestados, el 51.6% casi nunca identifican las necesidades de seguridad de los sistemas de información; el 23.1% a veces; el 12.1% siempre; el 11.0% casi siempre y el 2.2% nunca. Estos resultados evidencian que las necesidades de seguridad de los sistemas de información de la Universidad Nacional Hermilio Valdizán casi nunca se identifican.

Tabla 6. Se identifica vulnerabilidades en el sistema de información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Siempre	13	14,3	14,3	14,3
	Casi siempre	9	9,9	9,9	24,2
	A veces	18	19,8	19,8	44,0
	Casi nunca	48	52,7	52,7	96,7
	Nunca	3	3,3	3,3	100,0
	Total	91	100,0	100,0	

Nota. Datos obtenidos del procesamiento en SPSS

Figura 6. Se identifica vulnerabilidades en el sistema de información

Nota. Datos obtenidos del procesamiento en SPSS

Interpretación:

En la tabla 6 y figura 6, se observa que de los encuestados, el 52.7% casi nunca identifican vulnerabilidades en el sistema de información; el 19.8% a veces; el 14.3% siempre; el 9.9% casi siempre y el 3.3% nunca. Estos resultados evidencian que las vulnerabilidades de los sistemas de información de la Universidad Nacional Hermilio Valdizán casi nunca se identifican.

Tabla 7. Se evalúa vulnerabilidades en el sistema de información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Siempre	13	14,3	14,3	14,3
	Casi siempre	10	11,0	11,0	25,3
	A veces	16	17,6	17,6	42,9
	Casi nunca	46	50,5	50,5	93,4
	Nunca	6	6,6	6,6	100,0
	Total	91	100,0	100,0	

Nota. Datos obtenidos del procesamiento en SPSS

Figura 7. Se evalúa vulnerabilidades en el sistema de información

Nota. Datos obtenidos del procesamiento en SPSS

Interpretación:

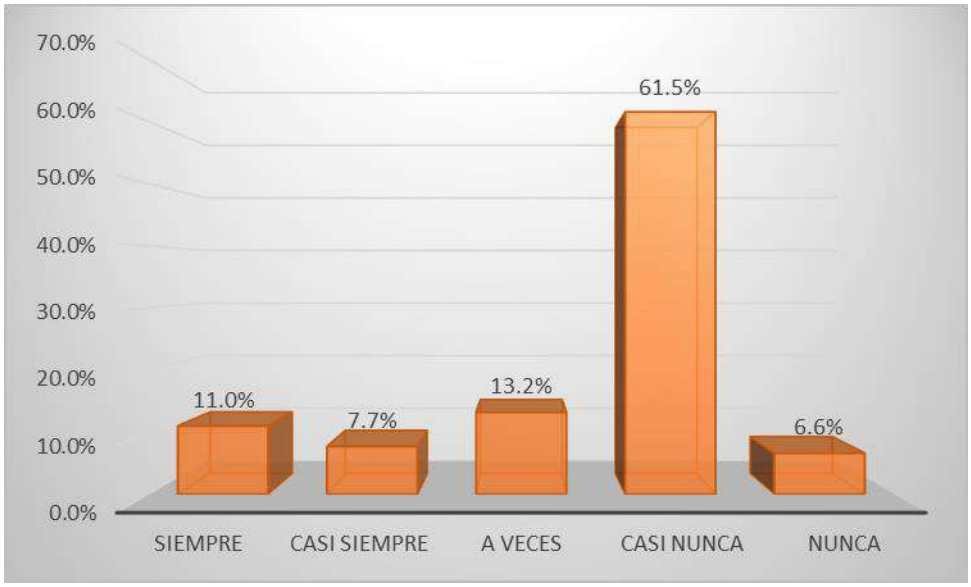
En la tabla 7 y figura 7, se observa que de los encuestados, el 50.5% casi nunca evalúan vulnerabilidades en el sistema de información; el 17.6% a veces; el 14.3% siempre; el 11.0% casi siempre y el 6.6% nunca. Estos resultados evidencian que las vulnerabilidades de los sistemas de información de la Universidad Nacional Hermilio Valdizán casi nunca se evalúan.

Tabla 8. Se analiza vulnerabilidades en el sistema de información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Siempre	10	11,0	11,0	11,0
	Casi siempre	7	7,7	7,7	18,7
	A veces	12	13,2	13,2	31,9
	Casi nunca	56	61,5	61,5	93,4
	Nunca	6	6,6	6,6	100,0
	Total	91	100,0	100,0	

Nota. Datos obtenidos del procesamiento en SPSS

Figura 8. Se analiza vulnerabilidades en el sistema de información



Nota. Datos obtenidos del procesamiento en SPSS

Interpretación:

En la tabla 8 y figura 8, se observa que de los encuestados, el 61.5% casi nunca analiza vulnerabilidades en el sistema de información; el 13.2% a veces; el 11.0% siempre; el 7.7% casi siempre y el 6.6% nunca. Estos resultados evidencian que las vulnerabilidades de los sistemas de información de la Universidad Nacional Hermilio Valdizán casi nunca se analizan.

Tabla 9. Se prioriza la atención de vulnerabilidades en el sistema de información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Siempre	13	14,3	14,3	14,3
	Casi siempre	10	11,0	11,0	25,3
	A veces	17	18,7	18,7	44,0
	Casi nunca	46	50,5	50,5	94,5
	Nunca	5	5,5	5,5	100,0
	Total	91	100,0	100,0	

Nota. Datos obtenidos del procesamiento en SPSS

Figura 9. Se prioriza la atención de vulnerabilidades en el sistema de información

Nota. Datos obtenidos del procesamiento en SPSS

Interpretación:

En la tabla 9 y figura 9, se observa que, de los encuestados, el 50.5% casi nunca se prioriza las vulnerabilidades en el sistema de información; el 18.7% a veces; el 14.3% siempre; el 11.0% casi siempre y el 5.5% nunca. Estos resultados evidencian que las vulnerabilidades de los sistemas de información de la Universidad Nacional Hermilio Valdizán casi nunca se priorizan.

Tabla 10. Se identifica los riesgos de información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Siempre	19	20,9	20,9	20,9
	Casi siempre	10	11,0	11,0	31,9
	A veces	14	15,4	15,4	47,3
	Casi nunca	47	51,6	51,6	98,9
	Nunca	1	1,1	1,1	100,0
	Total	91	100,0	100,0	

Nota. Datos obtenidos del procesamiento en SPSS

Figura 10. Se identifica los riesgos de información

Nota. Datos obtenidos del procesamiento en SPSS

Interpretación:

En la tabla 10 y figura 10, se observa que de los encuestados, el 51.6% casi nunca identifican los riesgos en el sistema de información; el 20.9% siempre; el 15.4% a veces; el 11.0% casi siempre y el 1.1% nunca. Estos resultados evidencian que los riesgos de los sistemas de información de la Universidad Nacional Hermilio Valdizán casi nunca se identifican.

Tabla 11. Se realiza controles de seguridad

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Siempre	2	2,2	2,2	2,2
	Casi siempre	38	41,8	41,8	44,0
	A veces	34	37,4	37,4	81,3
	Casi nunca	17	18,7	18,7	100,0
	Nunca	2	2,2	2,2	2,2
	Total	91	100,0	100,0	

Nota. Datos obtenidos del procesamiento en SPSS

Figura 11. Se realiza controles de seguridad

Nota. Datos obtenidos del procesamiento en SPSS

Interpretación:

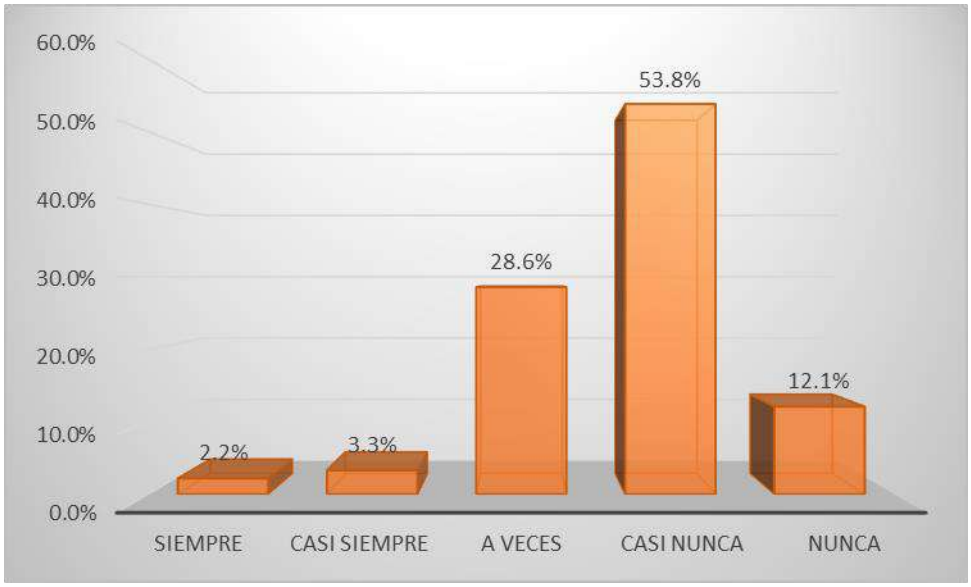
En la tabla 11 y figura 11, se observa que de los encuestados, el 40.9% casi siempre realizan controles de seguridad en el sistema de información; el 36.6% a veces; el 18.3% casi nunca; el 2.2% siempre y el 2.2% nunca. Estos resultados evidencian que los controles de seguridad de los sistemas de información de la Universidad Nacional Hermilio Valdizán casi siempre y a veces se realizan.

Tabla 12. Hay integración de controles

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Siempre	2	2,2	2,2	2,2
	Casi siempre	3	3,3	3,3	5,5
	A veces	26	28,6	28,6	34,1
	Casi nunca	49	53,8	53,8	87,9
	Nunca	11	12,1	12,1	100,0
	Total	91	100,0	100,0	

Nota. Datos obtenidos del procesamiento en SPSS

Figura 12. Hay integración de controles



Nota. Datos obtenidos del procesamiento en SPSS

Interpretación:

En la tabla 12 y figura 12, se observa que, de los encuestados, el 53.8% casi nunca hay integraciones de controles en el sistema de información; el 28.6% a veces; el 12.1% nunca; el 3.3% casi siempre y el 2.2% siempre. Estos resultados evidencian que la integración de controles de los sistemas de información de la Universidad Nacional Hermilio Valdizán casi nunca se integra.

Tabla 13. Realizan controles de acceso

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Siempre	13	14,3	14,3	14,3
	Casi siempre	9	9,9	9,9	24,2
	A veces	18	19,8	19,8	44,0
	Casi nunca	48	52,7	52,7	96,7
	Nunca	3	3,3	3,3	100,0
	Total	91	100,0	100,0	

Nota. Datos obtenidos del procesamiento en SPSS

Figura 13. Realizan controles de acceso

Nota. Datos obtenidos del procesamiento en SPSS

Interpretación:

En la tabla 13 y figura 13, se observa que de los encuestados, el 52.7% casi nunca realizan controles de acceso en el sistema de información; el 19.8% a veces; el 14.3% siempre; el 9.9% casi siempre y el 3.3% nunca. Estos resultados evidencian que el control de acceso a los sistemas de información de la Universidad Nacional Hermilio Valdizán casi nunca se realiza.

Tabla 14. Realizan encriptaciones a la información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Siempre	13	14,3	14,3	14,3
	Casi siempre	10	11,0	11,0	25,3
	A veces	16	17,6	17,6	42,9
	Casi nunca	46	50,5	50,5	93,4
	Nunca	6	6,6	6,6	100,0
	Total	91	100,0	100,0	

Nota. Datos obtenidos del procesamiento en SPSS

Figura 14. Realizan encriptaciones a la información

Nota. Datos obtenidos del procesamiento en SPSS

Interpretación:

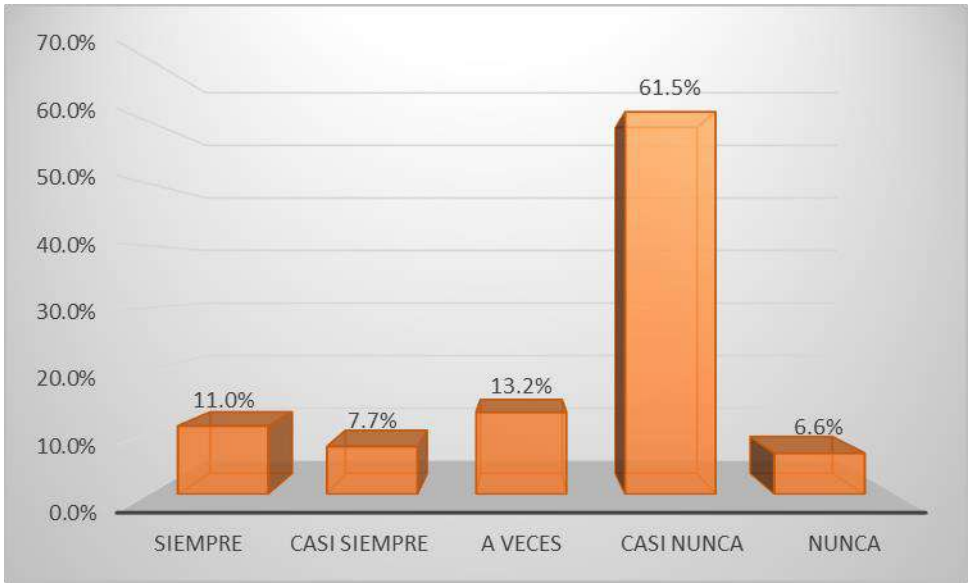
En la tabla 14 y figura 14, se observa que de los encuestados, el 50.5% casi nunca realizan encriptaciones a la información; el 17.6% a veces; el 14.3% siempre; el 11.0% casi siempre y el 6.6% nunca. Estos resultados evidencian que las encriptaciones de los sistemas de información de la Universidad Nacional Hermilio Valdizán casi nunca se realizan.

Tabla 15. Realizan controles de cambios

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Siempre	10	11,0	11,0	11,0
	Casi siempre	7	7,7	7,7	18,7
	A veces	12	13,2	13,2	31,9
	Casi nunca	56	61,5	61,5	93,4
	Nunca	6	6,6	6,6	100,0
	Total	91	100,0	100,0	

Nota. Datos obtenidos del procesamiento en SPSS

Figura 15. Realizan controles de cambios



Nota. Datos obtenidos del procesamiento en SPSS

Interpretación:

En la tabla 15 y figura 15, se observa que de los encuestados, el 61.5% casi nunca realizan controles de cambios en el sistema de información; el 13.2% a veces; el 11.0% siempre; el 7.7% casi siempre y el 6.6% nunca. Estos resultados evidencian que los cambios en los controles de los sistemas de información de la Universidad Nacional Hermilio Valdizán casi nunca se realizan.

Tabla 16. Validan la información mediante firmas digitales

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Siempre	13	14,3	14,3	14,3
	Casi siempre	10	11,0	11,0	25,3
	A veces	17	18,7	18,7	44,0
	Casi nunca	46	50,5	50,5	94,5
	Nunca	5	5,5	5,5	100,0
	Total	91	100,0	100,0	

Nota. Datos obtenidos del procesamiento en SPSS

Figura 16. Validan la información mediante firmas digitales

Nota. Datos obtenidos del procesamiento en SPSS

Interpretación:

En la tabla 16 y figura 16, se observa que de los encuestados, el 50.5% casi nunca validan la información mediante firmas digitales; el 18.7% a veces; el 14.3% siempre; el 11.0% casi siempre y el 5.5% nunca. Estos resultados evidencian que la validación de información de los sistemas de información de la Universidad Nacional Hermilio Valdizán casi nunca se realiza.

Tabla 17. Realizan una preparación en la gestión de incidentes

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Siempre	19	20,9	20,9	20,9
	Casi siempre	10	11,0	11,0	31,9
	A veces	14	15,4	15,4	47,3
	Casi nunca	47	51,6	51,6	98,9
	Nunca	1	1,1	1,1	100,0
	Total	91	100,0	100,0	

Nota. Datos obtenidos del procesamiento en SPSS

Figura 17. Realizan una preparación en la gestión de incidentes

Nota. Datos obtenidos del procesamiento en SPSS

Interpretación:

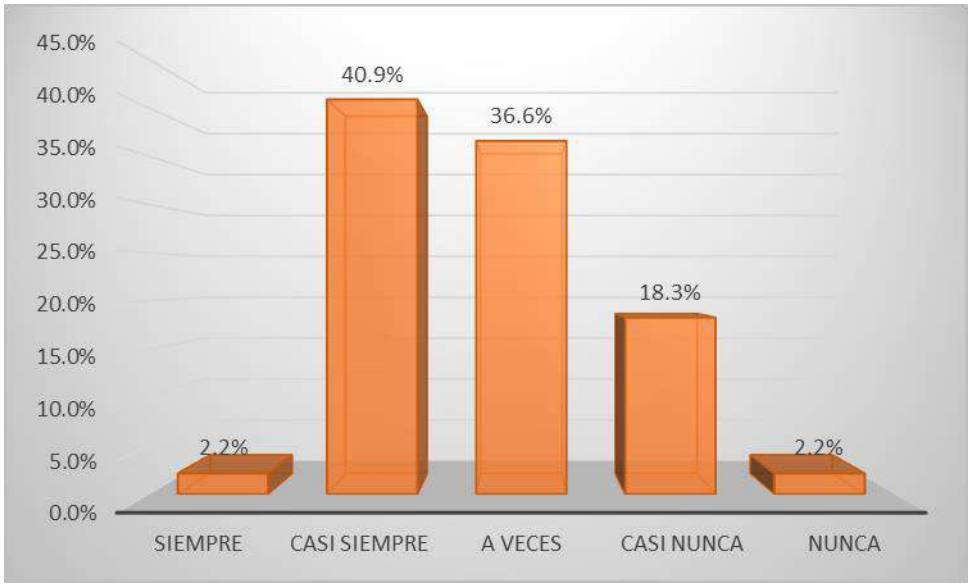
En la tabla 17 y figura 17, se observa que de los encuestados, el 51.6% casi nunca realizan una preparación en la gestión de incidentes; el 20.9% siempre; el 15.4% a veces; el 11.0% casi siempre y el 1.1% nunca. Estos resultados evidencian que la preparación en la gestión de incidentes de los sistemas de información de la Universidad Nacional Hermilio Valdizán casi nunca se realiza.

Tabla 18. Realizan un análisis para detectar incidentes

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Siempre	2	2,2	2,2	2,2
	Casi siempre	38	41,8	41,8	44,0
	A veces	34	37,4	37,4	81,3
	Casi nunca	17	18,7	18,7	100,0
	Nunca	2	2,2	2,2	2,2
	Total	91	100,0	100,0	

Nota. Datos obtenidos del procesamiento en SPSS

Figura 18. Realizan un análisis para detectar incidentes



Nota. Datos obtenidos del procesamiento en SPSS

Interpretación:

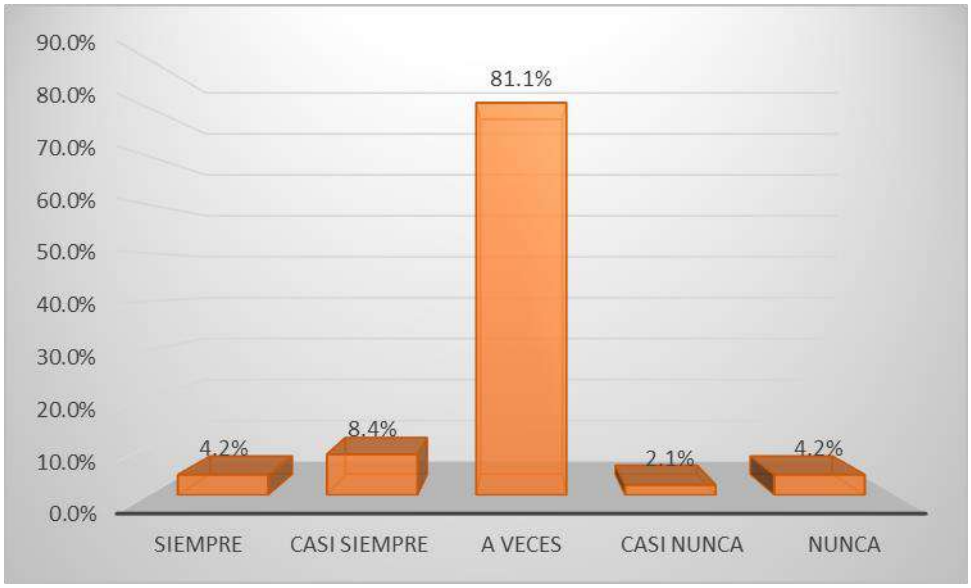
En la tabla 18 y figura 18, se observa que de los encuestados, el 40.9% casi siempre realizan un análisis para detectar incidentes en los sistemas de información; el 36.6% a veces; el 18.3% casi nunca; el 2.2% siempre y el 2.2% nunca. Estos resultados evidencian que el análisis para detectar incidentes de los sistemas de información de la Universidad Nacional Hermilio Valdizán casi siempre y a veces se realiza.

Tabla 19. Realizan actividades de contención, erradicación y recuperación de los sistemas de información ante algún incidente

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Siempre	4	4,4	4,4	4,4
	Casi siempre	8	8,8	8,8	13,2
	A veces	77	84,6	84,6	97,8
	Casi nunca	2	2,2	2,2	100,0
	Nunca	4	4,4	4,4	4,4
	Total	91	100,0	100,0	

Nota. Datos obtenidos del procesamiento en SPSS

Figura 19. Realizan actividades de contención, erradicación y recuperación de los sistemas de información ante algún incidente



Nota. Datos obtenidos del procesamiento en SPSS

Interpretación:

En la tabla 19 y figura 19, se observa que de los encuestados, el 81.1% a veces realizan actividades de contención, erradicación y recuperación de los sistemas de información ante algún incidente; el 8.4% casi siempre; el 4.2% nunca; el 4.2% siempre y el 2.1% casi nunca. Estos resultados evidencian que las actividades de contención, erradicación y recuperación de los sistemas de información de la Universidad Nacional Hermilio Valdizán a veces se realiza.

Tabla 20. Realizan actividades (informes de incidentes, comunicados) después de los incidentes

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Siempre	13	14,3	14,3	14,3
	Casi siempre	10	11,0	11,0	25,3
	A veces	20	22,0	22,0	47,3
	Casi nunca	46	50,5	50,5	97,8
	Nunca	2	2,2	2,2	100,0
	Total	91	100,0	100,0	

Nota. Datos obtenidos del procesamiento en SPSS

Figura 20. Realizan actividades (informes de incidentes, comunicados) después de los incidentes

Nota. Datos obtenidos del procesamiento en SPSS

Interpretación:

En la tabla 20 y figura 20, se observa que de los encuestados, el 50.5% casi nunca realizan actividades (informes de incidentes, comunicados) después de los incidentes; el 22.0% a veces; el 14.3% siempre; el 11.0% casi siempre y el 2.2% nunca. Estos resultados evidencian que las actividades (informes de incidentes, comunicados) después de los incidentes de los sistemas de información de la Universidad Nacional Hermilio Valdizán casi nunca se realiza.

Tabla 21. Escanean vulnerabilidades

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Siempre	13	14,3	14,3	14,3
	Casi siempre	11	12,1	12,1	26,4
	A veces	19	20,9	20,9	47,3
	Casi nunca	46	50,5	50,5	97,8
	Nunca	2	2,2	2,2	100,0
	Total	91	100,0	100,0	

Nota. Datos obtenidos del procesamiento en SPSS

Figura 21. Escanean vulnerabilidades

Nota. Datos obtenidos del procesamiento en SPSS

Interpretación:

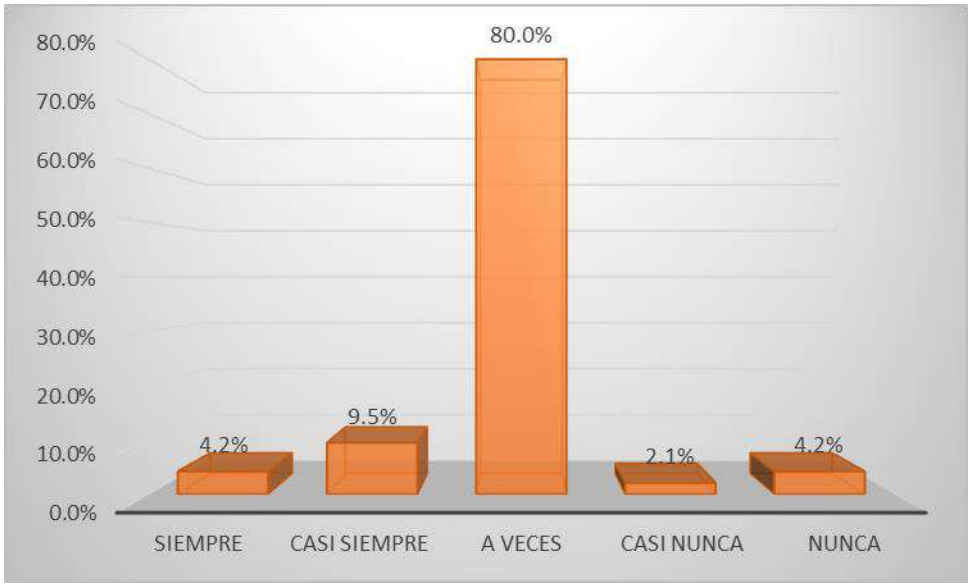
En la tabla 21 y figura 21, se observa que de los encuestados, el 50.5% casi nunca escanean vulnerabilidades; el 20.9% a veces; el 14.3% siempre; el 12.1% casi siempre y el 2.2% nunca. Estos resultados evidencian que las vulnerabilidades de los sistemas de información de la Universidad Nacional Hermilio Valdizán casi nunca se escanean.

Tabla 22. Realizan parches y actualizaciones

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Siempre	4	4,4	4,4	4,4
	Casi siempre	9	9,9	9,9	14,3
	A veces	76	83,5	83,5	97,8
	Casi nunca	2	2,2	2,2	100,0
	Nunca	4	4,4	4,4	4,4
	Total	91	100,0	100,0	

Nota. Datos obtenidos del procesamiento en SPSS

Figura 22. Realizan parches y actualizaciones



Nota. Datos obtenidos del procesamiento en SPSS

Interpretación:

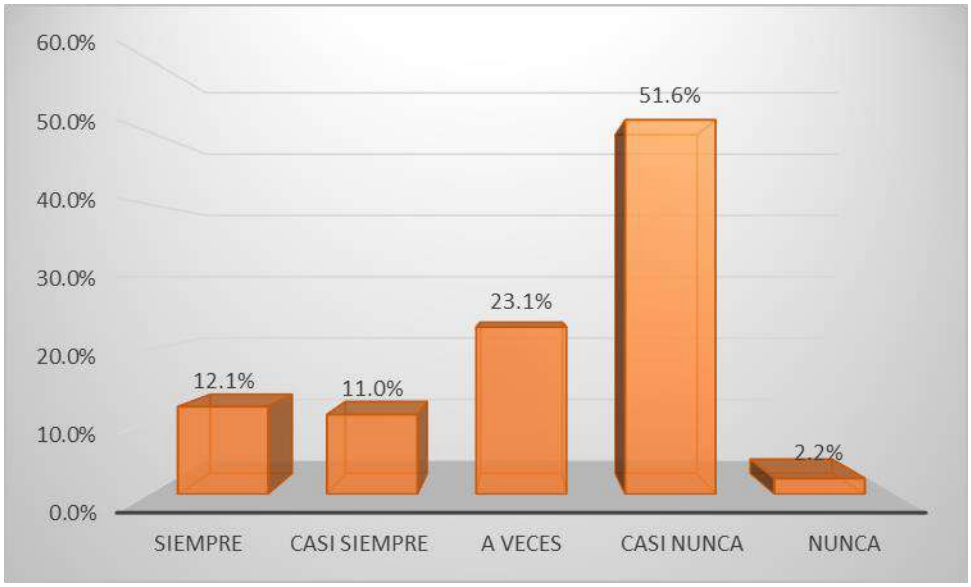
En la tabla 22 y figura 22, se observa que de los encuestados, el 80.0% a veces realizan parches y actualizaciones; el 9.5% casi siempre; el 4.2% siempre; el 4.2% nunca y el 2.1% casi nunca. Estos resultados evidencian que los parches y actualizaciones en los sistemas de información de la Universidad Nacional Hermilio Valdizán a veces se realizan.

Tabla 23. Evalúan las actualizaciones

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Siempre	11	12,1	12,1	12,1
	Casi siempre	10	11,0	11,0	23,1
	A veces	21	23,1	23,1	46,2
	Casi nunca	47	51,6	51,6	97,8
	Nunca	2	2,2	2,2	100,0
	Total	91	100,0	100,0	

Nota. Datos obtenidos del procesamiento en SPSS

Figura 23. Evalúan las actualizaciones



Nota. Datos obtenidos del procesamiento en SPSS

Interpretación:

En la tabla 23 y figura 23, se observa que de los encuestados, el 51.6% casi nunca evalúan actualizaciones; el 23.1% a veces; el 12.1% siempre; el 11.0% casi siempre y el 2.2% nunca. Estos resultados evidencian que las actualizaciones en los sistemas de información de la Universidad Nacional Hermilio Valdizán casi nunca se evalúan.

Tabla 24. Realizan auditorías y revisiones externas

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Siempre	13	14,3	14,3	14,3
	Casi siempre	9	9,9	9,9	24,2
	A veces	18	19,8	19,8	44,0
	Casi nunca	48	52,7	52,7	96,7
	Nunca	3	3,3	3,3	100,0
	Total	91	100,0	100,0	

Nota. Datos obtenidos del procesamiento en SPSS

Figura 24. Realizan auditorías y revisiones externas

Nota. Datos obtenidos del procesamiento en SPSS

Interpretación:

En la tabla 24 y figura 24, se observa que de los encuestados, el 52.7% casi nunca realizan auditorías y revisiones externas; el 19.8% a veces; el 14.3% siempre; el 9.9% casi siempre y el 3.3% nunca. Estos resultados evidencian que las auditorias y revisiones externas en los sistemas de información de la Universidad Nacional Hermilio Valdizán casi nunca se realizan.

Cuadro 1. Requerimientos de seguridad de los sistemas de información en la UNHEVAL.

Confidencialidad	Proteger las conexiones de autenticidad.
	Evitar dar accesos de privilegios en las cuentas de usuarios.
	Evitar mostrar referencias hacia objetos internos de la aplicación.
	Evitar almacenar datos sensibles de manera innecesaria.
	Deshabilitar el almacenamiento en caché de datos sensibles.
Integridad	Utilizar software que previenen automáticamente los ataques a los servidores de la universidad.
	Validar los datos entrantes y salvaguardar la integridad de los datos que se devuelven.
	Prevenir los ataques CSRF (del inglés Cross-Site Request Forgery o falsificación de petición en sitios cruzados).
	Evitar las inyecciones de código.
	Utilizar LIMIT y otros controles SQL para evitar la fuga masiva de datos en caso de inyecciones SQL.
Disponibilidad	Realizar estudio sobre las posibles vulnerabilidades que se puedan presentar en la tecnología utilizada.
	Utilizar tecnologías seguras para el desarrollo.
	Cumplir los requisitos exclusivos de los límites de negocio de las aplicaciones.
	Utilizar una herramienta para mantener un inventario y control de versiones de los componentes.
	Utilizar componentes únicamente de orígenes oficiales y utilizar canales seguros.
No repudio	Identificar o firmar de forma única los mensajes intercambiados.

	Cifrar todos los datos en tránsito utilizando protocolos seguros.
Autenticidad	Evitar mantener credenciales creadas por defecto, débiles o muy conocidas especialmente en el caso de los administradores del sistema.
	Definir mecanismos de autenticación personalizado para todos los usuarios del sistema.
	Evitar utilizar cuentas suministradas por defecto.
	Evitar ataques de fuerza bruta y/o ataques automatizados.
	Utilizar controles contra contraseñas débiles.

Nota. Elaboración propia

Cuadro 2. Vulnerabilidades de la infraestructura a los que están expuestos los sistemas de información de la UNHEVAL

Vulnerabilidades de la infraestructura	Descripción
Desactualización de software	Los sistemas operativos, el software y las herramientas obsoletos pueden incluir vulnerabilidades bien conocidas que pueden ser explotadas por personas malintencionadas. Descuidar la aplicación de parches y actualizaciones de seguridad puede dejar la infraestructura vulnerable a posibles amenazas.
Configuraciones inseguras	Las configuraciones erróneas o inseguras de servidores, bases de datos y otros componentes de la infraestructura pueden dar lugar a vulnerabilidades. El acceso no autorizado puede facilitarse accediendo a configuraciones por defecto o utilizando contraseñas débiles.
Falta de encriptación	La transmisión de datos sensibles a través de la red sin cifrado puede exponer potencialmente la información a la interceptación. Un uso insuficiente del cifrado en la transmisión de información entre sistemas podría poner en peligro la confidencialidad de los datos.
Acceso no autorizado	Los controles de acceso insuficientes, como la ausencia de autenticación multifactor y de restricciones de mínimo privilegio, pueden dar lugar a la entrada ilegal en sistemas vitales. Los individuos que poseen derechos superfluos pueden suponer un peligro sustancial.
Fallos en la gestión de identidad	Los problemas de gestión de identidades, como las cuentas de usuario inactivas, el uso compartido de contraseñas o la mala gestión de las transiciones laborales, pueden crear vulnerabilidades ante riesgos tanto internos como externos.

Ataques de inyección	Las aplicaciones y bases de datos susceptibles de ataques de inyección, como SQL o XSS, pueden ser objeto de abusos malintencionados para obtener acceso no autorizado a los datos almacenados o modificarlos.
Falta de respaldo y recuperación	La aplicación inadecuada de protocolos de copia de seguridad y recuperación puede aumentar la susceptibilidad a la pérdida de datos como consecuencia de sucesos como ataques de ransomware o fallos de hardware.

Nota. Elaboración propia

Cuadro 3. Plan y estrategia de mejora en la seguridad de los sistemas de información de la UNHEVAL.

Variable	Dimensiones	Problema encontrado	Propuesta de mejora	Responsable
Metodología Octave	Requerimientos de seguridad	No se identifica los activos de los sistemas de información. No se clasifica los activos de los sistemas de información. No se identifica los riesgos de los sistemas de información. No se identifica las defensas de los sistemas de información. No se identifica las necesidades de seguridad.	Los administradores en base a la asesoría de los ingenieros deben identificar y clasificar los activos. Los ingenieros deben identificar los riesgos de los sistemas de información y deben identificar las defensas y necesidades de seguridad que se encuentren. Todo ello se debe basar a los requerimientos de seguridad.	Ingeniero de sistemas y coordinador de los sistemas de información.
	Vulnerabilidades de la infraestructura	No se identifica vulnerabilidades en el sistema de información. No se evalúa vulnerabilidades en el sistema de información. No se analiza vulnerabilidades en el sistema de información. No se prioriza las vulnerabilidades en el sistema de información.	Los administradores en base a la asesoría de los ingenieros deben identificar, evaluar y analizar las vulnerabilidades dentro del sistema de información. Además, se debe priorizar las vulnerabilidades encontradas mediante en seguimiento de los requerimientos.	Ingeniero de sistemas y coordinador de los sistemas de información.
	Plan y estrategia de seguridad	No se identifica los riesgos de información. No se realiza controles de seguridad. No hay integración de controles.	Los administradores en base a la asesoría de los ingenieros deben identificar los riesgos y realizar controles de seguridad mediante la integración de los controles cada semana; para salvaguardar la información; además ello debe	Ingeniero de sistemas y coordinador de los sistemas de información.

			regirse a base de los requerimientos identificados.	
Seguridad de los Sistemas de Información	Confidencialidad e integridad	No realizan controles de acceso. No realizan encriptaciones a la información. No realizan controles de cambios. No validan la información mediante firmas digitales.	Los administradores en base a la asesoría de los ingenieros deben realizar controles de acceso a los usuarios; además la información ingresada debe ser encriptada y la información importante deben regirse a la validación mediante firmas digitales; además ello debe regirse a base de los requerimientos identificados.	Ingeniero de sistemas y coordinador de los sistemas de información.
	Gestión de incidentes	No realizan una preparación en la gestión de incidentes No realizan un análisis para detectar incidentes No realizan actividades de contención, erradicación y recuperación de los sistemas de información ante algún incidente No realizan actividades (informes de incidentes, comunicados) después de los incidentes.	Los administradores en base a la asesoría de los ingenieros deben realizar una preparación en la gestión de incidentes y un análisis. Se debe realizar actividades de contención e informes de los incidentes presentados, rigiéndose de los requerimientos identificados.	Ingeniero de sistemas y coordinador de los sistemas de información.
	Gestión de vulnerabilidades	No se prioriza las vulnerabilidades en el sistema de información. Se identifica los riesgos de información.	Los ingenieros deben priorizar las vulnerabilidades e identificar los riesgos de los sistemas de información, siguiendo los requerimientos.	Ingeniero de sistemas y coordinador de los sistemas de información.
	Cumplimiento legal y regulatorio	No se realiza controles de seguridad. No hay integración de controles.	Los ingenieros deben integrar controles para realizar un análisis de seguridad mediante los requerimientos.	Ingeniero de sistemas y coordinador de los sistemas de información.

4.2 Resultados inferenciales

Tabla 25. Prueba de normalidad

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Metodología Octave	,147	91	,000	,912	91	,000
Seguridad de los Sistemas de Información	,170	91	,000	,888	91	,000

a. Corrección de significación de Lilliefors

Interpretación:

En la tabla 25, se evidencia en el estadístico Kolmogorov-Smirnov, que el valor del sig. resultó igual a 0.000 y 0.000 respectivamente de cada variable, estos valores son menores a 0.05 por tanto indica que los datos presentan una distribución no paramétrica; en consecuencia, se utilizará el estadístico de hipótesis Spearman, lo cual es el indicado para medir correlaciones con datos que provienen de una distribución no paramétrica.

De acuerdo con la hipótesis general

Hi: Existe relación estadísticamente significativa entre la Metodología Octave y la seguridad de los Sistemas de Información de la Universidad Nacional Hermilio Valdizán, Huánuco, 2023.

Ho: No existe relación estadísticamente significativa entre la Metodología Octave y la seguridad de los Sistemas de Información de la Universidad Nacional Hermilio Valdizán, Huánuco, 2023.

Tabla 26. Correlación de Spearman de la hipótesis general

Correlaciones

			Metodología Octave	Seguridad de los Sistemas de Información
Rho de Spearman	Metodología Octave	Coeficiente de correlación	1,000	,979**
		Sig. (bilateral)	.	,000
		N	91	91
	Seguridad de los Sistemas de Información	Coeficiente de correlación	,979**	1,000
		Sig. (bilateral)	,000	.
		N	91	91

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

Análisis e interpretación

El coeficiente de correlación fue de 0,979, la cual indica que existe una relación positiva muy fuerte; además el sig. obtenido fue de 0.000 menor al error permitido de 0.05, la cual establece que la relación encontrada es significativa; por ello se rechaza la hipótesis nula y se acepta la hipótesis de investigación; indicando que, existe relación estadísticamente significativa entre la Metodología Octave y la seguridad de los Sistemas de Información de la Universidad Nacional Hermilio Valdizán, Huánuco, 2023.

De acuerdo con la hipótesis específica 1

Hi1: Los requerimientos de seguridad con la metodología Octave se relacionan significativamente con la seguridad de los sistemas de información de la UNHEVAL, Huánuco, 2023.

Ho1: Los requerimientos de seguridad con la metodología Octave no se relacionan significativamente con la seguridad de los sistemas de información de la UNHEVAL, Huánuco, 2023.

Tabla 27. Correlación de Spearman de la hipótesis específica 1

Correlaciones

			Requerimientos de seguridad	Seguridad de los sistemas de información
Rho de Spearman	Requerimientos de seguridad	Coeficiente de correlación	1,000	,857**
		Sig. (bilateral)	.	,000
		N	91	91
	Seguridad de los sistemas de información	Coeficiente de correlación	,857**	1,000
		Sig. (bilateral)	,000	.
		N	91	91

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

Análisis e interpretación

El coeficiente de correlación fue de 0,857, la cual indica que existe una relación positiva muy fuerte; además el sig. obtenido fue de 0.000 menor al error permitido de 0.05, la cual establece que la existe una relación significativa; por ello se rechaza la hipótesis nula y se acepta la hipótesis de investigación; indicando que, los requerimientos de seguridad con la metodología Octave se relacionan significativamente con la seguridad de los sistemas de información de la UNHEVAL, Huánuco, 2023.

De acuerdo con la hipótesis específica 2

Hi2: La identificación de las vulnerabilidades de la infraestructura con la metodología Octave se relacionan significativamente con la seguridad de los sistemas de información de la UNHEVAL, Huánuco, 2023.

Ho2: La identificación de las vulnerabilidades de la infraestructura con la metodología Octave no se relacionan significativamente con la seguridad de los sistemas de información de la UNHEVAL, Huánuco, 2023.

Tabla 28. Correlación de Spearman de la hipótesis específica 2

Correlaciones

			Vulnerabilidades de la infraestructura	Seguridad de los sistemas de información
Rho de Spearman	Vulnerabilidades de la infraestructura	Coeficiente de correlación	1,000	,915**
		Sig. (bilateral)	.	,000
		N	91	91
	Seguridad de los sistemas de información	Coeficiente de correlación	,915**	1,000
		Sig. (bilateral)	,000	.
		N	91	91

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

Análisis e interpretación

El coeficiente de correlación fue de 0,915, la cual indica que existe una relación positiva muy fuerte; además el sig. obtenido fue de 0.000 menor al error permitido de 0.05, la cual establece que la existe una relación significativa; por ello se rechaza la hipótesis nula y se acepta la hipótesis de investigación; indicando que, la identificación de las vulnerabilidades de la infraestructura con la metodología Octave se relacionan significativamente con la seguridad de los sistemas de información de la UNHEVAL, Huánuco, 2023.

De acuerdo con la hipótesis específica 3

Hi3: El establecimiento de un plan y estrategia mejora significativamente la seguridad de los sistemas de información de la UNHEVAL, Huánuco, 2023.

Ho3: El establecimiento de un plan y estrategia no mejora significativamente la seguridad de los sistemas de información de la UNHEVAL, Huánuco, 2023.

Análisis e interpretación

El plan y estrategia de mejora evidenciado en el cuadro 3, muestra los problemas identificados en las dimensiones de ambas variables, los cuales se identificaron mediante el análisis de la encuesta; por lo que, se propone mejorar las debilidades identificadas en el uso de la metodología Octave y la seguridad de los sistemas de información mediante la incorporación de un personal capacitado para coordinar los requerimientos de vulnerabilidades y estrategias que se relacionen con los sistemas de información de la Universidad Nacional Hermilio Valdizán. Esto demuestra que, utilizar adecuada y oportunamente la metodología Octave permite mejorar la seguridad de los sistemas de información. Por ello se rechaza la hipótesis nula y se acepta la hipótesis especifica 3, indicando que el establecimiento de un plan y estrategia mejora significativamente la seguridad de los sistemas de información de la UNHEVAL, Huánuco, 2023.

CAPÍTULO V. DISCUSIÓN

Los resultados de acuerdo a la metodología OCTAVE indicaron que el 84.6% casi nunca identifica activos de los sistemas de información; el 50.5% casi nunca clasifican los activos de los sistemas de información; el 50.5% casi nunca identifican los riesgos de los sistemas de información; el 83.5% casi nunca identifican las defensas de los sistemas de información; el 51.6% casi nunca identifican las necesidades de seguridad de los sistemas de información; el 52.7% casi nunca identifican vulnerabilidades en el sistema de información; el 50.5% casi nunca evalúan vulnerabilidades en el sistema de información; el 61.5% casi nunca analiza vulnerabilidades en el sistema de información; el 50.5% casi nunca se prioriza las vulnerabilidades en el sistema de información; el 51.6% casi nunca identifican los riesgos en el sistema de información; el 40.9% casi siempre realizan controles de seguridad en el sistema de información y el 53.8% casi nunca hay integraciones de controles en el sistema de información. Evidenciándose que en los sistemas de información de la UNHEVAL no aplican correctamente la metodología OCTAVE al momento de identificar requerimientos de seguridad, vulnerabilidades de infraestructura de datos y estrategias de seguridad. Estos resultados no cumplen con adoptar una metodología adecuada por lo que Campos y León (2020) indican que la técnica OCTAVE adopta un enfoque de nivel corporativo para su proceso, que evalúa las numerosas Fases, Procedimientos y Actividades que componen un Sistema de Gestión de Riesgos Informáticos. La primera etapa, "construcción del perfil de amenazas basado en los activos", implica establecer criterios de evaluación del impacto, identificar los activos de la organización y evaluar las prácticas de seguridad de la organización, entre otras cosas; y seleccionar los activos críticos, identificar los requisitos de seguridad para los activos críticos e identificar las amenazas a los activos críticos, entre otras cosas, para crear el perfil de amenazas. En la segunda fase, se buscarán puntos débiles en la infraestructura informática, revisando las operaciones relacionadas con la tecnología y estudiando las vías de acceso a los recursos críticos. En la tercera y última etapa, desarrollará estrategias y planes de seguridad, incluyendo pasos como: identificar y analizar los riesgos mediante acciones como: determinar la gravedad de las amenazas; crear criterios para evaluar la probabilidad de eventos

adversos; y sopesar los riesgos relativos de varios escenarios. Planifique los peligros potenciales mediante acciones como la descripción de su estrategia de protección actual y la elección de métodos de mitigación.

Por otro lado, los resultados según la seguridad de los sistemas de información de la UNHEVAL indicaron que, el 52.7% casi nunca realizan controles de acceso en el sistema de información; el 50.5% casi nunca realizan encriptaciones a la información; el 61.5% casi nunca realizan controles de cambios en el sistema de información; el 50.5% casi nunca validan la información mediante firmas digitales; el 51.6% casi nunca realizan una preparación en la gestión de incidentes; el 40.9% casi siempre realizan un análisis para detectar incidentes en los sistemas de información; el 81.1% a veces realizan actividades de contención, erradicación y recuperación de los sistemas de información ante algún incidente; el 50.5% casi nunca realizan actividades (informes de incidentes, comunicados) después de los incidentes; el 50.5% casi nunca escanean vulnerabilidades; el 80.0% a veces realizan parches y actualizaciones; el 51.6% casi nunca evalúan actualizaciones y el 52.7% casi nunca realizan auditorías y revisiones externas; estos resultados indican que la seguridad de los sistemas de información no están implementadas adecuadamente; ello indica que existe una relación entre el uso de la metodología OCTAVE y la seguridad de los sistemas de información; ello se aprecia en el coeficiente de correlación que fue de 0,979, la cual indica que existe una relación positiva muy fuerte; además el sig. obtenido fue de 0.000 menor al error permitido de 0.05, la cual establece que la relación encontrada es significativa. Además, se aprecia que los involucrados en los sistemas de información de la Universidad Nacional Hermilio Valdizán no aplican correctamente la metodología Octave por lo que la seguridad de los sistemas de información es vulnerable antes los hackers. Al respecto Rivera y Valdivia (2021) indican que la verificación del nivel de cumplimiento de las salvaguardas reduce el nivel de impacto de los activos informáticos; por lo que se interpreta que el correcto uso de metodologías como el OCTAVE benefician la seguridad e integridad de los sistemas de información.

CONCLUSIONES

De acuerdo con el objetivo general

Se determinó la relación que existe entre la Metodología Octave y la seguridad de los sistemas de información de la Universidad Nacional Hermilio Valdizán, Huánuco, 2023. Se obtuvo un coeficiente de correlación de 0,979, la cual indica que existe una relación positiva muy fuerte; además el sig. obtenido fue de 0.000 menor al error permitido de 0.05, la cual establece que la relación encontrada es significativa; ello indica que la aplicación correcta la metodología OCTAVE mejora la seguridad de los sistemas de información y si esta no se aplica correctamente vulnera la seguridad de la información.

De acuerdo con el objetivo específico 1

Se estableció los requerimientos de seguridad de los sistemas de información de la UNHEVAL con la metodología Octave, siendo estos requerimientos que se basan en la confidencialidad, integridad, disponibilidad, no repudio y autenticidad (Ver cuadro 1). Además, se obtuvo un coeficiente de correlación de 0,857, la cual indica que existe una relación positiva muy fuerte; además el sig. obtenido fue de 0.000 menor al error permitido de 0.05, la cual establece que la existe una relación significativa; por ello se afirma que. los requerimientos de seguridad con la metodología Octave se relacionan significativamente con la seguridad de los sistemas de información de la UNHEVAL, Huánuco, 2023.

De acuerdo con el objetivo específico 2

Se identificó las vulnerabilidades de la infraestructura con la metodología Octave a los que están expuestos los sistemas de información de la UNHEVAL, donde las vulnerabilidades que más se puedan presentar son: Desactualización de software, configuraciones inseguras, falta de encriptación, acceso no autorizado, fallos en la gestión de identidad, ataques de inyección, falta de respaldo y recuperación (Ver cuadro 2). Además, se obtuvo un coeficiente de correlación de 0,915, la cual indica que existe una relación positiva muy fuerte; además el sig. obtenido fue de 0.000 menor al error permitido de 0.05, la cual establece que la existe una relación

significativa; por ello se afirma que, la identificación de las vulnerabilidades de la infraestructura con la metodología Octave se relacionan significativamente con la seguridad de los sistemas de información de la UNHEVAL, Huánuco, 2023.

De acuerdo con el objetivo específico 3

Se estableció un plan y estrategia de mejora en la seguridad de los sistemas de información de la UNHEVAL, Huánuco, 2023. En lo cual se ha identificado los problemas a nivel de la metodología OCTAVE y la seguridad de los sistemas de información, donde se propuso que personales capacitados como los ingenieros de sistemas ayuden a los administrativos a verificar funciones básicas de seguridad como la identificación de vulnerabilidades y reportarlo oportunamente (Ver cuadro 3).

RECOMENDACIONES O SUGERENCIAS

Asegurar el compromiso y apoyo activo de la alta dirección de la UNHEVAL; ya que la implementación de la metodología OCTAVE requiere recursos y liderazgo para garantizar una evaluación efectiva y la aplicación de medidas de seguridad recomendadas.

Formar un equipo multidisciplinario que incluya representantes de TICs, seguridad de la información y gestión de riesgos para garantizará una evaluación integral.

Establecer un alcance claro y bien definido para la evaluación OCTAVE. Esto incluye identificar los activos críticos, las amenazas relevantes y los límites específicos del sistema o procesos a evaluar.

Realizar un inventario exhaustivo de los activos críticos de información de la UNHEVAL, incluyendo datos, sistemas, redes y procesos fundamentales para sus operaciones.

Identificar y evaluar las amenazas específicas que podrían afectar a los activos críticos. Esto incluye amenazas tanto internas como externas, y considerar escenarios de riesgo realistas.

REFERENCIAS BIBLIOGRÁFICAS

Abanto, C., & Rivera, J. (2022). *Propuesta de un modelo de sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 para la Sede Central del Gobierno Regional de Huánuco – 2022.* [Tesis de pregrado, Universidad Nacional Hermilio Valdizán] Repositorio UNHEVAL. doi:20.500.13080/8032

Álvarez, E., & Silva, O. (2019). *Auditoría Informática aplicando la metodología OCTAVE de los procesos de recaudaciones y permisos en el Gobierno Autónomo Descentralizado (GAD) de San Pedro de Pelileo.* [Tesis de pregrado, Universidad Tecnica de Ambato] Repiositorio institucional UTA. Obtenido de https://repositorio.uta.edu.ec/handle/123456789/30111

Alzórriz, I. (2014). *Procesos y herramientas para la seguridad de redes.* UNED - Universidad Nacional de Educación a Distancia. Obtenido de https://elibro.net

Arevalo, F., Cortez, A., Ordoñez, I., & Solís, J. (2020). Importancia de la seguridad en los Sistemas de Información. *POCAIP, 5*(20), 136-144. doi:10.23857/fipcaec.v5i5.285

Arias, F. (2006). *El proyecto de investigación* (6.a ed.). Episteme. Obtenido de https://www.researchgate.net/publication/301894369_el_proyecto_de_investigacion_6a_edicion

Barraza, J. (2021). *Sistema de gestión de la seguridad de la información en las pequeñas y medianas empresas.* [Tesis de pregrado, Universidad de Cartagena] Repositorio UNICARTAGENA. doi:11227/15043

Barría, C. (2020). *Nuevos espacios de seguridad nacional: Cómo proteger la información en el ciberespacio.* Editorial ebooks Patagonia - Ediciones UM. Obtenido de https://elibro.net

Bunge, M. (2004). *La Investigación Científica su Estrategia y su Filisofía.* México: Siglo XXI Editores.

Campos, C., & León, D. (2020). *Comparativa de las metodologías Magerit y Octave, para determinar la más adecuada en la gestión de riesgos de tecnologías de información en la Unidad de Red Telemática de la Universidad Nacional Pedro Ruiz Gallo.* [Tesis de pregrado, Universidad Nacional Pedro Ruiz Gallo] Repositorio UNPRG. doi:20.500.12893/8244

Carvajal, C. (2019). La encriptación de datos empresariales: ventajas y desventajas. *Mundo de investigación el conocimiento, 3*(2), 980-997. Obtenido de https://recimundo.com/index.php/es/article/view/487/630

Díaz, H. (2018). Implementación de la metodología Octave para el diagnóstico seguridad informática. *Universidad Autónoma de Baja California, II*, 9. Obtenido de http://fcqi.tij.uabc.mx/usuarios/revistaaristas/numeros/N12/articulos/56-64.pdf

El peruano. (2021). *Decreto Legislativo N° 1412, que aprueba la ley de gobierbno digital*. Obtenido de https://cdn.www.gob.pe/uploads/document/file/1680865/DS%20029-2021-PCM.pdf.pdf?v=1643322501

Enrique, L. (3 de Abril de 2023). *Cómo elaborar e implementar un plan de mitigación*. Recuperado el 12 de Agosto de 2023, de https://leadcareillinois.org/es/como-elaborar-e-implementar-un-plan-de-mitigacion/

Esteban, G., & Pacienzia, J. (2015). *Metodologías de desarrollo de software.* [Tesis de pregrado, Pontificia Universidad Católica Argentina] Repositorio institucional PUC. Obtenido de https://repositorio.uca.edu.ar/bitstream/123456789/522/1/metodologias-desarrollo-software.pdf

Fuentes, F., Castro, D., & Nájera, L. (2018). *Investigación metodológica Octave.* [Tesis de posgrado, Universidad Fidelitas] Repositorio UFIDELITA. doi:426111802

García, J., & Huamani, S. (2019). *Modelo de gestión de riesgos de seguridad de la información para pymes en el Perú.* [Tesis de pregrado, Universidad Peruana de Ciencias Aplicables] Repositorio institucional UPC. Obtenido de https://repositorioacademico.upc.edu.pe/handle/10757/625905

Gigant, N. (2016). *Ciber seguridad para la i-generación: usos y riesgos de las redes y sus aplicaciones.* Narcea Ediciones. Obtenido de https://elibro.net

Guerra, E. (2020). *Sistema de gestión para la seguridad de la información basado en metodología de identificación y análisis de riesgo en la biblioteca de la universidad de la Costa.* [Tesis de posgrado, Universidad de la Costa] Repositorio CUC. doi:11323/7436

Gutierrez, A. (5 de Abril de 2019). *Actualizaciones de software: qué son, para qué sirven, cuándo instalarlas*. Recuperado el 12 de Agosto de 2023, de https://www.idearius.com/es/blog/actualizaciones-de-software-que-son-para-que-sirven-cuando-instalarlas/

Gutiérrez, N. (22 de Febrero de 2022). *30 Estadísticas Importantes de Seguridad Informática (2022)*. Recuperado el 2 de Agosto de 2023, de https://preyproject.com/es/blog/30-estadisticas-seguridad-informatica

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. d. (2017). *Metodología de la investigación* (Vol. 6ta Edición). México: McGRAW-HILL/INTERAMERCIANA EDITORES S.A.

Hernández, M. (2020). *Ciclo de vida de desarrollo ágil de software seguro.* Fundación Universitaria Los Libertadores. Obtenido de https://elibro.net

Hernández, R., & Mendoza, C. (2018). *Metodológia de la Investigación: Las rutas cuantitativa, cualitativa y mixta.* McGraw-Hill / Interamericana Editores.

Hincapie, A. (2018). *La calidad del dato en los sistemas de información de convivencia y seguridad ciudadana.* Programa Editorial Universidad del Valle. Obtenido de https://elibro.net

Hurtado, M. (2021). Gestión de riesgo metodologías OCTAVE y MAGERIT. *Universidad Piloto de Colombia, II*(3), 12. Obtenido de http://polux.unipiloto.edu.co:8080/00004420.pdf

Inoguchi, A., & Macha, E. (2017). *Gestión de la ciberseguridad y prevención de los ataques cibernéticos en las PYMES del Perú.* [Tesis de pregrado, Universidad San Ignacio de Loyola] Repositorio institucional USIL. Obtenido de https://repositorio.usil.edu.pe/entities/publication/9449a061-bfd2-4ecc-8cf1-770fba7cee45

Llauce, L. (2022). *Análisis comparativo de metodologías de gestión de riesgos de tecnologías de la Información en el marco de la NTP - ISO/IEC 27001:2014.* [Tesis de posgrado, Universidad Nacional Pedro Ruiz Gallo] Repositorio UNPRG. doi:20.500.12893/10411

López, D., & Vásquez, S. (2016). *Comparación entre metodologías de gestión de riesgo informático.* [Tesis de pregrado, Universidad de Azuay] Repositorio UAZUAY. doi:5391/1/11751

Martinez, C. (2020). *Confidencialidad, integridad y disponibilidad*. Obtenido de https://es.linkedin.com/pulse/confidencialidad-integridad-y-disponibilidad-martinez-ramirez

Molina, J. (2000). *Seguridad de la información criptología.* El cid editor. Obtenido de https://elibro.net

Muñoz, A. (2020). *Un Enfoque en la Protección de Sistemas de Agentes.* [Tesis de pregrado, Universidad de Málaga Repositorio institucional UDM. Obtenido de http://anto.t2v.com/documentos/Tesis.pdf

Pacheco, A., Suarez, L., & Gonzáles, J. (2021). Aplicar la Metodología OCTAVE de Identifiacación de Amenazas y Vulnerabilidades en una Entidad Bancaria. *Departamento de Ingenieria de Sistemas y Computación Universidad de los Andes*, 13. Obtenido de https://proyectosmaestrias.virtual.uniandes.edu.co/images/mlC4bCJ5XSVNmWQUD6uN4V2gJFMiZDbyVCkn22QE.pdf

Pert, C. (2 de Agosto de 2023). *Auditorías del IRS*. Obtenido de https://www.irs.gov/es/businesses/small-businesses-self-employed/irs-audits

RENIEC. (2015). *Identidad digital. La identificación desde los registros parroquiales al DNI electrónico.* PUNTO Y GRAFIA S.A.C.

Rivera, D., & Valdivia, J. (2021). *Implementación de la metodología Octave para mejorar la gestión de riesgos de Seguridad de la Información y propuesta de políticas de seguridad en la Dirección Regional de Trabajo y Promoción del Empleo.* [Tesis de

pregrado, Universidad Nacional Hermilio Valdizan] Repositorio institucional UNHEVAL. Obtenido de https://repositorio.unheval.edu.pe/handle/20.500.13080/7066

Rodríguez, J. (2023). *Propuesta de un modelo de mejora continua para la gestión de riesgos de la seguridad de la información a una institución educativa privada mediante el ciclo CAP-Do.* [Tesis de pregrado, Universidad Estatal Península de Santa Elena] Repositorio UPSE. doi:46000/9273

Rubiano, C. (2018). Como ayudar a preparar la entidad, ante la posible perdida de informacion. *UNI Piloto de Colomia*, 2-12. Obtenido de http://repository.unipiloto.edu.co/handle/20.500.12277/8624

Saeckel, A. (2023). *Gestión de la vulnerabilidad en el contexto de la norma ISO 27001*. Obtenido de https://www.dqsglobal.com/es-ar/aprenda/blog/gestion-de-la-vulnerabilidad-en-el-contexto-de-la-norma-iso-27001

Sánchez, H., & Reyes, C. (2015). *Metodología y diseños en la investigación científica* (5.a ed.). Business Support Anneth SRL. Obtenido de https://www.academia.edu/78002369/METODOLOG%C3%8DA_Y_DISE%C3%91OS_EN_LA_INVESTIGACI%C3%93N_CIENT%C3%8DFICA

Santos, J. (8 de Agosto de 2023). *¿Qué es una vulnerabilidad informática y cómo protegerse?* Recuperado el 12 de Agosto de 2023, de https://www.deltaprotect.com/blog/vulnerabilidad-informatica

Segura, M. (2022). *Diseño de un sistema de gestión de seguridad de la información: caso de estudio universidad nacional intercultural FAbiola Salazar Leguía.* [Tesis de pregrado, Universidad Señor de Sipán] Repositorio USS. doi:20.500.12802/10186

Tavosnanska, N. (2011). *Seguridad y política criminal.* Ediciones Cathedra Jurídica. Obtenido de https://elibro.net

Terrell, K. (7 de Abril de 2022). *El fraude de identidad afectó a 42 millones de personas en el 2021*. Recuperado el 6 de Agosto de 2023, de https://www.aarp.org/espanol/dinero/estafas-y-fraudes/info-2022/reporte-javelin-afectados-por-robo-de-identidad.html

Torres, S., & Rojas, J. (2017). *Modelo de gestión de riesgos aplicando metodología OCTAVE Allegro en entidades del sector Fiduciario.* [Tesis de pregrado, Universidad Distrital Francisco José de Caldas Facultad Técnológica] Repositorio UDISTRITAL. doi:11349/6607

Vara, A. (2012). *Desde la idea hasta la sustentación: 7 pasos para una tesis exitosa* (tercera ed.). Lima, Perú: USMP. doi:www.aristidesvara.net

Villadeza, K., & Condor, R. (2022). *Diseño de un sistema de gestión de seguridad de la información basado en la norma técnica peruana -ISO/IEC 27001:2014 para la Municipalidad Distrital de Huácar 2022.* [Tesis de pregrado, Universidad Nacional Hermilio Validizán] Repositorio UNHEVAL. doi:20.500.13080/8238

Villaverde, H. (2021). *Implementación de una gestión de riesgos de TI para mejorar la seguridad de la información de una empresa de agencia publicitaria - 2021.* [Tesis de pregrado, Universidad Tecnológica del Perú] Repositorio institucional UTP. Obtenido de https://repositorio.utp.edu.pe/handle/20.500.12867/5529

Voutssas, J. (2010). Preservación documental digital y seguridad informática. *Centro Universitario de Investigaciones Bibliotecológicas de la UNAM, 24*(50), 127-155. Obtenido de https://www.scielo.org.mx/pdf/ib/v24n50/v24n50a8.pdf

ANEXOS

Anexo 01: Matriz de consistencia

Formulación del problema	Objetivos	Hipótesis	Variables	Dimensiones	Indicadores	Metodología
General: ¿Cuál es la relación entre la Metodología Octave y la seguridad de los sistemas de información de la Universidad Nacional Hermilio Valdizán, Huánuco, 2023? **Específicos:** • ¿De qué manera se establecerá los requerimientos de seguridad de los sistemas de información de la UNHEVAL, Huánuco, 2023? • ¿De qué manera se identificará las vulnerabilidades de la infraestructura a los que están expuestos los sistemas de información de la UNHEVAL, Huánuco, 2023? • ¿De qué manera se establecerá un plan y estrategia de mejora para la seguridad de los sistemas de información de la UNHEVAL, Huánuco, 2023?	**General:** Determinar la relación que existe entre la Metodología Octave y la seguridad de los sistemas de información de la Universidad Nacional Hermilio Valdizán, Huánuco, 2023. **Específicos:** • Establecer los requerimientos de seguridad con la metodología Octave y su relación con la seguridad de los sistemas de información de la UNHEVAL, Huánuco, 2023. • Identificar las vulnerabilidades de la infraestructura con la metodología Octave y su relación con la seguridad de los sistemas de información de la UNHEVAL, Huánuco, 2023. • Establecer un plan y estrategia de mejora para la seguridad de los sistemas de información de la UNHEVAL, Huánuco, 2023.	**General:** **Hi:** Existe relación estadísticamente significativa entre la Metodología Octave y la seguridad de los Sistemas de Información de la Universidad Nacional Hermilio Valdizán, Huánuco, 2023. **Ho:** No existe relación estadísticamente significativa entre la Metodología Octave y la seguridad de los Sistemas de Información de la Universidad Nacional Hermilio Valdizán, Huánuco, 2023. **Especificas:** **Hi1:** Los requerimientos de seguridad con la metodología Octave se relacionan significativamente con la seguridad de los sistemas de información de la UNHEVAL, Huánuco, 2023. **Ho1:** Los requerimientos de seguridad con la metodología Octave no se relacionan significativamente con la seguridad de los sistemas de	VARIABLE 1: Metodología Octave	**Requerimientos de seguridad** - Identificación de activos - Clasificación de activos - Identificación de riesgos - Identificación de defensas - Necesidades de seguridad	- Número de activos identificados - Número de activos clasificados - Número de riesgos identificados - Número de defensas identificados - Nivel de las necesidades de seguridad	• Nivel: Descriptivo correlacional • Tipo: Básica • Diseño: No experimental correlacional transversal • Población: Está conformada por 91 administrativos de la UNHEVAL. • Muestra: Muestreo no probabilístico intencional o de conveniencia; está conformada por 91 administrativos de la
				Vulnerabilidades de la infraestructura - Identificación de vulnerabilidades - Evaluación de vulnerabilidades - Análisis de vulnerabilidades - Priorización de atención de vulnerabilidades.	- Número de componentes críticos identificados - Cantidad de puntos débiles evaluados en la infraestructura - Cantidad de puntos débiles analizados en la infraestructura - Cantidad de prioridades en la atención de vulnerabilidades.	

		información de la UNHEVAL, Huánuco, 2023. **Hi2:** La identificación de las vulnerabilidades de la infraestructura con la metodología Octave se relacionan significativamente con la seguridad de los sistemas de información de la UNHEVAL, Huánuco, 2023. **Ho2:** La identificación de las vulnerabilidades de la infraestructura con la metodología Octave no se relacionan significativamente con la seguridad de los sistemas de información de la UNHEVAL, Huánuco, 2023. **Hi3:** El establecimiento de un plan y estrategia mejora significativamente la seguridad de los sistemas de información de la UNHEVAL, Huánuco, 2023. **Ho3:** El establecimiento de un plan y estrategia no mejora significativamente la seguridad de los sistemas de información de la UNHEVAL, Huánuco, 2023.		**Plan y estrategia de seguridad** - Identificación y priorización de riesgos de información. - Control de seguridad - Integración de los controles	- Número de riesgos de información identificados - Número de controles de seguridad - Número de integración de controles	UNHEVAL.
			VARIABLE 2: Seguridad de los Sistemas de Información	**Confidencialidad e integridad** - Control de acceso - Encriptación - Control de cambios - Firmas digitales	- Cantidad de controles de acceso - Número de encriptaciones - Cantidad de controles de cambios - Cantidad de firmas digitales	
				Gestión de incidentes - Preparación - Análisis y detección - Contención, erradicación y recuperación - Actividades después de incidentes	- Números de preparación en la gestión de incidentes - Números de análisis y detección de incidentes - Números de actividades de contención, erradicación y recuperación - Números de	

					actividades después de incidentes	
				Gestión de vulnerabilidades - Escaneo de vulnerabilidades - Parches y actualizaciones	- Número de escáner de vulnerabilidades - Números de actividades de parches y actualizaciones	
				Cumplimiento legal y regulatorio - Evaluación y conformidad - Auditorías y revisiones externas	- Número de evaluaciones y conformidades - Número de auditorías y revisiones externas	

Anexo 02: Instrumento de recolección de datos

CUESTIONARIO

Marque con una X, la respuesta que crea conveniente.

Variable 1: Metodología Octave

N°		Siempre	Casi siempre	A veces	Casi nunca	Nunca
1	Se identifica los activos de los sistemas de información					
2	Se clasifica los activos de los sistemas de información					
3	Se identifica los riesgos de los sistemas de información					
4	Se identifica las defensas de los sistemas de información					
5	Se identifica las necesidades de seguridad					
6	Se identifica vulnerabilidades en el sistema de información					
7	Se evalúa vulnerabilidades en el sistema de información					
8	Se analiza vulnerabilidades en el sistema de información					
9	Se prioriza atender las vulnerabilidades en el sistema de información					
10	Se identifica los riesgos de información.					
11	Se realiza controles de seguridad					
12	Hay integración de controles					

Variable 2: Seguridad de los sistemas de información

N°		Siempre	Casi siempre	A veces	Casi nunca	Nunca
1	Realizan controles de acceso					
2	Realizan encriptaciones a la información					
3	Realizan controles de cambios					
4	Validan la información mediante firmas digitales					
5	Realizan una preparación en la gestión de incidentes					
6	Realizan un análisis para detectar incidentes					
7	Realizan actividades de contención, erradicación y recuperación de los sistemas de información ante algún incidente					
8	Realizan actividades (informes de incidentes, comunicados) después de los incidentes					
9	Escanean vulnerabilidades					
10	Realizan parches y actualizaciones					
11	Evalúan las actualizaciones					
12	Realizan auditorías y revisiones externas					

Anexo 03: Validación del (de los) instrumento (s) por jueces

FICHA DE VALIDACIÓN DE INSTRUMENTOS

TITULO. METODOLOGÍA OCTAVE Y SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN DE LA UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN, HUÁNUCO, 2023

I. DATOS INFORMATIVOS DEL EXPERTO VALIDADOR

Apellidos y nombres : Garcia Bonilla, Hernan Wilmer

Cargo o institución donde labora : Universidad Nacional Hermilio Valdizan

Nombre del instrumento de evaluación : Cuestionario

Teléfono : 962981893

Lugar y fecha : Cayhuayna, 31 de enero de 2024

Autor del instrumento :

II. ASPECTOS DE VALIDACIÓN DEL INSTRUMENTO:

Indicadores	Criterios	Valoración	
		SI	NO
Claridad	Los indicadores están formulados con un lenguaje apropiado y claro.	X	
Objetividad	Los indicadores que se están midiendo están expresados en conductas observables.	X	
Organización	Los ítems guardan un criterio de organización lógica.	X	
Intencionalidad	Sus instrumentos son adecuados para valorar aspectos de las estrategias	X	
Consistencia	Sus dimensiones e indicadores están basados en aspectos teórico científicos	X	
Coherencia	Existe coherencia entre los indicadores y las dimensiones de su variable	X	

Metodología	La estrategia que se está utilizando responde al propósito de la investigación	X	
Oportunidad	El instrumento será aplicado en el momento oportuno o más adecuado	X	

III. OPINIÓN GENERAL DEL EXPERTO ACERCA DE LOS INSTRUMENTOS

.....

.....

.....

.....

IV. RECOMENDACIONES

.....

.....

Huánuco, 31 de enero del 2024

.....

Firma del experto

DNI 45123493

FICHA DE VALIDACIÓN DE INSTRUMENTOS

TITULO. METODOLOGÍA OCTAVE Y SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN DE LA UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN, HUÁNUCO, 2023

I. DATOS INFORMATIVOS DEL EXPERTO VALIDADOR

Apellidos y nombres : Tello Saldaña Jhonny Alighiery

Cargo o institución donde labora : Especialista – Unheval.

Nombre del instrumento de evaluación : Cuestionario

Teléfono : 960634152

Lugar y fecha : 31/01/2024

Autor del instrumento :

II. ASPECTOS DE VALIDACIÓN DEL INSTRUMENTO:

Indicadores	Criterios	Valoración	
		SI	NO
Claridad	Los indicadores están formulados con un lenguaje apropiado y claro.	X	
Objetividad	Los indicadores que se están midiendo están expresados en conductas observables.	X	
Organización	Los ítems guardan un criterio de organización lógica.	X	
Intencionalidad	Sus instrumentos son adecuados para valorar aspectos de las estrategias	X	
Consistencia	Sus dimensiones e indicadores están basados en aspectos teórico científicos	X	
Coherencia	Existe coherencia entre los indicadores y las dimensiones de su variable	X	

Metodología	La estrategia que se está utilizando responde al propósito de la investigación	X	
Oportunidad	El instrumento será aplicado en el momento oportuno o más adecuado	X	

III. OPINIÓN GENERAL DEL EXPERTO ACERCA DE LOS INSTRUMENTOS

.....

.....

.....

.....

IV. RECOMENDACIONES

.....

.....

Huánuco, 31 de enero del 2024

Jhonny A. Tello Saldaña
INGENIERO DE SISTEMAS
CIP 282766

.....

Firma del experto

DNI 45250338

FICHA DE VALIDACIÓN DE INSTRUMENTOS

TITULO. METODOLOGÍA OCTAVE Y SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN DE LA UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN, HUÁNUCO, 2023

I. DATOS INFORMATIVOS DEL EXPERTO VALIDADOR

Apellidos y nombres : Gomez Meza Lincol Jarly

Cargo o institución donde labora : UNHEVAL

Nombre del instrumento de evaluación : Cuestionario

Teléfono : 931933005

Lugar y fecha : Cayhuayna – 31 de enero 2024

Autor del instrumento :

II. ASPECTOS DE VALIDACIÓN DEL INSTRUMENTO:

Indicadores	Criterios	Valoración	
		SI	NO
Claridad	Los indicadores están formulados con un lenguaje apropiado y claro.	X	
Objetividad	Los indicadores que se están midiendo están expresados en conductas observables.	X	
Organización	Los ítems guardan un criterio de organización lógica.	X	
Intencionalidad	Sus instrumentos son adecuados para valorar aspectos de las estrategias	X	
Consistencia	Sus dimensiones e indicadores están basados en aspectos teórico científicos	X	
Coherencia	Existe coherencia entre los indicadores y las dimensiones de su variable	X	

Metodología	La estrategia que se está utilizando responde al propósito de la investigación	X	
Oportunidad	El instrumento será aplicado en el momento oportuno o más adecuado	X	

III. OPINIÓN GENERAL DEL EXPERTO ACERCA DE LOS INSTRUMENTOS

.....

.....

.....

.....

IV. RECOMENDACIONES

.....

.....

Huánuco, 31 de enero del 2024

.....

Firma del experto

DNI 71695147

Anexo 04: Consentimiento informado

CONSENTIMIENTO INFORMADO

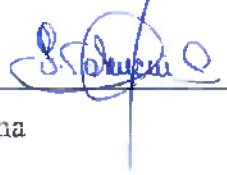
La presente investigación se titula "METODOLOGÍA OCTAVE Y SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN DE LA UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN, HUÁNUCO, 2023", la cual está siendo desarrollada por el estudiante Fredy Gallardo Valverde de la Universidad Nacional Hermilio Valdizán.

El objetivo general es determinar la relación que existe entre la Metodología Octave y la seguridad de los Sistemas de Información de la Universidad Nacional Hermilio Valdizán.

Para ello, nos gustaría como conocedores de los sistemas de información, contar con su participación en un estudio de investigación de forma estrictamente voluntaria y confidencial.

Si está de acuerdo con los puntos anteriores, complete los siguientes espacios.

Yo..Gladis V. Valentin Cañari.....identificado con número de DNI:..22401933....., estoy de acuerdo en participar con la investigación titulada "METODOLOGÍA OCTAVE Y SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN DE LA UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN, HUÁNUCO, 2023", la cual es desarrollada con fines de estudio.



Firma

CONSENTIMIENTO INFORMADO

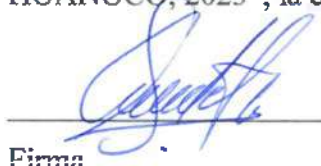
La presente investigación se titula "METODOLOGÍA OCTAVE Y SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN DE LA UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN, HUÁNUCO, 2023", la cual está siendo desarrollada por el estudiante Fredy Gallardo Valverde de la Universidad Nacional Hermilio Valdizán.

El objetivo general es determinar la relación que existe entre la Metodología Octave y la seguridad de los Sistemas de Información de la Universidad Nacional Hermilio Valdizán.

Para ello, nos gustaría como conocedores de los sistemas de información, contar con su participación en un estudio de investigación de forma estrictamente voluntaria y confidencial.

Si está de acuerdo con los puntos anteriores, complete los siguientes espacios.

Yo..Jesus Martel Rojas.....identificado con número de DNI:.22488742....., estoy de acuerdo en participar con la investigación titulada "METODOLOGÍA OCTAVE Y SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN DE LA UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN, HUÁNUCO, 2023", la cual es desarrollada con fines de estudio.



Firma

CONSENTIMIENTO INFORMADO

La presente investigación se titula "METODOLOGÍA OCTAVE Y SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN DE LA UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN, HUÁNUCO, 2023", la cual está siendo desarrollada por el estudiante Fredy Gallardo Valverde de la Universidad Nacional Hermilio Valdizán.

El objetivo general es determinar la relación que existe entre la Metodología Octave y la seguridad de los Sistemas de Información de la Universidad Nacional Hermilio Valdizán.

Para ello, nos gustaría como conocedores de los sistemas de información, contar con su participación en un estudio de investigación de forma estrictamente voluntaria y confidencial.

Si está de acuerdo con los puntos anteriores, complete los siguientes espacios.

Yo.....Mariela Renay Asca Martino.....identificado con número de DNI:.....44235178....., estoy de acuerdo en participar con la investigación titulada "METODOLOGÍA OCTAVE Y SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN DE LA UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN, HUÁNUCO, 2023", la cual es desarrollada con fines de estudio.

Firma

CONSENTIMIENTO INFORMADO

La presente investigación se titula "METODOLOGÍA OCTAVE Y SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN DE LA UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN, HUÁNUCO, 2023", la cual está siendo desarrollada por el estudiante Fredy Gallardo Valverde de la Universidad Nacional Hermilio Valdizán.

El objetivo general es determinar la relación que existe entre la Metodología Octave y la seguridad de los Sistemas de Información de la Universidad Nacional Hermilio Valdizán.

Para ello, nos gustaría como conocedores de los sistemas de información, contar con su participación en un estudio de investigación de forma estrictamente voluntaria y confidencial.

Si está de acuerdo con los puntos anteriores, complete los siguientes espacios.

Yo. Naroshina Ginat Soto Garro .....identificado con número de DNI:.73369689., estoy de acuerdo en participar con la investigación titulada "METODOLOGÍA OCTAVE Y SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN DE LA UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN, HUÁNUCO, 2023", la cual es desarrollada con fines de estudio.

Firma

CONSENTIMIENTO INFORMADO

La presente investigación se titula "METODOLOGÍA OCTAVE Y SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN DE LA UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN, HUÁNUCO, 2023", la cual está siendo desarrollada por el estudiante Fredy Gallardo Valverde de la Universidad Nacional Hermilio Valdizán.

El objetivo general es determinar la relación que existe entre la Metodología Octave y la seguridad de los Sistemas de Información de la Universidad Nacional Hermilio Valdizán.

Para ello, nos gustaría como conocedores de los sistemas de información, contar con su participación en un estudio de investigación de forma estrictamente voluntaria y confidencial.

Si está de acuerdo con los puntos anteriores, complete los siguientes espacios.

Yo.....Treysi Tito Quispe.....identificado con número de DNI:.....46932525....., estoy de acuerdo en participar con la investigación titulada "METODOLOGÍA OCTAVE Y SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN DE LA UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN, HUÁNUCO, 2023", la cual es desarrollada con fines de estudio.

Firma

Anexo 05: Autorización de la aplicación del instrumento

"Decenio de la Igualdad de oportunidades para mujeres y hombres"
"Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho"
Huánuco - Perú
UNIVERSIDAD LICENCIADA (Resolución de Consejo Directivo N° 099-SUNEDU/CD)

Cayhuayna, 15 de enero de 2024

OFICIO N° 011- 2024-UNHEVAL-R
Señor:
FREDY GALLARDO VALVERDE
DNI:48207721
Presente. -

ASUNTO : RESPECTO A PERMISO PARA RECOLECTAR DATOS EN EL PERSONAL ADMINISTRATIVO QUE LABORA EN LAS FACULTADES DE LA UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN.
REFERENCIA: CARTA N° 001-2024-FGV-UNHEVAL

Tengo el agrado de dirigirme a usted para expresarle mi cordial saludo, y que habiendo recibido el documento de la referencia respecto a solicitud de permiso para recolectar datos en el personal administrativo que labora en las Facultades de la Universidad Nacional Hermilio Valdizán, debe manifestar que se autoriza el permiso para aplicación del respectivo cuestionario en los días y horas que usted crea conveniente una vez recibida el presente.

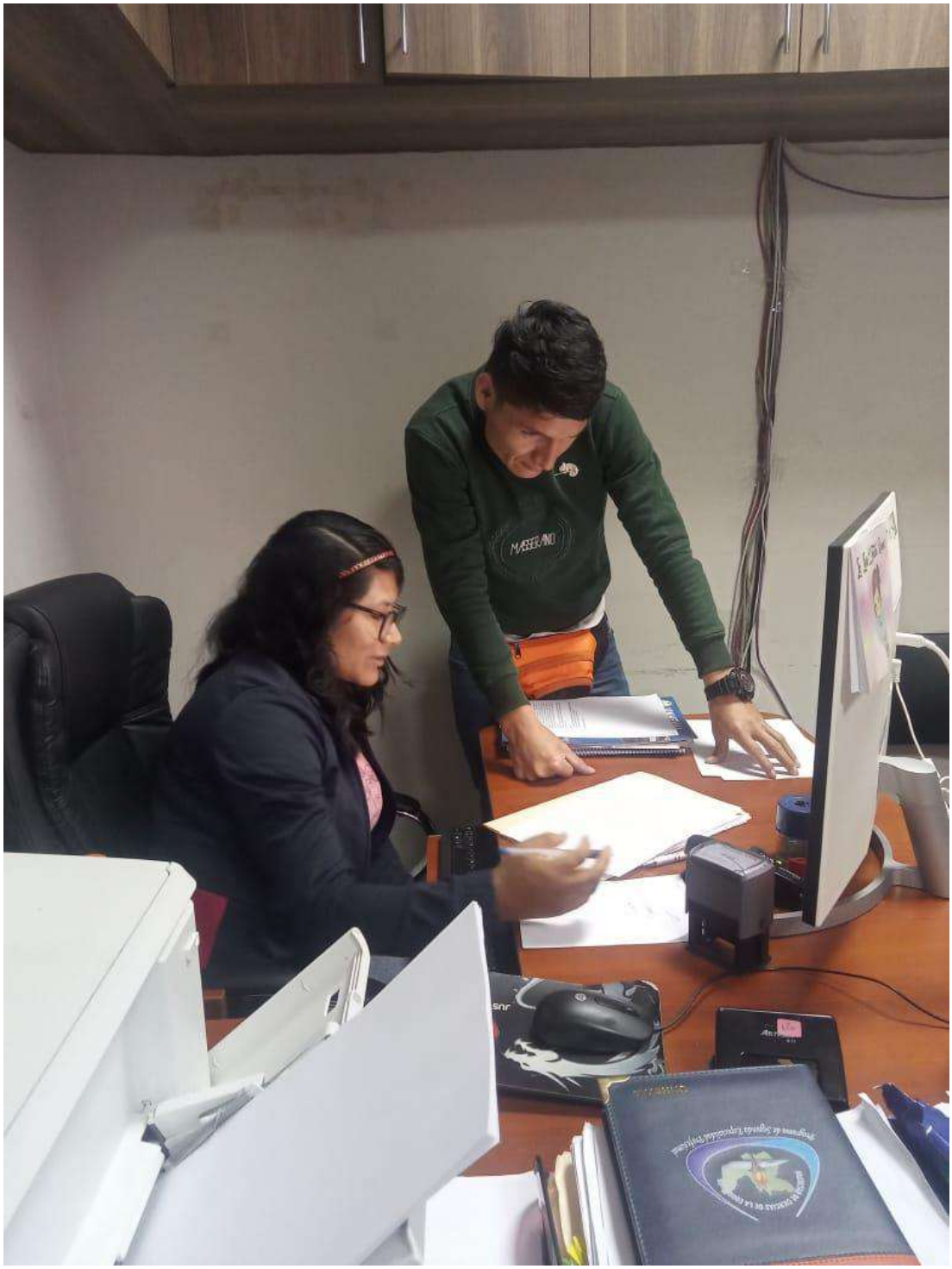
Sin otro particular, hago propicia la ocasión para expresarle las muestras de mi especial consideración y estima personal.

Atentamente,

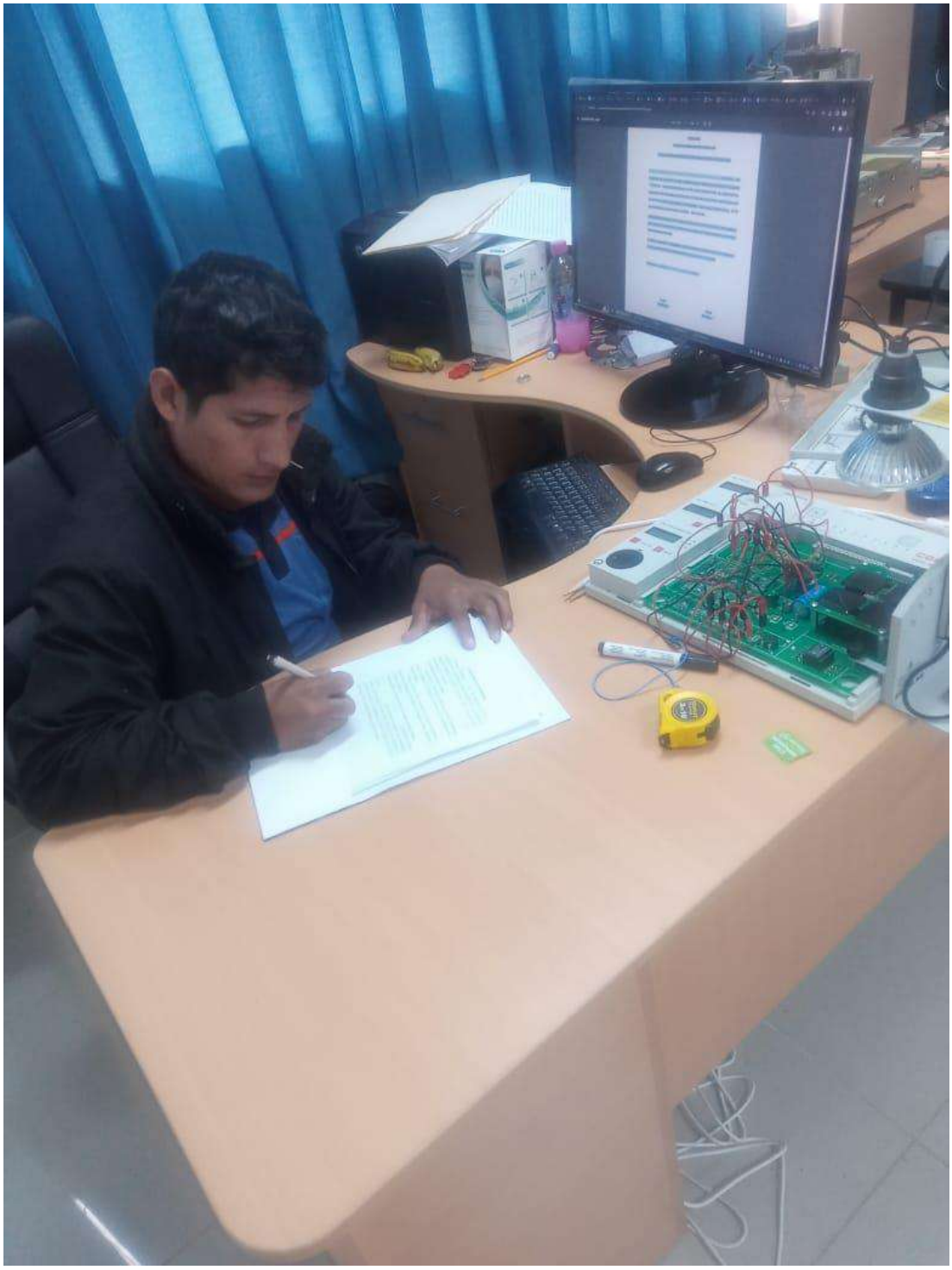
UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN
RECTOR
Dr Guillermo A. Bocangel Weydert
RECTOR

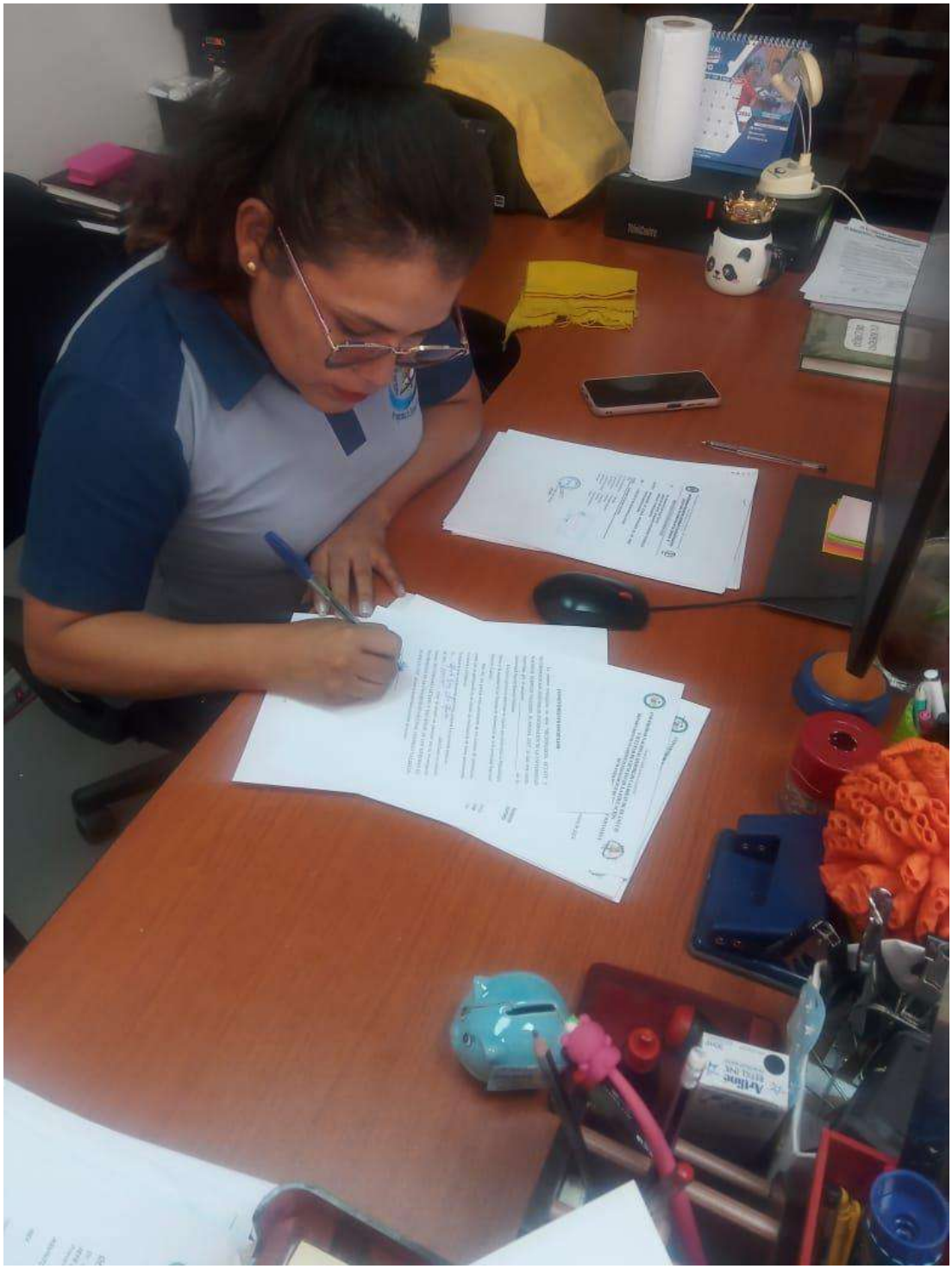
C.c. Archivo

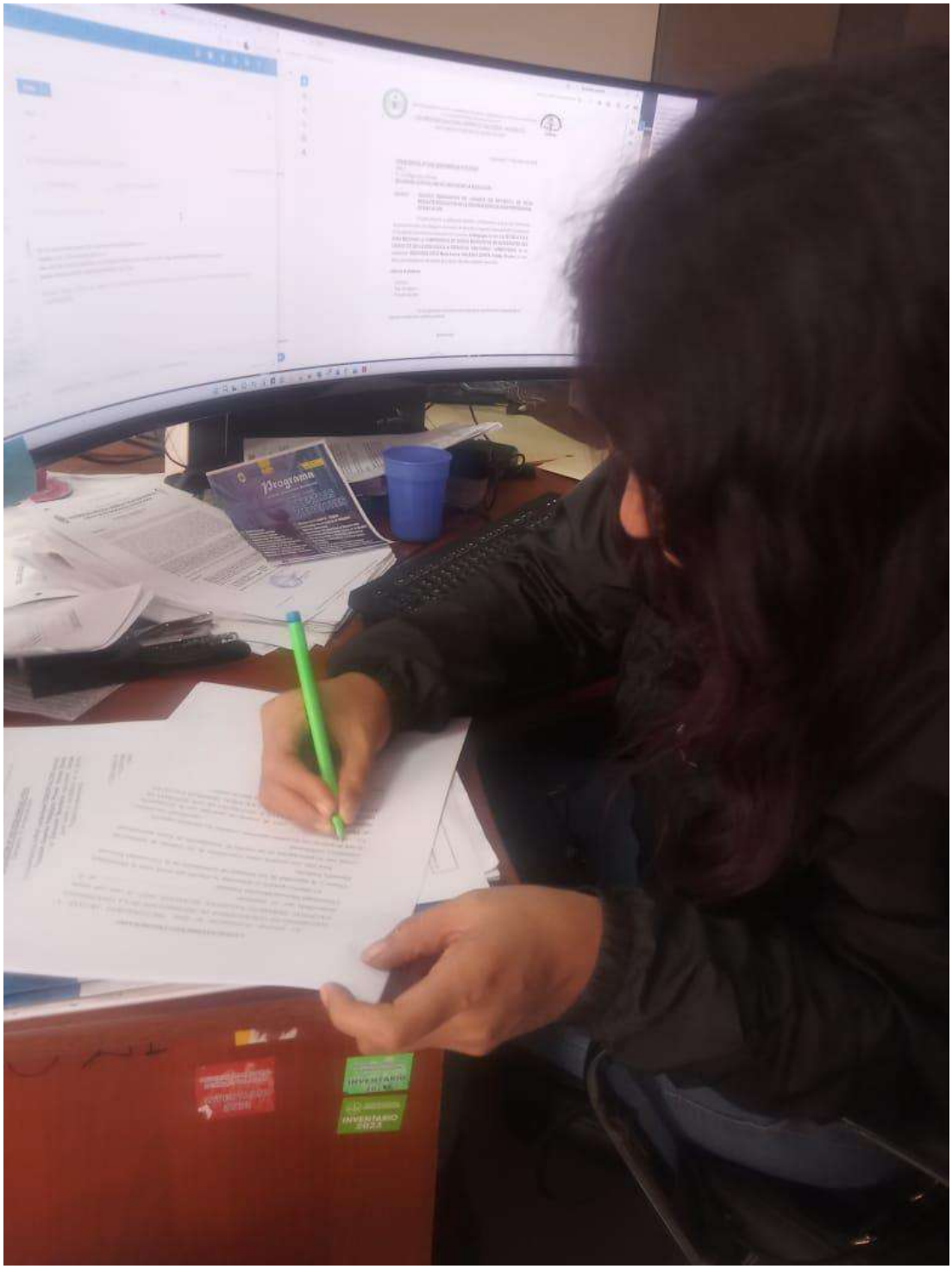
Anexo 06: Aplicación del instrumento




BUSCA Y COLOREA






Programa
INVENTARIO
2023

Anexo 07: Nota Biográfica

Fredy Gallardo Valverde, nacido en el Distrito de Huánuco Provincia de Huánuco del Departamento de Huánuco en el año 1994, demostró su temprano interés por la tecnología. Durante su paso por la Universidad, se ha destacado por su compromiso con el estudio, su capacidad para colaborar en equipo y su incansable curiosidad por ampliar sus conocimientos en su área de especialización.

Realizo sus estudios universitarios de pregrado en la Universidad Nacional Hermilio Valdizán, llegando a egresar y obtener el grado académico de Bachiller en Ingeniería de Sistemas y aspirando posteriormente al título profesional y grados académicos superiores, actualmente tramitando el grado de maestría en Ingeniería de Sistemas en la Universidad Nacional Hermilio Valdizán mención en Tecnología de Información y Comunicación y estudiando un doctorado en Ciencias de la Educación.

Complementa sus estudios con especializaciones en administración de base de datos, análisis de datos, inteligencia artificial, ofimática, sistemas del gobierno (SIGA y SIAF), manejo de herramientas digitales, diplomado en diseño gráfico y producción audiovisual profesional.

Poseyendo una mente curiosa y un firme compromiso con la calidad, siente entusiasmo por proseguir su trayecto en el ámbito de la ingeniería, aspirando a realizar aportes relevantes y generar impacto en la sociedad mediante la aplicación innovadora de sus capacidades y saberes.

Anexo 08: Acta de sustentación

UNHEVAL
UNIVERSIDAD NACIONAL HERMILIO VALDIZAN
DECANATO
FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS

ACTA DE SUSTENTACIÓN DE TESIS PARA OPTAR EL TÍTULO PROFESIONAL

En la ciudad universitaria de Cayhuayna, siendo las ...10:00..... horas del día ..19 de Junio..... del 2024, nos reunimos en la Sala de sustentaciones de la Facultad de Ingeniería Industrial y de Sistemas de la UNHEVAL, los miembros integrantes del Jurado Evaluador:

Mg. FLORES VIDAL JIMMY GROVER	**PRESIDENTE**
Dr. FRANCISCO PAREDES ABIMAEL ADAM	**SECRETARIO**
Mg. REYNA GONZALEZ JULISSA ELIZABETH	**VOCAL.**

Acreditados mediante Resolución N° **0185-2024-UNHEVAL/FIIS-D de fecha 15.ABR.2024**, de la tesis titulada: **"METODOLOGIA OCTAVE Y SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN DE LA UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN, HUÁNUCO, 2023"**, presentado por el titulando: **GALLARDO VALVERDE FREDY,** bajo el asesoramiento de la docente **Dra. HEIDY VELSY RIVERA VIDAL DE SANCHEZ**, se procedió a dar inicio el acto de sustentación para optar el **TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS.**

Concluido el acto de sustentación, cada miembro del Jurado Evaluador procedió a la evaluación del titulando, teniendo presente los siguientes criterios:

1. Presentación
2. Exposición y dominio del tema
3. Absolución de preguntas

Nombres y Apellidos del Titulando	Jurado Evaluador			Promedio Final
	Presidente	Secretario	Vocal	
GALLARDO VALVERDE FREDY	16	16	16	16

Obteniendo en consecuencia el titulando: **GALLARDO VALVERDE FREDY,** la nota de ...DIECISEIS (...16...), equivalente a ...BUENO..... por lo que se declara ...Aprobado

Calificación que se realiza de acuerdo con el Art. 46° del Reglamento General de Grados y Títulos 2024 de la UNHEVAL.

Se da por finalizado el presente acto, siendo las 11:30 horas, del día 19 de Junio del 2024, firmando en señal de conformidad.

PRESIDENTE
DNI N° 22527461

SECRETARIO
DNI N° 22498084

VOCAL
DNI N° 18032294

Leyenda:
19 a 20: Excelente
17 a 18: Muy Bueno
14 a 16: Bueno
0 a 13: Desaprobado

Anexo 09: Constancia de similitud y el reporte

UNIVERSIDAD NACIONAL "HERMILIO VALDIZÁN"

Licenciada con Resolución del Consejo Directivo N° 099-2019-SUNEDU/CD

FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

CARRERA PROFESIONAL DE INGENIERÍA DE SISTEMAS

CONSTANCIA DE SIMILITUD N° 09-2024 SOFTWARE ANTIPLAGIO TURNITIN-FIIS-UNHEVAL.

La Unidad de Investigación de la Facultad de Ingeniería Industrial y de Sistemas, emite la presente constancia de Antiplagio, aplicando el Software TURNITIN, la cual reporta un 13% de similitud, correspondiente al interesado (a) **FREDY GALLARDO VALVERDE.** Del trabajo de investigación ***"METODOLOGIA OCTAVE Y SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN DE LA UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN, HUÁNUCO, 2023"***, considerado como asesor(a) al Dra. Heidy Velsy Rivera Vidal de Sánchez.

DECLARANDO (APTO)

Se expide la presente, para los trámites pertinentes

Pillco Marca, 25 de junio 2024

Dr. (a) Guadalupe Ramírez Reyes
Director(a) de la Unidad de Investigación
de la Facultad de Ingeniería Industrial y de Sistemas
UNHEVAL

Reporte de similitud

NOMBRE DEL TRABAJO

"METODOLOGIA OCTAVE Y SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN DE LA UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN, HUÁNUCO, 2023"

AUTOR

FREDY GALLARDO VALVERDE

RECUENTO DE PALABRAS

24093 Words

RECUENTO DE CARACTERES

136048 Characters

RECUENTO DE PÁGINAS

126 Pages

TAMAÑO DEL ARCHIVO

2.5MB

FECHA DE ENTREGA

Jun 25, 2024 8:19 AM GMT-5

FECHA DEL INFORME

Jun 25, 2024 8:21 AM GMT-5

13% de similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base de datos.

- 12% Base de datos de Internet
- 1% Base de datos de publicaciones
- Base de datos de Crossref
- Base de datos de contenido publicado de Crossref
- 6% Base de datos de trabajos entregados

Reporte de similitud

13% de similitud general

Principales fuentes encontradas en las siguientes bases de datos:

- 12% Base de datos de Internet
- 1% Base de datos de publicaciones
- Base de datos de Crossref
- Base de datos de contenido publicado de Crossref
- 6% Base de datos de trabajos entregados

FUENTES PRINCIPALES

Las fuentes con el mayor número de coincidencias dentro de la entrega. Las fuentes superpuestas no se mostrarán.

1	repositorio.unheval.edu.pe Internet	4%
2	repositorio.unamba.edu.pe Internet	2%
3	pmg-ssi.com Internet	<1%
4	melissav17.blogspot.com Internet	<1%
5	hdl.handle.net Internet	<1%
6	repositorio.uta.edu.ec Internet	<1%
7	transparencia.unheval.edu.pe Internet	<1%
8	proyectosmaestrias.virtual.uniandes.edu.co Internet	<1%

9	repositorio.utp.edu.pe Internet	<1%
10	repositorio.uladech.edu.pe Internet	<1%
11	Enterprise-Escuela de Educacion Superior Pedagogica Marcos Duran ... Submitted works	<1%
12	Universidad Alas Peruanas on 2019-07-24 Submitted works	<1%
13	Universidad Nacional Abierta y a Distancia, UNAD,UNAD on 2023-05-28 Submitted works	<1%
14	Universidad Cesar Vallejo on 2016-04-25 Submitted works	<1%
15	Universidad Politecnica Salesiana del Ecuador on 2023-03-08 Submitted works	<1%
16	Universidad Carlos III de Madrid on 2013-01-11 Submitted works	<1%
17	apirepositorio.unh.edu.pe Internet	<1%
18	Enterprise-Escuela de Educacion Superior Pedagogica Marcos Duran ... Submitted works	<1%
19	Gaby Cañazaca-Poma, Manuel Urrutia-Flores. "Cultura Tributaria y la E... Crossref	<1%
20	Corporación Universitaria Minuto de Dios, UNIMINUTO on 2022-11-20 Submitted works	<1%

21	repositorio.udh.edu.pe Internet	<1%
22	distancia.udh.edu.pe Internet	<1%
23	repositorio.utn.edu.ec Internet	<1%
24	Universidad Internacional de la Rioja on 2023-09-20 Submitted works	<1%
25	Universidad Tecnológica Centroamericana UNITEC on 2023-06-26 Submitted works	<1%
26	Universidad de Guayaquil on 2023-07-31 Submitted works	<1%
27	jhosesbuelvas.blogspot.com Internet	<1%

Anexo 10: Autorización de publicación

UNHEVAL UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN | VICERRECTORADO DE INVESTIGACIÓN | DIRECCIÓN DE INVESTIGACIÓN

ANEXO N° 26

AUTORIZACIÓN DE PUBLICACIÓN DIGITAL Y DECLARACIÓN JURADA DEL TRABAJO DE INVESTIGACIÓN, TESIS, TRABAJO DE SUFIENCIA PROFESIONAL O TRABAJO ACADÉMICO PARA OPTAR UN GRADO O TÍTULO PROFESIONAL

1. Autorización de Publicación: *(Marque con una "X" según corresponda)*

Bachiller		Título Profesional	X	Segunda Especialidad		Maestro		Doctor	

Ingrese los datos según corresponda.

Facultad/Escuela	INGENIERÍA INDUSTRIAL Y DE SISTEMAS
Escuela/Carrera Profesional	INGENIERÍA DE SISTEMAS
Programa	
Grado que otorga	
Título que otorga	INGENIERO DE SISTEMAS

2. Datos del (los) Autor(es): *(Ingrese los datos según corresponda)*

Apellidos y Nombres:	GALLARDO VALVERDE FREDY								
Tipo de Documento:	**DNI**	X	**Pasaporte**		**C.E.**		**N° de Documento:**	48207721	
Correo Electrónico:	fredy_1994_5@hotmail.com								
Apellidos y Nombres:									
Tipo de Documento:	**DNI**		**Pasaporte**		**C.E.**		**N° de documento:**		
Correo Electrónico:									
Apellidos y Nombres:									
Tipo de Documento:	**DNI**		**Pasaporte**		**C.E.**		**N° de Documento:**		
Correo Electrónico:									

3. Datos del Asesor: *(Ingrese los datos según corresponda)*

Apellidos y Nombres:	RIVERA VIDAL DE SANCHEZ HEIDY VELSY							
Tipo de Documento:	**DNI**	X	**Pasaporte**		**C.E.**		**N° de Documento:**	41048834
ORCID ID:	https://orcid.org/0000-0002-5206-356X							

4. Datos de los Jurados: *(Ingrese los datos según corresponda, primero apellidos luego nombres)*

Presidente	FLORES VIDAL JIMMY GROVER
Secretario	FRANCISCO PAREDES ABIMAEL ADAM
Vocal	REYNA GONZALEZ JULISSA ELIZABETH
Vocal	
Vocal	
Accesitario	JESUS TOLENTINO INES EUSEBIA

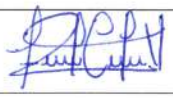
5. Datos del Documento Digital a Publicar: *(Ingrese los datos y marque con una "X" según corresponda)*

Ingrese solo el año en el que sustentó su Trabajo de Investigación: *(Verifique la Información en el **Acta de Sustentación**)*							2024	
Modalidad de obtención del Grado Académico o Título Profesional: *(Marque con **X** según corresponda)*	**Trabajo de Investigación**		**Tesis**	x	**Trabajo Académico**		**Trabajo de Suficiencia Profesional**	
Palabras claves	METODOLOGÍA OCTAVE				SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN		ACTIVOS DE LOS SISTEMAS DE INFORMACIÓN	
Tipo de acceso: *(Marque con **X** según corresponda)*	**Abierto**	x	**Cerrado***		**Restringido***		**Periodo de Embargo**	
(*) Sustentar razón:								

6. Declaración Jurada: (Ingrese todos los datos requeridos completos)

Soy Autor (a) (es) del Trabajo de Investigación Titulado: *(Ingrese el título tal y como está registrado en el **Acta de Sustentación**)*
"METODOLOGIA OCTAVE Y SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN DE LA UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN, HUÁNUCO, 2023"
Mediante la presente asumo frente a la Universidad Nacional Hermilio Valdizán (en adelante LA UNIVERSIDAD), cualquier responsabilidad que pueda derivarse por la autoría, originalidad y veracidad del contenido del trabajo de investigación, así como por los derechos de la obra y/o invención presentada. En consecuencia, me hago responsable frente a LA UNIVERSIDAD y frente a terceros de cualquier daño que pudiera ocasionar a LA UNIVERSIDAD o a terceros, por el incumplimiento de lo declarado o que pudiera encontrar causas en los trabajos de investigación presentado, asumiendo toda la carga pecuniaria que pudiera derivarse de ello. Asimismo, por la presente me comprometo a asumir además todas las cargas pecuniarias que pudiera derivar para LA UNIVERSIDAD en favor de terceros con motivos de acciones, reclamaciones o conflictos derivados del incumplimiento de lo declarado o las que encontraren causa en el contenido del Trabajo de Investigación. De identificarse fraude, piratería, plagio, falsificación o que el trabajo haya sido publicado anteriormente; asumo las consecuencias y sanciones que de mis acciones se deriven, sometiéndome a las acciones legales y administrativas vigentes.

7. Autorización de Publicación Digital:

A través de la presente autorizo de manera gratuita a la Universidad Nacional Hermilio Valdizan a publicar la versión digital de este trabajo de investigación en su biblioteca virtual, repositorio institucional y base de datos, por plazo indefinido, consintiendo que con dicha autorización cualquier tercero podrá acceder a dichas paginas de manera gratuita pudiendo revisarla, imprimirla o grabarla siempre y cuando se respete la autoría y sea citada correctamente.			
Apellidos y Nombres	GALLARDO VALVERDE FREDY	**Firma**	
Apellidos y Nombres		**Firma**	
Apellidos y Nombres		**Firma**	

FECHA: Huánuco, 21 de junio del 2024

Nota:

- ✓ No modificar los textos preestablecidos, conservar la estructura del documento.
- ✓ Marque con una X en el recuadro que corresponde.
- ✓ Llenar este formato de forma digital, con tipo de letra calibri, tamaño de fuente 09, manteniendo la alineación del texto que observa en el modelo, sin errores gramaticales (recuerde las mayúsculas también se tildan si corresponde).
- ✓ La información que escriba en este formato debe coincidir con la información registrada en los demás archivos y/o formatos que presente, tales como: DNI, Acta de Sustentación, Trabajo de Investigación (PDF), Constancia de Similitud, Reporte de Similitud.
- ✓ Cada uno de los datos requeridos en este formato, es de carácter obligatorio según corresponda.
- ✓ Se debe de imprimir, firmar y luego escanear el documento (legible).