UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

PROGRAMA ACADÉMICO DE MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

Análisis de vulnerabilidades e Incidencias en la Seguridad Informática de la Empresa CRATI E.I.R.L.

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:
Maestro en Ingeniería de Sistemas con Mención en Tecnologías de la Información

AUTOR:

Sanchez Rueda, Jose Luis (orcid.org/0000-0002-1749-3935)

ASESORES:

Mg. Poletti Gaitan, Eduardo Humberto (orcid.org/0000-0002-2143-4444)
Mg. Tejada Ruiz, Roberto Juan (orcid.org/ 0000-0003-3669-836X)

LÍNEA DE INVESTIGACIÓN:

Sistemas de Información y Comunicaciones.

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Innovación tecnológica y desarrollo sostenible

LIMA – PERÚ

2023

DEDICATORIA

Quiero dedicar mi trabajo a todos los miembros de mi familia, ya que me han ayudado a mantenerme inspirado y motivado para cumplir mis objetivos y porque me han apoyado constantemente todo lo que me he propuesto en mi carrera profesional.

AGRADECIMIENTO

Ante todo, doy las gracias a mi madre por haberme dado el don de la vida, que me ha permitido alcanzar todas las metas que me he propuesto hasta ahora.

A mi familia, que siempre me ha apoyado, me ha ofrecido consejo y me ha inspirado a seguir adelante demostrándome que las aspiraciones y metas de esta vida son alcanzables con mucho trabajo duro.

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

Declaratoria de Autenticidad del Asesor

Yo, POLETTI GAITAN EDUARDO HUMBERTO, docente de la ESCUELA DE POSGRADO MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, asesor de Tesis titulada: "Análisis de vulnerabilidades e Incidencias en la Seguridad Informática de la Empresa CRATI E.I.R.L.", cuyo autor es SANCHEZ RUEDA JOSE LUIS, constato que la investigación tiene un índice de similitud de 13.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

He revisado dicho reporte y concluyo que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la Tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

En tal sentido, asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

LIMA, 01 de Agosto del 2023

Apellidos y Nombres del Asesor:	Firma
POLETTI GAITAN EDUARDO HUMBERTO **DNI:** 18073124 **ORCID:** 0000-0002-2143-4444	Firmado electrónicamente por: EPOLETTIG el 02-08-2023 14:23:03

Código documento Trilce: TRI - 0634481

INVESTIGA UCV

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

Declaratoria de Originalidad del Autor

Yo, SANCHEZ RUEDA JOSE LUIS estudiante de la ESCUELA DE POSGRADO del programa de MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, declaro bajo juramento que todos los datos e información que acompañan la Tesis titulada: "Análisis de vulnerabilidades e Incidencias en la Seguridad Informática de la Empresa CRATI E.I.R.L.", es de mi autoría, por lo tanto, declaro que la Tesis:

1. No ha sido plagiada ni total, ni parcialmente.
2. He mencionado todas las fuentes empleadas, identificando correctamente toda cita textual o de paráfrasis proveniente de otras fuentes.
3. No ha sido publicada, ni presentada anteriormente para la obtención de otro grado académico o título profesional.
4. Los datos presentados en los resultados no han sido falseados, ni duplicados, ni copiados.

En tal sentido asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de la información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

Nombres y Apellidos	Firma
SANCHEZ RUEDA JOSE LUIS **DNI:** 48137100 **ORCID:** 0000-0002-1749-3935	Firmado electrónicamente por: JSANCHEZR1 el 02-08-2023 15:43:45

Código documento Trilce: INV - 1230430

INVESTIGA UCV

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

Este estudio aborda la problemática central al investigar el impacto del análisis de vulnerabilidades en la gestión de incidencias en la seguridad informática en una organización de servicios de tecnología. Se tiene en cuenta estudios previos realizados por varios autores que han abordado problemáticas similares, lo cual sirve de base para desarrollar esta investigación. La base principal de esta tesis es establecer cómo se relacionan los incidentes de seguridad informática en la empresa mencionada con las vulnerabilidades. Se empleó una técnica cuantitativa con una estrategia de investigación aplicada y un diseño preexperimental. Se tuvo en cuenta los requisitos esenciales y la dependencia del análisis de vulnerabilidades en la seguridad informática. Es recomendable argumentar que contar con una herramienta sólida para mejorar la seguridad informática puede contribuir a un mejor diseño y comprensión en la ejecución del análisis de vulnerabilidades e incidencias. Esto podría conducir a mejoras en indicadores clave como el Índice de Vulnerabilidades corregidas, el Índice de vulnerabilidades no corregidas, el Tiempo de Resolución de Incidencias y el Nivel de incidencias atendidas.

Palabras clave: análisis de vulnerabilidades, análisis de incidencias, seguridad informática.

ABSTRACT

By examining the effect of vulnerability analysis on the management of incidents in computer security in an IT consulting firm, this study seeks to solve the main issue. The foundation for this research's development comes from earlier studies conducted by a number of writers that focused on related issues. Finding the relationship between computer security-related incidents at the aforementioned firm and vulnerabilities was the main objective of this investigation. A pre-experimental design was used, and an applied research technique was the major emphasis. The essential requirements and reliance of the investigation of computer security vulnerabilities were taken into account. It is recommended to make the case that having a reliable tool to increase computer security will help with better design and comprehension of how to implement vulnerability and incident analysis. The Corrected Vulnerability Index, the Uncorrected Vulnerability Index, the Incident Resolution Time, and the Level of incidents attended may all see improvements as a result of this.

Keywords: vulnerability analysis, incident analysis, computer security.

I. INTRODUCCIÓN

La seguridad informática es crucial para las empresas que manejan datos valiosos. Detectar y abordar tempranamente las vulnerabilidades e incidencias de seguridad es fundamental para proteger los activos y la reputación de una empresa. La detección temprana de problemas de seguridad ahorra costos, minimiza el impacto en las operaciones y la confianza de los clientes, y ayuda a cumplir con requisitos legales y regulatorios. Este artículo destaca los beneficios y cualidades de la detección temprana de vulnerabilidades e incidencias en la seguridad informática para las empresas. La detección temprana de vulnerabilidades e incidencias en la seguridad informática es crucial para proteger a las empresas en el entorno digital actual. Les permite gestionar los problemas antes de que se materialicen en riesgos reales., minimizar el impacto financiero y de reputación, proteger la confianza de los clientes y cumplir con las regulaciones y requisitos de seguridad. La detección temprana de problemas de seguridad en la informática tiene múltiples beneficios para las empresas. Además de proteger sus activos y reputación, les permite mejorar su eficiencia y garantía en la gestión de la seguridad.

En un plano internacional Riggs, H et al. (2023) en un proyecto realizado en la Universidad Internacional de Florida, Miami menciona que la tecnología de la información se está transformando en parte del funcionamiento diario de varias infraestructuras cruciales. y, como resultado, la superficie de ataque cibernético se extiende sobre una amplia gama de estas infraestructuras. Los ataques cibernéticos han sido un problema grave a nivel mundial para las industrias desde principios de la década de 2000, causando interrupciones significativas en su capacidad para producir bienes u ofrecer servicios a sus clientes. La próspera economía del delito cibernético abarca el lavado de dinero, los mercados negros y los ataques a los sistemas físicos cibernéticos que resultan en interrupciones del servicio. Además, las violaciones de datos extensas han comprometido la información de identificación personal de millones de personas.

En un enfoque a nivel nacional, la problemática del análisis de vulnerabilidades e incidencias en la seguridad informática en el Perú es una realidad que ha sido señalada por diversas fuentes. Según el Centro Nacional de Incidentes de Seguridad

de la Información del Perú (CENSI) (2020) según una encuesta publicada recientemente, El número de incidencias de seguridad de la información notificados en todo el país aumentó un 66%, hasta alcanzar los 27.155. La mayoría de las empresas peruanas, según la encuesta, carecen de sistemas de gestión de la seguridad de la información establecidos, así como de las personas cualificadas y los recursos necesarios para identificar y abordar eficazmente los problemas de seguridad de la información.

Por otro lado, un estudio realizado por la consultora PwC en el año 2020 reveló que el 80% de las empresas en el Perú ha sufrido al menos un incidente de seguridad informática en los últimos 12 meses, y que el 66% de ellas no cuenta con un plan de respuesta a incidencias de seguridad.

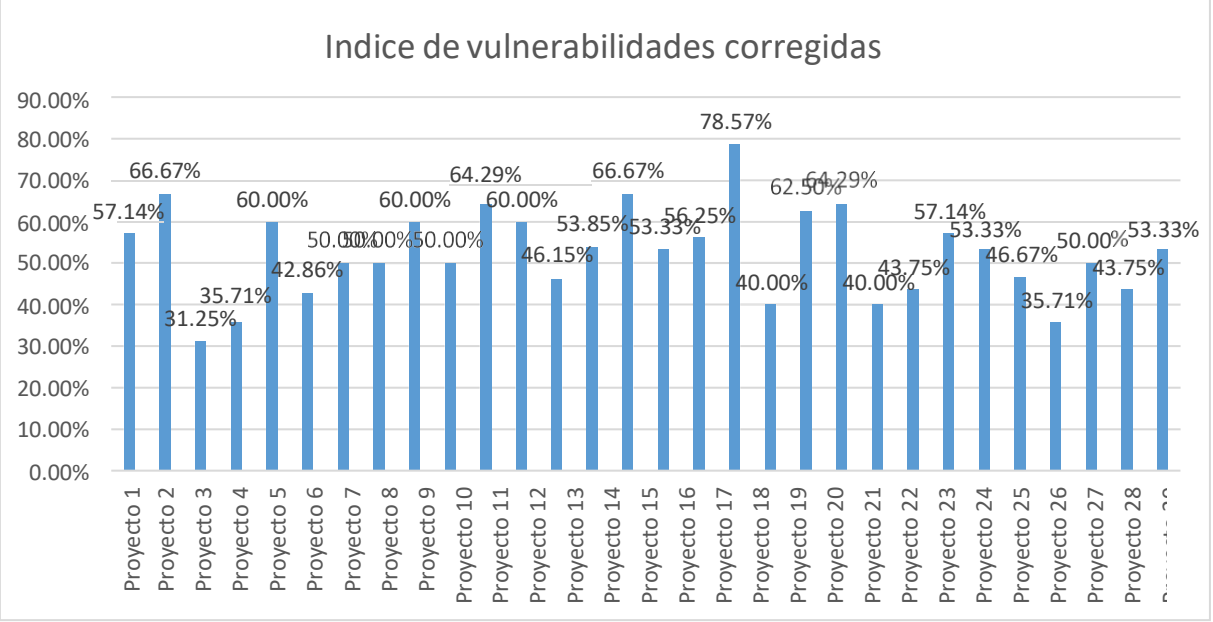
Los indicadores del problema de vulnerabilidad y análisis de incidencias de seguridad informática en Perú incluyen el aumento de incidencias de seguridad informática reportados, la ausencia de sistemas formales de gestión de seguridad informática en las empresas, la falta de capacitación y recursos para detectar y enfrentar amenazas de seguridad informática, y el aumento de incidencias de seguridad informática reportados. Los datos aquí expuestos provienen de dos fuentes respetadas en el entorno de la seguridad informática: el estudio de PwC y el informe del Centro Nacional de Incidentes de Seguridad Informática del Perú.

La misión de esta investigación, que tiene una relación directa con la empresa, es analizar los riesgos de seguridad informática a los que se enfrenta el proveedor de servicios sin tener acceso a las respuestas a las cuestiones que se plantean a lo largo del proceso de análisis. Su objetivo es determinar las causas profundas de los inconvenientes de seguridad informática de la organización, así como sus posibles repercusiones. Algunas fuentes probables de riesgos para la seguridad informática en la empresa de servicios son la ausencia de medidas de seguridad adecuadas, la falta de formación del personal involucrado en el campo de seguridad informática y la existencia de vulnerabilidades en el software o el hardware utilizados. A fin de sugerir medidas preventivas y correctivas eficaces para reducir los riesgos, es importante examinar estas razones.

Se prevé que el estudio ofrezca un conocimiento exhaustivo de los retos de seguridad informática a los que se enfrenta el proveedor de servicios, así como información valiosa para elegir las mejores soluciones de seguridad a implantar. El objetivo último es mantener la continuidad del negocio frente a los posibles riesgos de seguridad informática y la cláusula de la información exclusiva de los actores involucrados de la empresa.

Para complementar la información se realizó la evaluación de los indicadores en el mes de abril previo al análisis de vulnerabilidades, obteniendo para el indicador: índice de vulnerabilidades corregidas un promedio de 52.44% de un total de 30 proyectos.

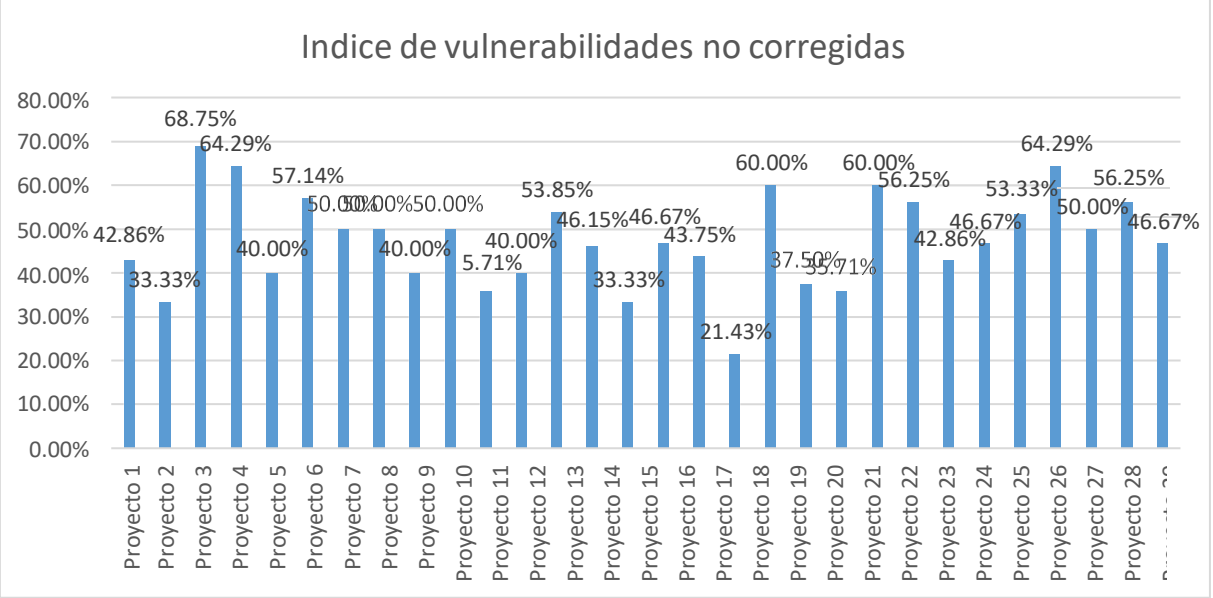
Figura 1: Índice de vulnerabilidades corregidas pre test mes de abril



Nota: Elaboración propia

Asimismo, se realizó para el indicador: índice de vulnerabilidades no corregidas en donde el promedio obtenido fue de 47.56% de un total de 30 proyectos también

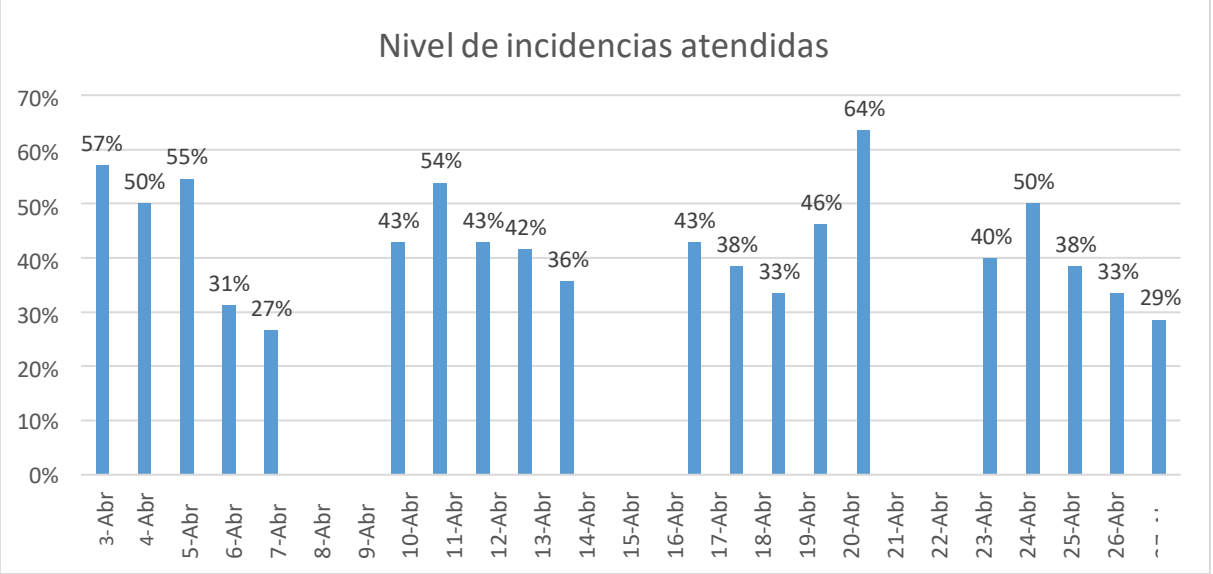
Figura 2: Índice de vulnerabilidades no corregidas pre test mes de abril



Nota: Elaboración propia

Y para el indicador nivel de incidencias atendidas con una muestra de 269 incidencias se obtuvo un promedio de un 43 %

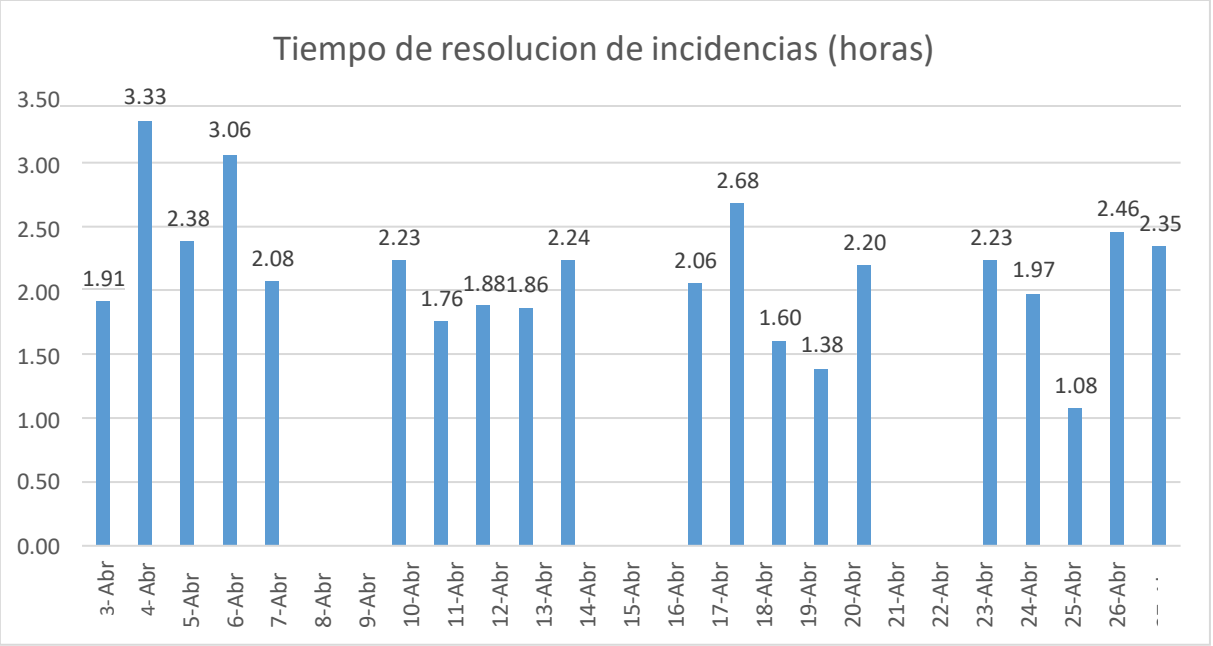
Figura 3: Nivel de incidencias atendidas pre test mes de abril



Nota: Elaboración propia

Según el indicador de tiempo de resolución de incidencias, se tardó una media de 2,14 horas en resolver cada incidente:

Figura 4: Tiempo de resolución de incidencias pre test mes de abril



Nota: Elaboración propia

En tal sentido se plantea como problema general:

¿Las vulnerabilidades impactan en las incidencias en la gestión de proyectos de una empresa de servicios de tecnología en Lima, 2023?

Y como problemas específicos:

- ¿De qué manera impacta el análisis de vulnerabilidades en el índice de Vulnerabilidades corregidas en la gestión de incidencias para la Seguridad Informática en una empresa de servicios de tecnología?

- ¿De qué manera impacta el análisis de vulnerabilidades en el Índice de vulnerabilidades no corregidas en la gestión de incidencias para la Seguridad Informática en una empresa de servicios de tecnología?

- ¿De qué manera impacta el análisis de vulnerabilidades en el Tiempo de Resolución de Incidencias en la gestión de incidencias para la Seguridad Informática en una empresa de servicios de tecnología?

- ¿De qué manera impacta el análisis de vulnerabilidades en el Nivel de incidencias atendidas en la gestión de incidencias para la Seguridad Informática en una empresa de servicios de tecnología?

Los eventos de seguridad como los asaltos a la red y las fugas de datos han aumentado en frecuencia recientemente como resultado del rápido crecimiento técnico de industrias como internet de las cosas, cloud computing, big data, e internet móvil. Los enfoques basados en el mecanismo convencional de resguardo de la la información han resultado progresivamente infructuosos, lo que indica que el sistema de información existente se encuentra en un escenario de seguridad crítica. La identificación temprana de las vulnerabilidades y eventos de seguridad informática es crucial para cualquier empresa preocupada por proteger sus valiosos activos y datos en este sentido. He aquí algunas de las principales justificaciones de por qué una empresa debe detectar y gestionar los problemas e incidentes de seguridad informática lo antes posible.

Con todo lo anterior, se plantea el objetivo general:

Determinar el impacto de las vulnerabilidades en las incidencias en la gestión de proyectos de una empresa de servicios de tecnología en Lima, 2023.

Como también los objetivos específicos:

- Determinar de qué manera impacta el análisis de vulnerabilidades en el índice de Vulnerabilidades corregidas en la gestión de incidencias para la Seguridad Informática en una empresa de servicios de tecnología.

- Determinar de qué manera impacta el análisis de vulnerabilidades en el Índice de vulnerabilidades no corregidas en la gestión de incidencias para la Seguridad Informática en una empresa de servicios de tecnología.

- Determinar de qué manera impacta el análisis de vulnerabilidades en el tiempo de Resolución de Incidencias en la gestión de incidencias para la Seguridad Informática en una empresa de servicios de tecnología.

- Determinar de qué manera impacta el análisis de vulnerabilidades en el nivelde incidencias atendidas en la gestión de incidencias para la Seguridad Informática en una empresa de servicios de tecnología.

Asimismo, la hipótesis general: Las vulnerabilidades impactan significativamente en las incidencias en la gestión de proyectos de una empresa de servicios de tecnología en Lima, 2023 y las hipótesis específicas:

- El análisis de vulnerabilidades impacta significativamente en el índice de Vulnerabilidades corregidas en la gestión de incidencias para la Seguridad Informática en una empresa de servicios de tecnología.

- El análisis de vulnerabilidades reduce el Índice de vulnerabilidades no corregidas en la gestión de incidencias para la Seguridad Informática en una empresa de servicios de tecnología.

- El análisis de vulnerabilidades reduce el tiempo de Resolución de Incidencias en la gestión de incidencias para la Seguridad Informática en una empresa de servicios de tecnología.

- El análisis de vulnerabilidades mejora el nivel de incidencias atendidas en la gestión de incidencias para la Seguridad Informática en una empresa de servicios de tecnología.

II. MARCO TEÓRICO

Touloumis et.al (2022) En su artículo titulado “A tool for assisting in the forensic investigation of cyber-security incidents”, “Una herramienta para ayudar en la investigación forense de incidentes de ciberseguridad” mencionan que la capacidad de las redes ha aumentado rápidamente, incluida la Internet de las cosas (IoT), ha provocado una explosión de ciberataques. Muchos ciberataques bien documentados se han dirigido a infraestructuras energéticas críticas, así como a cualquier tipo de plataforma de TI basada en la nube. El examen temprano de las vulnerabilidades de los sistemas críticos, así como los incidentes de seguridad cibernética anteriores, son de suma importancia para prevenir nuevos. Una investigación exhaustiva para examinar el contexto de la violación de seguridad cibernética puede revelar hechos sobre la fuente del ataque, el perfil del atacante, los recursos y las habilidades requeridas y puede revelar más mitigaciones para evitar que el ataque reaparezca en el futuro. Para salvaguardar las infraestructuras energéticas críticas, se han desarrollado muchos enfoques forenses para recopilar, analizar y digitalizar evidencia que ayude en la investigación profunda de un incidente. Sin embargo, hasta ahora, las muchas fuentes de datos de vulnerabilidad de código abierto que se han desarrollado para proporcionar información valiosa para un ataque cibernético aún no se han empleado para ayudar en la investigación forense. Este documento presenta la herramienta forense automatizada, una plataforma que emplea algoritmos de aprendizaje automático para combinar diferentes fuentes de datos de vulnerabilidad para facilitar el procedimiento forense y minimizar el tiempo y el esfuerzo necesarios. También se demuestra un caso de uso que muestra cómo se puede usar la herramienta para ayudar en la investigación forense de incidentes de seguridad cibernética en una infraestructura energética, pero la herramienta también se puede aplicar a otras infraestructuras energéticas y de TI críticas con adaptaciones menores.

Amin y Bhowmik (2022) Desarrollaron su investigación titulado “Existing vulnerability information in security requirements elicitation”, “Información de vulnerabilidad existente en la obtención de requisitos de seguridad”. En de resumen que en ingeniería de software, el aspecto de abordar los requisitos de seguridad se considera de suma relevancia. Sin embargo, en el gran porcentaje de los casos, los

requisitos de seguridad para un sistema se consideran requisitos no funcionales (NFR) y se abordan en el último ciclo de vida del desarrollo del software. El creciente número de incidentes de seguridad en los sistemas de software en todo el mundo ha hecho que los investigadores y desarrolladores reconsideren y consideren este problema en una etapa anterior. Un paso importante y esencial hacia este proceso es la obtención de los requisitos de seguridad pertinentes. En un trabajo reciente, Imtiaz et al. propuso un marco para crear un mapeo entre los requisitos existentes y las vulnerabilidades asociadas con ellos. La idea es que los desarrolladores puedan usar este mapeo para predecir posibles vulnerabilidades asociadas con nuevos requisitos funcionales y capturar requisitos de seguridad para evitar estas vulnerabilidades. Sin embargo, hasta qué punto dicha información de vulnerabilidad existente puede ser útil en la obtención de requisitos de seguridad sigue siendo una pregunta abierta. En este artículo, diseñamos un estudio con sujetos humanos para responder a esta pregunta. También presentamos los resultados de un estudio piloto y discutimos sus implicaciones. Los resultados preliminares muestran que la información de vulnerabilidad existente puede ser un recurso útil para obtener requisitos de seguridad y sienta las bases para un estudio a gran escala.

Álaba, Basurto y Toála (2022) A lo largo de su estudio, cuyo objetivo principal era efectuar un estudio de la literatura sobre las "10 principales vulnerabilidades de los sistemas informáticos del OWASP". Los ataques informáticos han aumentado como consecuencia de los innumerables peligros a los que deben hacer frente los dispositivos actuales conectados a Internet. Es esencial actuar con rapidez identificando las debilidades potenciales que los atacantes pueden explotar para detener estos asaltos. El estudio se centra en esbozar los rasgos y circunstancias de diversas vulnerabilidades. Empleamos el esquema OWASP-Top-10-2021, una metodología de investigación basada en el marco del Open Web Security Project (OWASP) que se centra en la identificación de inseguridades y la información sobre la probabilidad y el efecto técnico. Los resultados también contienen defensas contra estas debilidades.

En conclusión, se presentará un conjunto de recomendaciones de seguridad para sistemas informáticos con el fin de protegerlos adecuadamente.

En el artículo "Análisis de vulnerabilidades en sistemas de información" publicado en la revista peruana "Seguridad y Defensa", el autor Fajardo (2017) explica la importancia del análisis de vulnerabilidades de los sistemas de información. El autor analiza los numerosos tipos de vulnerabilidades de los que pueden aprovecharse los ciberdelincuentes y cómo un análisis rutinario de vulnerabilidades puede detectar problemas de seguridad y solucionarlos antes de que sean aprovechados por atacantes malintencionados. El artículo subraya la obligación de ejecutar medidas de seguridad para salvaguardar los datos importantes de las empresas y organizaciones, y hace hincapié en lo crucial que es contar con personal de seguridad informática cualificado para garantizar que estas medidas se ponen en marcha con eficacia. El ensayo hace un trabajo fantástico al esbozar la importancia del análisis de vulnerabilidades y las medidas de seguridad para certificar la seguridad de los datos en los sistemas de información.

A continuación, algunas definiciones relacionadas al tema:

- **Variable Independiente:** Vulnerabilidades en la seguridad informática

Las vulnerabilidades en seguridad de la información son fallos, debilidades o defectos en el diseño, implementación o funcionamiento de los sistemas informáticos, que pueden ser explotados por los atacantes para comprometer la confiabilidad, integridad o garantía de los datos y sistemas (Alqahtani & Zou, 2021, p. 1).

- **Variable Dependiente:** Incidencias de seguridad informática.

Una incidencia de seguridad informática es cualquier evento que compromete la confiabilidad, integridad o garantía de los datos o sistemas informáticos (Sahin et al., 2021, p. 38).

III. METODOLOGÍA

3.1. Tipo y diseño de Investigación

3.1.1 Tipo de Investigación: Aplicada

La investigación cuantitativa aplicada trata de obtener información y conocimientos a través de la medición y el análisis de datos numéricos utilizando metodología y técnicas cuantitativas. Hace hincapié en la recolección y el análisis de datos verificables y cuantificables para abordar determinados temas de investigación y apoyar para la toma de decisiones. En torno a la investigación cuantitativa aplicada, la palabra "aplicada" se refiere al objetivo de emplear los resultados y conclusiones del estudio para abordar problemas o situaciones del mundo real (Álvarez, 2020). Entre otros campos, la investigación cuantitativa aplicada se emplea con frecuencia en psicología, sociología, economía, educación y salud. Cuando se trata de medir tamaños o frecuencias de ocurrencias y probar hipótesis, el enfoque cuantitativo es aceptable (Hernández, 2018).

Para estos tipos de estudios se recopilan datos numéricos a través de técnicas que incluyen encuestas, cuestionarios, pruebas estandarizadas, análisis estadísticos y experimentos controlados. Estos datos se evalúan y analizan estadísticamente para llegar a conclusiones y emitir juicios razonados. La metodología objetiva y sistemática de la investigación cuantitativa aplicada permite medir variables, establecer vínculos causa-efecto y generalizar las conclusiones a una población más amplia. Su principal objetivo es proporcionar datos cuantitativos fiables e imparciales que puedan utilizarse en situaciones reales para mejorar la toma de decisiones y abordar problemas concretos.

3.1.2 **Diseño:** No experimental

En estos proyectos no se manipulan las variables, los resultados se visualizan de forma natural y luego se analizan. Son muy útiles en variables que no pueden ser manipuladas por sus dificultades o cuestiones éticas (Arispe et.al, 2020).

El estudio se clasifica como no experimental porque no hay un sistema de inducción o manipulación para cambiar una de las variables, sino que el fenómeno se examina a la luz de su propia dinámica, o de cómo se percibe en el contexto del estudio. El estudio también se clasifica como transversal porque los datos se recogen en un momento concreto de cada actividad, en este caso para determinar el nivel de riesgo.

3.1.3 **Instrumentos de aplicación:** Recopilar información (Análisis estadístico).

3.2. Variables y Operacionalización

- **Definición conceptual:**

  Variable Independiente: Vulnerabilidades en la seguridad informática.

  Las vulnerabilidades en seguridad de la información son fallos, debilidades o defectos en el diseño, implementación o funcionamiento de los sistemas informáticos, que pueden ser explotados por los atacantes para comprometer la confiabilidad, integridad o garantía de los datos y sistemas (Alqahtani & Zou, 2021, p. 1).

  Variable Dependiente: Incidencias de seguridad informática.

  Una incidencia de seguridad informática es cualquier suceso que compromete la confiabilidad, integridad o garantía de los datos o sistemas informáticos (Sahin et al., 2021, p. 38).

- **Definición operacional:**

  Variable Independiente: Vulnerabilidades en la seguridad informática

  Se refiere a identificar y describir de manera específica los puntos débiles, fallos o brechas en los sistemas, aplicaciones, redes o dispositivos informáticos que puedan ser explotados por atacantes con el fin de asegurar la integridad, confiabilidad o disposición de la información y los recursos digitales.

  Variable Dependiente: Incidencias de seguridad informática

  Se refiere a eventos o sucesos específicos que involucran amenazas o violaciones de la seguridad en sistemas informáticos, redes, aplicaciones o datos. Estas incidencias pueden abarcar una amplia gama de situaciones, como intentos de acceso no autorizado, malware, robo de información, denegación de servicio, ataques de phishing, entre otros.

- **Indicadores:**

  Enfocándonos en las dimensiones e indicadores para la variable dependiente:

  Dimensión: Vulnerabilidades técnicas: se refiere a las debilidades de seguridad en el software, hardware o infraestructura que podrían ser explotadas por un atacante para comprometer la seguridad. Algunos indicadores para esta dimensión incluyen:

  • **Índice de vulnerabilidades corregidas** es un indicador que mide la proporción de vulnerabilidades conocidas en un sistema o software que han sido solucionadas o corregidas mediante la implementación de parches o actualizaciones de seguridad. Este índice proporciona una medida del nivel de eficacia en la gestión de vulnerabilidades y la respuesta a las amenazas de seguridad. La fórmula para calcular el índice de vulnerabilidades corregidas es la siguiente:

  Índice de Vulnerabilidades Corregidas = (Número de vulnerabilidades corregidas / Número total de vulnerabilidades conocidas) * 100

Este índice se calcula contando el número de vulnerabilidades que se han encontrado y calculando después la proporción de las que se han corregido mediante el uso de parches, actualizaciones u otras técnicas de mitigación. Para calcular el porcentaje, se divide el número de vulnerabilidades que se han corregido por el total del número de vulnerabilidades que se sabe que existen. La cantidad resultante se multiplica por 100.

- **Índice de vulnerabilidades no corregidas:** Es un indicador que calcula el porcentaje de vulnerabilidades conocidas en un sistema o software que aún no han sido corregidas mediante la aplicación de parches o actualizaciones de seguridad. Este indicador proporciona una visión de la eficacia de las prácticas del manejo de parches y actualizaciones de seguridad en una organización. La fórmula del IVNC es la siguiente:

IVNC = (Número de vulnerabilidades no corregidas / Número total de vulnerabilidades conocidas) * 100
Para calcular el IVNC, se cuenta el número de vulnerabilidades que han sido identificadas, pero no se han aplicado los parches o actualizaciones correspondientes. Para calcular el porcentaje, divida esta cantidad por el número total de vulnerabilidades conocidas y, a continuación, multiplique el resultado por 100.

Un IVNC alto puede indicar una falta de atención a la seguridad, una falta de recursos para implementar las actualizaciones necesarias o la obligación de optimizar los procesos de gestión de parches y actualizaciones. Por otro lado, un IVNC bajo sugiere una mayor eficiencia en la corrección de vulnerabilidades y una menor exposición a posibles ataques.

Dimensiones e indicadores para la variable independiente:

Monitoreo y Mejora: El monitoreo y mejora es una dimensión fundamental dentro de la gestión de incidentes. Esta dimensión se enfoca en la supervisión continua de los incidentes, la evaluación de los procesos y la ejecución de

perfeccionamientos para prevenir incidentes futuros y garantizar una gestión eficaz. El monitoreo implica la observación activa y constante de los incidentes que ocurren en un entorno o sistema. Esto se puede lograr mediante la utilización de herramientas de monitoreo, como sistemas de detección de intrusiones, registros de eventos y monitoreo en tiempo real. El objetivo es identificar y registrar los incidentes en el momento que ocurren, lo que permite una respuesta rápida y eficiente. La mejora se enfoca en el análisis de los incidentes y la identificación de oportunidades para fortalecer los procesos y evitar la recurrencia de problemas similares. Esto implica revisar y evaluar los incidentes pasados, identificar las causas raíz, analizar las carencias en los procesos de gestión de incidentes y tomar medidas correctivas para prevenir incidentes similares en el futuro.

• **Tiempo de Resolución de Incidencias:** Este indicador mide la eficiencia del equipo de seguridad al resolver las incidencias de seguridad. Cuanto menor sea el tiempo de resolución, más eficiente será el equipo en mitigar los riesgos. La fórmula para calcular este indicador podría ser:

Tiempo de Resolución de Incidencias = (Tiempo total empleado en resolver incidencias / Número total de incidencias)

Donde:

- Tiempo total empleado en resolver incidencias: La suma del tiempo dedicado a resolver todas las incidencias de seguridad durante un período determinado.
- Número total de incidencias: El total de incidencias de seguridad registradas en ese mismo período.

Este indicador se expresa en unidades de tiempo (por ejemplo, minutos u horas) y permite evaluar la eficiencia en la respuesta y resolución de incidencias de seguridad.

• **Nivel de incidencias atendidas:** Según la guía de ITIL (2019), el indicador denominado "Nivel de incidencias atendidas" es una estadística utilizada para evaluar el rendimiento de un equipo o departamento que gestiona incidencias relacionadas con los servicios de TI. El objetivo de este indicador es comparar el número total de incidentes notificados durante un periodo de tiempo específico con la proporción de incidentes atendidos durante ese mismo periodo.

El cálculo del Nivel de incidencias atendidas puede variar en función de la definición específica adoptada por cada organización. Algunas posibles metodologías para calcular este indicador son las siguientes:

Porcentaje de incidencias atendidas: Esta métrica se obtiene dividiendo el número de incidencias atendidas durante un tiempo determinado entre el total de incidencias registradas en ese mismo período, y luego multiplicando el resultado por 100. Por ejemplo, si se registraron 100 incidencias en un mes y se atendieron satisfactoriamente 80 de ellas, el Nivel de incidencias atendidas sería del 80%.

Nivel de incidencias atendidas = (Número de incidencias atendidas / Total de incidencias registradas) x 100

- **Escala de medición:**

  La opción más adecuada para esta investigación, es la escala de medición "razón", ya que proporciona la capacidad de realizar análisis estadísticos sólidos, establecer relaciones proporcionales, calcular medidas de variabilidad y aplicar técnicas avanzadas de análisis.

Tabla 1 Operacionalización de variables

Tipo	Variable	Definición Conceptual	Definición Operacional	Dimensión	Indicador	Escala de Medición
Independiente	Análisis de Vulnerabilidades en la seguridad informática	Las vulnerabilidades en seguridad de la información son fallos, debilidades o defectos en el diseño, implementación o funcionamiento de los sistemas informáticos, que pueden ser explotados por los atacantes paracomprometer la confiabilidad, integridad o disponibilidad de los datos y sistemas (Alqahtani & Zou, 2021, p. 1).	Las vulnerabilidades informáticas son debilidades o defectos en los sistemas, redes o programas que pueden ser explotados por personas malintencionadas o utilizados accidentalmente por los usuarios sin intención de causar daño. Estas vulnerabilidades podrían permitir el acceso no autorizado, la manipulación de datos, la interrupción del funcionamiento normal del sistema o la ejecución de código malicioso.	Vulnerabilidades técnicas	Índice de Vulnerabilidades corregidas	Razón
					Índice de vulnerabilidades no corregidas	Razón
Dependiente	Incidencias de seguridad informática	Una incidencia de seguridad informática es cualquier suceso que compromete la confiabilidad, integridad o disponibilidad de los datos o sistemas informáticos (Sahin et al., 2021, p. 38).	Los incidentes relacionados con la seguridad informática pueden ser cosas que ocurren o circunstancias que afectan a la seguridad de los sistemas, redes o datos en un entorno informático. Estos sucesos pueden ser indicadores de rendimiento, errores, fallos de calidad o características de los factores, y pueden suponer un riesgo para la privacidad, la precisión o la velocidad de los datos.	Monitoreo y mejora	Tiempo de Resolución de Incidencias	Razón
					Nivel de incidencias atendidas	Razón

Nota: *Elaboración propia*

Como definición operacional:

Tabla 2 Indicadores de Vulnerabilidades Técnicas

DIMENSIÓN	INDICADOR	DESCRIPCIÓN	TÉCNICA	INSTRUMENTO	UNIDAD DE MEDIDA	FÓRMULA
Vulnerabilidades técnicas	Índice de Vulnerabilidades corregidas	Es un indicador que mide la proporción de vulnerabilidades conocidas en un sistema o software que han sido solucionadas o corregidas mediante la implementación de parches o actualizaciones de seguridad. Este índice proporciona una medida del nivel de eficacia en la gestión de vulnerabilidades y la respuesta a las amenazas de seguridad	Fichaje	Ficha	Porcentaje	Índice de Vulnerabilidades Corregidas = (Número de vulnerabilidades corregidas / Número total de vulnerabilidades conocidas) * 100
	Índice de vulnerabilidades no corregidas	Es un indicador que calcula el porcentaje de vulnerabilidades conocidas en un sistema o software que aún no han sido corregidas mediante la aplicación de parches o actualizaciones de seguridad. Este indicador proporciona una visión de la eficacia de las prácticas de gestión de parches y actualizaciones de seguridad en una organización.	Fichaje	Ficha	Porcentaje	Índice de Vulnerabilidades no Corregidas = (Número de vulnerabilidades no corregidas / Número total de vulnerabilidades conocidas) * 100
	Tiempo de Resolución de Incidencias	Este indicador mide la eficiencia del equipo de seguridad al resolver las incidencias de seguridad. Cuanto menor sea el tiempo de resolución, más eficiente será el equipo en mitigar los riesgos. La fórmula para calcular este indicador podría ser:	Fichaje	Ficha	Porcentaje	Tiempo de Resolución de Incidencias = (Tiempo total empleado en resolver incidencias / Número total de incidencias)
Monitoreo y mejora	Nivel de incidencias atendidas	Una estadística utilizada para evaluar lo bien que un equipo o departamento está abordando los problemas relacionados con los servicios de TI es el indicador "Nivel de incidencias atendidos". El objetivo de este indicador es comparar el número total de incidentes notificados durante un periodo de tiempo específico con la proporción de incidentes atendidos durante ese mismo periodo.	Fichaje	Ficha	Porcentaje	Nivel de incidencias atendidas = (Número de incidencias atendidas / Total de incidencias registradas) x 100

Nota: *Elaboración propia*

3.3. Población, muestra muestreo, unidad de análisis

3.3.1. Población: Según Arizmendi (2019), población describe a un grupo de individuos que comparten características similares que permiten a los científicos identificar y medir indicadores relevantes. La población puede consistir en sujetos de investigación que no se limitan a los seres humanos, sino que puede incluir cualquier elemento, documento, encuentro, bicicleta u otro elemento, vivo o no.

Para esta investigación se tiene 4 indicadores en donde el objeto de estudio para los dos primeros indicadores es decir el índice de vulnerabilidades corregidas y no corregidas son los proyectos, entonces se toma como población 30 proyectos, y para los otros dos indicadores el objeto de estudio son las incidencias, y en promedio son 900 incidencias mensuales, estacantidad se toma como la población.

Tabla 3 Definición de la población de los indicadores

Indicador	Tiempo de evaluación	Población
Índice de Vulnerabilidades corregidas	1 mes	30 proyectos
Índice de vulnerabilidades no corregidas	1 mes	30 proyectos
Tiempo de Resolución de Incidencias	1 mes	900 incidencias
Nivel de incidencias atendidas	1 mes	900 incidencias

Nota: Elaboración propia

3.3.2. Muestra: En el contexto de la investigación, una muestra es una selección escogida de personas, cosas o unidades analíticas extraídas de una población más amplia. La muestra se escoge para representar y proporcionar información sobre las características y propiedades de interés en la población, con el objetivo de realizar inferencias válidas y generalizables. La muestra se emplea cuando estudiar o analizar a todos los miembros de una población resulta poco

práctico o no es posible debido a limitaciones de tiempo, recursos o accesibilidad. Para obtener resultados precisos y fiables, se elige en su lugar una muestra que se estima representa a la población.

Fórmula para calcular la muestra

$$n = \frac{Z^2 N}{Z^2 + 4N(EE^2)}$$

Donde:

- n = Tamaño de muestra.
- Z = Nivel de confianza al 95% (1.96) elegido para esta investigación.
- N = Población total del estudio.
- EE = Representa el margen de error siendo un 5% (0.0.5)

Para los dos primeros indicadores la muestra es la misma que la población, por ser una población pequeña, es decir 30 proyecto. Pero para los otros dos, se realiza el cálculo y la muestra es de 269 incidentes

Tabla 4 Definición de la muestra de los indicadores

Indicador	**Población**	**Muestra**
Índice de Vulnerabilidades corregidas	30 proyectos	30 proyectos
Índice de vulnerabilidades no corregidas	30 proyectos	30 proyectos
Tiempo de Resolución de Incidencias	900 incidencias	269 incidencias
Nivel de incidencias atendidas	900 incidencias	269 incidencias

Nota: Elaboración propia

3.3.3. Muestreo: El muestreo se divide en dos categorías principales. Uno de ellos es el muestreo probabilístico, el cual se fundamenta en la probabilidad. Estas

técnicas pretenden garantizar que los miembros de una población tengan las mismas probabilidades de ser elegidos para ser parte de la muestra y representarla. Estos métodos son ampliamente utilizados debido a que buscan lograr una mayor representatividad en la muestra (Hernández y Carpio, 2019).

Para esta tesis se usó el muestreo no probabilístico por comodidad los sujetos fueron elegidos en función de su accesibilidad y proximidad al área de influencia.

3.3.4. Unidad de análisis: En este caso, la unidad de análisis sería "proyectos" y "incidencias". La muestra está compuesta por 30 proyectos y 269 incidencias relacionadas con esos proyectos en un periodo de un mes. Cada proyecto y cada incidencia serían unidades de análisis independientes que se considerarían en el estudio de los datos nacidos de la muestra.

3.4. Técnicas e instrumentos de recolección de datos

El análisis documental es una técnica de investigación que consiste en examinar y evaluar documentos o fuentes escritas para obtener información relevante y significativa. Esta técnica implica un conjunto de pasos e instrucciones que permiten analizar y comprender el contenido de los documentos seleccionados de manera sistemática (Peña, 2022).

Como Instrumento usaremos la ficha de investigación. Una ficha de investigación es un instrumento utilizado para registrar y organizar la información relevante extraída de diferentes fuentes documentales durante el proceso de investigación. La ficha de investigación es una herramienta útil para mantener un registro sistemático de los datos obtenidos y facilitar su posterior análisis y citación en el informe final (Loayza, 2021).

Una hoja de registro es un documento o formulario utilizado para recopilar y almacenar información sobre un individuo, evento, objeto u otro tipo de datos de interés. Esta herramienta facilita la recogida de datos estructurados y estructurados, posibilitando su posterior consulta, análisis y gestión eficiente. En esta investigación se elaboraron dos fichas durante un mes de acuerdo a las técnicas de cada indicador para el test y Re test respectivo.

Ficha de registro N°1: Indicador índice de vulnerabilidades

Ficha de registro N°2: Indicador tiempo de resolución de incidencias

El análisis de confiabilidad técnica es una técnica que permite a un investigador utilizar enfoques estándar para evaluar la relación inicial entre un instrumento y un sujeto para determinar la confiabilidad de un instrumento. Se utilizan diversos métodos, como el uso de indicadores como el coeficiente de Pearson, así como pruebas observacionales y pruebas escritas de conocimiento. Para evaluar la confiabilidad del formulario de recolección de datos, deben registrarse en una tabla separada los resultados (Correa, 2019).

Figura 5 Nivel de confiabilidad

Escala	Nivel
0.00 < sig. <0.20	Muy bajo
0.20 ≤ sig. < 0.40	Bajo
0.40 ≤ sig. < 0.60	Regular
0.60 ≤ sig. < 0.80	Aceptable
0.80 ≤ sig. < 1.00	Elevado

Nota*:* Se obtuvo de Correa (2019)

3.5. Procedimientos

Al principio, los datos sobre los indicadores se recogen mediante una pre-test, es decir, antes de poner en marcha el programa. Estos datos se recogen utilizando una tabla de recogida de datos y basándose en una muestra elegida.

Se aplica naturalmente ya que el enfoque de este trabajo incluye el diseño y ejecución de software para encontrar soluciones a los desafíos de gestión de mantenimiento. Este estudio se basa en el uso de instrucciones detalladas el análisis de las técnicas de uso de esta tecnología y los resultados obtenidos de los indicadores.

Dado que se trata de una prueba piloto previa, esta investigación se lleva a cabo como un experimento que debe evaluarse al menos dos veces. Mediante el Análisis de vulnerabilidades e Incidencias en la Seguridad Informática en una empresa de servicios de tecnología.

Asimismo, al medir los indicadores, índice de vulnerabilidades y tiempo de resolución de incidencias, los datos recolectados se llevarán a cabo manejando las fichas de recolección de datos, y se analizarán a través las muestras definidas en los momentos designados como pretest.

Durante el pretest, los datos se recopilarán manualmente utilizando la técnica de fichaje y el instrumento de ficha de datos recolectados, contando con las facilidades de la organización para recolectar la información necesaria.

Se procede con el análisis descriptivo, lo cual consiste en describir los valores obtenidos en ambos resultados. Luego, se realiza una validación estadística a través de la prueba de normalidad para establecer la colocación de los valores registrados. Una vez que los datos han sido analizados, es posible determinar si se debe admitir la hipótesis alternativa y rechazar la hipótesis nula.

3.6. Método de análisis de datos

El análisis de los datos recolectados a través del enfoque cuantitativo permite al investigador adquirir destrezas y recursos para examinar e interpretar los hallazgos (Blanco, 2021).

Los resultados anteriores y posteriores a la prueba se resumen en el análisis descriptivo, que también proporciona datos sobre la media, el mínimo, el máximo y el rango posterior de los resultados experimentales. Su objetivo es elaborar un resumen de los resultados. (Fávero, 2020).

En cuanto a la prueba de normalidad, esta evaluación nos permite observar la distribución de los datos recogidos para determinar qué método utilizar en la comprobación de hipótesis. El análisis descriptivo implica resumir los resultados del pre-tes y post-test, proporcionando información como la media, el mínimo, el máximo y el rango posterior si el tamaño previsto de la muestra es menor a 50, se aplican pruebas como las de Shapiro-Wilk y Kolmogorov. Si los niveles de significación de ambas pruebas son superiores o iguales a 0,05, se dice que la distribución es normal. Ambas pruebas proporcionan dos valores de salida conocidos como niveles de significación. Los resultados experimentales se analizan usando la prueba de

Wilcoxon en lugar de la prueba t de Student si la distribución es anormal. Su objetivo es elaborar un resumen de los resultados. (Fávero, 2020).

El objetivo de la prueba de hipótesis es aceptar la hipótesis alternativa al tiempo que se rechaza la hipótesis nula. La hipótesis nula se evalúa para ver si cae dentrode la zona de rechazo después de crearla junto con una hipótesis alternativa. El objetivo es determinar si hay datos suficientes para respaldar la hipótesis alternativa (Fávero, 2020).

3.7. Aspectos éticos

La investigación presentada cumple con las normas éticas y moralesestablecidas por el equipo investigador peruano, así como la Ley Nacional de Integridad Científica del Consejo Nacional de Ciencia, Tecnología e Innovación Tecnológica (CONCYTEC) y el Código Ético y Moral de la Universidad César Vallejo(2016). Estos valores incluyen la pericia, corrección, profesionalismo y honestidad delos investigadores que intentan el avance de la ciencia. El autor no pretende poseer ni beneficiarse de ninguna propiedad intelectual que aparezca en este estudio; simplemente se utiliza con fines educativos. Así mismo se adhiere firmemente a los principios éticos universales que guían la investigación científica y académica a nivel internacional. Se busca asegurar la integridad, la imparcialidad y el respeto hacia todos los actores implicados en el proceso de investigación, así como hacia los sujetos de estudio y la comunidad científica en general.

IV. ASPECTOS ADMINISTRATIVOS

4.1 Recursos y Presupuestos

4.1.1. Recursos

Recursos Humanos: para el presente proyecto se emplearán los siguientes recursos humanos:

Tabla *5* Tabla de recursos humanos

Nombre	Cargo	Descripción
Ing. Sanchez Rueda, Jose Luis	Jefe de proyecto, Analista desarrollador	Encargada de realizar los procesos de planificación y efectuar las tareas importantes para la ejecución del proyecto.

Nota: Elaboración propia

Recursos Materiales: Se emplearán los siguientes materiales:

- **Materiales:**

Tabla 6 Tabla de materiales

Descripción	Cantidad	Mes 1	Mes 2	Mes 3	Mes 4	Total
Equipos tecnológicos						
Laptop	1	-	-	-	-	-
Computadora	1	-	-	-	-	-
Equipo móvil	1	-	-	-	-	-
Software						
Windows 10 Pro	1	-	-	-	-	-
Microsoft Office 2018	1	-	-	-	-	-
Antivirus Avast	**1**	**-**	**-**	**-**	**-**	**-**
Hardware						
Memoria Ram DDR4 4GB	1	-	-	S/ 220.00	-	S/ 220.00
TOTAL						**S/ 265.48**

- **Asesorías especializadas**

Tabla 7 Tabla de asesorías especializadas

Nombre	Cargo
Mg. Poletti Gaitan, Eduardo Humberto	Asesor metodológico y temático
Mg. Tejada Ruiz, Roberto Juan	Asesor metodológico y temático

Nota: Elaboración propia

- **Gastos operativos**

Tabla 8 Tabla gastos operativos

Clasificador de gastos	Descripción	Mes 1	Mes 2	Mes 3	Mes 4	Monto total
Viajes						
2.3.1.2	Pasajes, transporte	S/ 80.00	S/ 80.00	S/ 80.00	S/ 80.00	S/ 320.00
Servicios						
2.3.1.3	Servicio de energía eléctrica	S/ 75.00	S/ 75.00	S/ 75.00	S/ 75.00	S/ 300.00
2.3.1.4	Servicios de Telefonía e Internet	S/ 100.00	S/ 100.00	S/ 100.00	S/ 100.00	S/ 400.00
TOTAL						**S/ 1,020.00**

Nota: Elaboración propia

4.1.2.- Presupuesto

Tabla 9 Presupuesto

Rubros	Aporte monetario	
	Descripción	**Costo**
Recursos Humanos	Ing. Sanchez Rueda, Jose Luis	**S/ 0.00**
Recursos Materiales	Materiales	
	Memoria Ram DDR4	**S/ 35.48**
	4GB	**S/ 10.00**
	Gastos operativos	**S/ 220.00**

	Pasajes, transporte	
	Servicio de energía eléctrica	**S/ 265.48**
	Servicios de Telefonía e Internet	**S/ 320.00**
		S/ 300.00
		S/ 400.00
		S/ 1,020.00
TOTAL		S/ 1,285.48

Nota: Elaboración propia

4.2 Financiamiento

Se detalla el aporte de inversión de este proyecto que será financiado por el autor de este estudio.

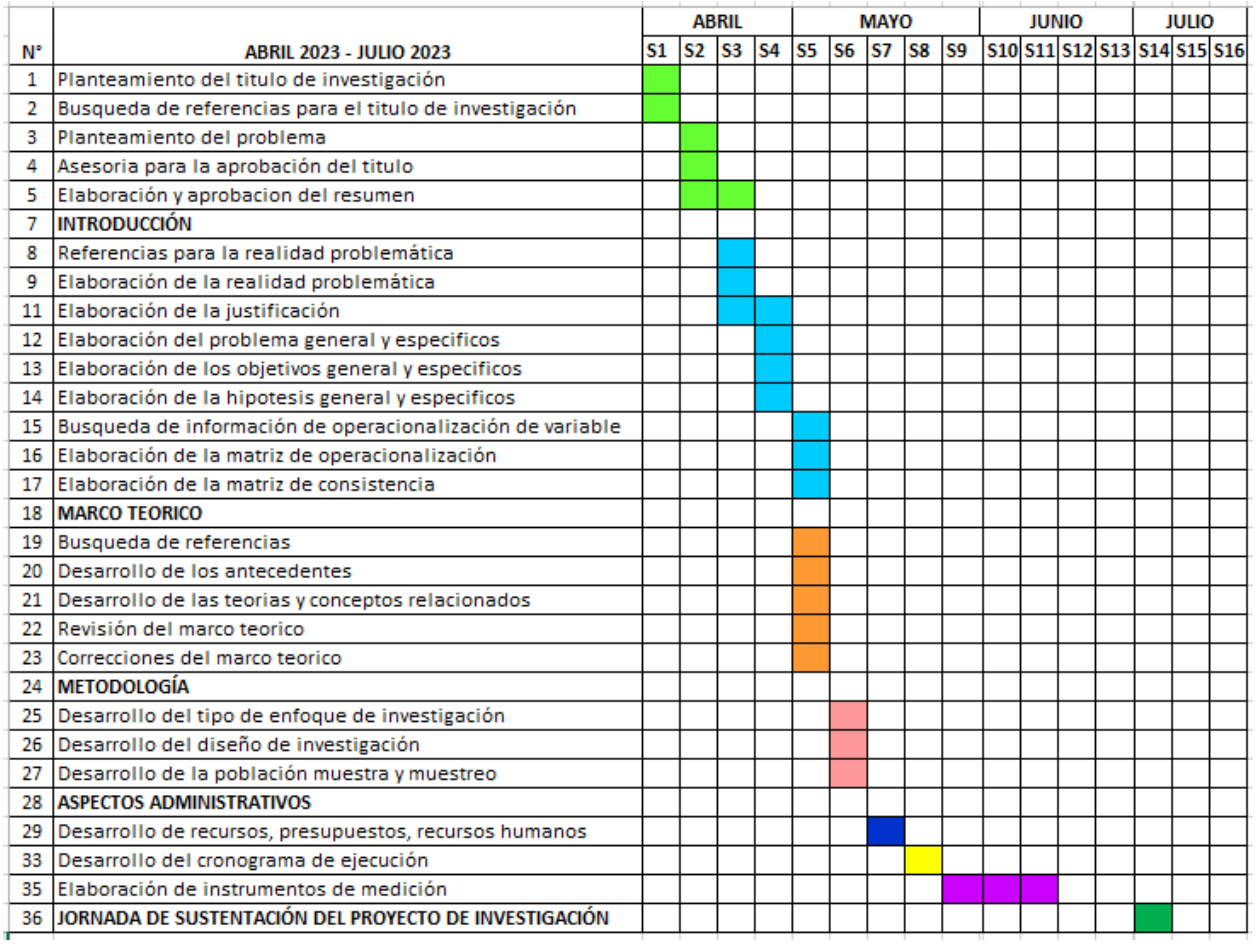
Tabla 10 Financiadores

Entidad financiera	**Monto**	**Porcentaje**
Ing. Sanchez Rueda, Jose Luis	S/. 1,285.00	100%

Nota: Elaboración propia

4.3 Cronograma de Ejecución

Figura 6 Cronograma de ejecución



N°	ABRIL 2023 - JULIO 2023	ABRIL				MAYO					JUNIO				JULIO		
		S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12	S13	S14	S15	S16
1	Planteamiento del titulo de investigación																
2	Busqueda de referencias para el titulo de investigación																
3	Planteamiento del problema																
4	Asesoria para la aprobación del titulo																
5	Elaboración y aprobacion del resumen																
7	**INTRODUCCIÓN**																
8	Referencias para la realidad problemática																
9	Elaboración de la realidad problemática																
11	Elaboración de la justificación																
12	Elaboración del problema general y especificos																
13	Elaboración de los objetivos general y especificos																
14	Elaboración de la hipotesis general y especificos																
15	Busqueda de información de operacionalización de variable																
16	Elaboración de la matriz de operacionalización																
17	Elaboración de la matriz de consistencia																
18	**MARCO TEORICO**																
19	Busqueda de referencias																
20	Desarrollo de los antecedentes																
21	Desarrollo de las teorias y conceptos relacionados																
22	Revisión del marco teorico																
23	Correcciones del marco teorico																
24	**METODOLOGÍA**																
25	Desarrollo del tipo de enfoque de investigación																
26	Desarrollo del diseño de investigación																
27	Desarrollo de la población muestra y muestreo																
28	**ASPECTOS ADMINISTRATIVOS**																
29	Desarrollo de recursos, presupuestos, recursos humanos																
33	Desarrollo del cronograma de ejecución																
35	Elaboración de instrumentos de medición																
36	**JORNADA DE SUSTENTACIÓN DEL PROYECTO DE INVESTIGACIÓN**																

Nota: Elaboración Propia

V. RESULTADOS

En este apartado se muestran los resultados empíricos de dos fases: antes y después del análisis de vulnerabilidades e incidentes. El objetivo de este diagnóstico es determinar cómo afectan los análisis de vulnerabilidades e incidentes a la seguridad informática. Los resultados se presentan con un resumen analítico al principio. A continuación, se utiliza una prueba de normalidad para evaluar la distribución de los datos obtenidos. Por último, la hipótesis nula se rechaza intencionadamente durante la prueba de hipótesis, mientras que la hipótesis alternativa se acepta activamente.

5.1 Análisis descriptivo

En primer término, se lleva a cabo el desarrollo del análisis descriptivo, lo cual se trata de una descripción detallada de los resultados derivados tanto en la evaluación previa al Test como en la evaluación posterior al Test.

Vulnerabilidades corregidas

En la próxima tabla se presentan los resultados de la apreciación del indicador de vulnerabilidades corregidas, comparando la evaluación previa al análisis de vulnerabilidades e incidencias con la evaluación posterior al análisis. Inicialmente, el nivel de vulnerabilidades corregidas obtenido fue del 52.46%, el cual experimentó un incremento significativo hasta alcanzar un 75.1%, lo que representa un aumento del 22.64%. En cuanto a los valores mínimos registrados, fueron del 31% y 56%, mientras que los valores máximos fueron del 79% y 87% respectivamente, antes y después del análisis de vulnerabilidades e incidencias.

Tabla 11 Resultados descriptivos para vulnerabilidades corregidas

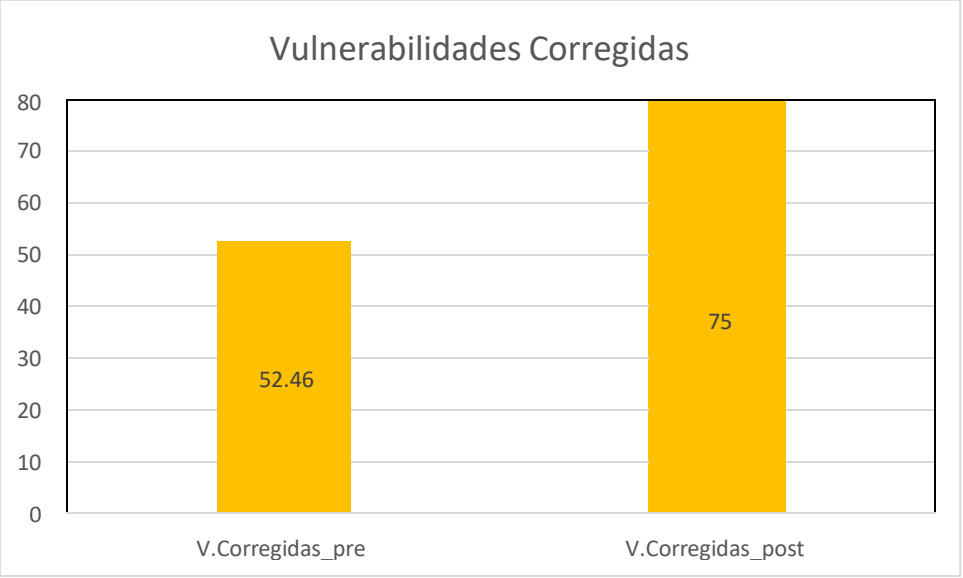
Estadísticos descriptivos

	N	Mínimo	Máximo	Media	Desviación estándar
pre_VC	30	31,00	79,00	52,4667	10,78547
post_VC	30	56,00	87,00	75,1000	7,81841
N válido (por lista)	30				

Nota: Elaboración propia

La siguiente figura muestra un histograma comparativo que representa de manera general los resultados obtenidos en el análisis descriptivo. En dicho análisis, se visualiza que el porcentaje de vulnerabilidades corregidas antes del análisis fue del 52.46%, mientras que después del análisis aumentó al 75%. Esto demuestra claramente que hubo un aumento relevante en el porcentaje de vulnerabilidades corregidas.

Figura 7 Comparativo de los resultados de vulnerabilidades corregidas



Nota: Elaboración propia

Vulnerabilidades no corregidas

En la próxima tabla se presentan los resultados de la estimación del indicadorde vulnerabilidades no corregidas, comparando la evaluación previa al análisis de vulnerabilidades e incidencias con la evaluación posterior al análisis. Inicialmente, el nivel de vulnerabilidades no corregidas obtenido fue del 47.56%, el cual experimentó una disminución significativa hasta alcanzar un 24.96%, lo que representa una disminución del 22.6%. En cuanto a los valores mínimos registrados, fueron del 21% y 13%, mientras que los valores máximos fueron del 69% y 44% respectivamente, antes y después del análisis de vulnerabilidades e incidencias.

Tabla 12 Resultados descriptivos para vulnerabilidades no corregidas

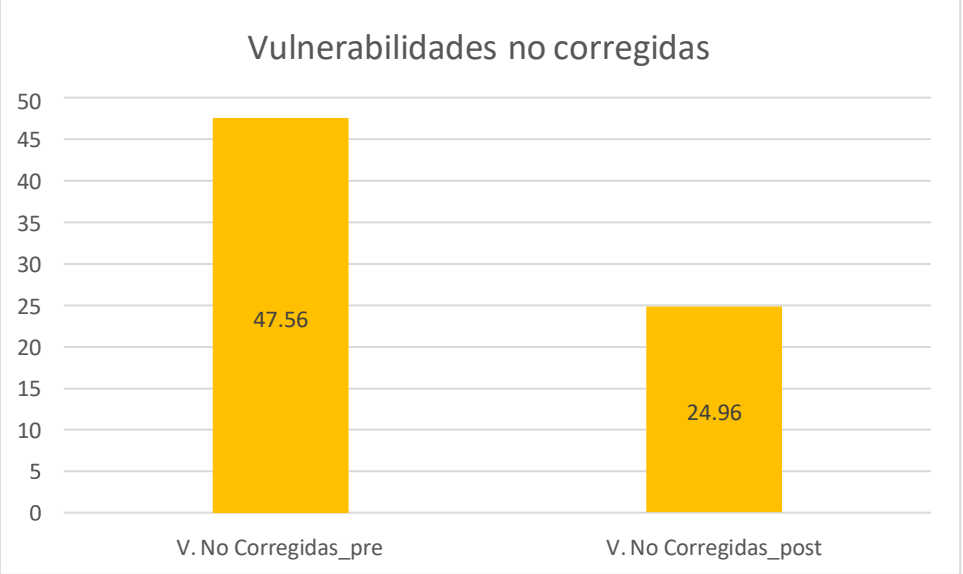
Estadísticos descriptivos

	N	Mínimo	Máximo	Media	Desviación estándar
pre_VNC	30	21,00	69,00	47,5667	10,75329
post_VNC	30	13,00	44,00	24,9667	7,92849
N válido (por lista)	30				

Nota: Elaboración propia

La siguiente figura muestra un histograma comparativo que representa de manera general los resultados obtenidos en el análisis descriptivo. En dicho análisis, se visualiza que el porcentaje de vulnerabilidades corregidas antes del análisis fue del 47.56%, mientras que después del análisis disminuyó al 24.96%. Esto demuestra inequívocamente que el porcentaje de vulnerabilidades que siguen sin corregirse ha disminuido significativamente.

Figura 8 Comparativo de los resultados de vulnerabilidades no corregidas



Nota: Elaboración propia

Nivel de incidencias atendidas

Los resultados de la evaluación de los incidentes atendidos se exponen en la siguiente tabla, que compara las evaluaciones realizadas antes y después de la investigación de vulnerabilidades e incidentes. Inicialmente, el nivel de incidencias

atendidas obtenido fue del 42.60%, el cual experimentó un aumento significativo hasta alcanzar un 77.35%, lo que representa un aumento del 34.75%. En cuanto a los valores mínimos registrados, fueron del 27% y 60%, mientras que los valores máximos fueron del 64% y 92% respectivamente, antes y después del análisis de vulnerabilidades e incidencias.

Tabla 13 Comparativo de los resultados de Nivel de incidencias atendidas

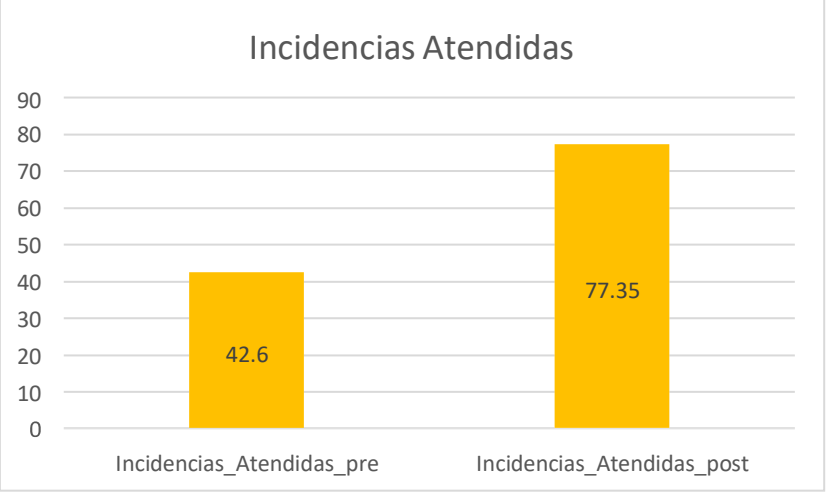
Estadísticos descriptivos

	N	Mínimo	Máximo	Media	Desv. Desviación
nivel_incidencias_atendidas_pre	20	27,00	64,00	42,6000	10,02838
nivel_incidencias_atendidas_post	20	60,00	92,00	77,3500	7,63148
N válido (por lista)	20				

Nota: Elaboración propia

La siguiente figura muestra un histograma comparativo que representa de manera general los resultados obtenidos en el análisis descriptivo. En dicho análisis, se representa que el porcentaje de incidencias atendidas antes del análisis fue del 42.60%, mientras que después del análisis aumentó al 77.35%. Esto demuestra claramente que hubo un incremento significativo en el porcentaje de incidencias atendidas.

Figura 9 Comparativo de los resultados de incidencias atendidas



Nota: Elaboración propia

Tiempo de resolución de incidencias

En la siguiente tabla se presentan los resultados de la evaluación del indicador de tiempo de resolución de incidencias, comparando la evaluación previa al análisis de vulnerabilidades e incidencias con la evaluación posterior al análisis. Inicialmente, el tiempo de resolución de incidencias obtenido fue del 2.13 horas, el cual experimentó una disminución significativa hasta alcanzar un 1.29 horas, lo que representa una disminución del 0.84. En cuanto a los valores mínimos registrados, fueron del 1.08 y 0.83%, mientras que los valores máximos fueron del 3.33 y 2.23 respectivamente, antes y después del análisis de vulnerabilidades e incidencias.

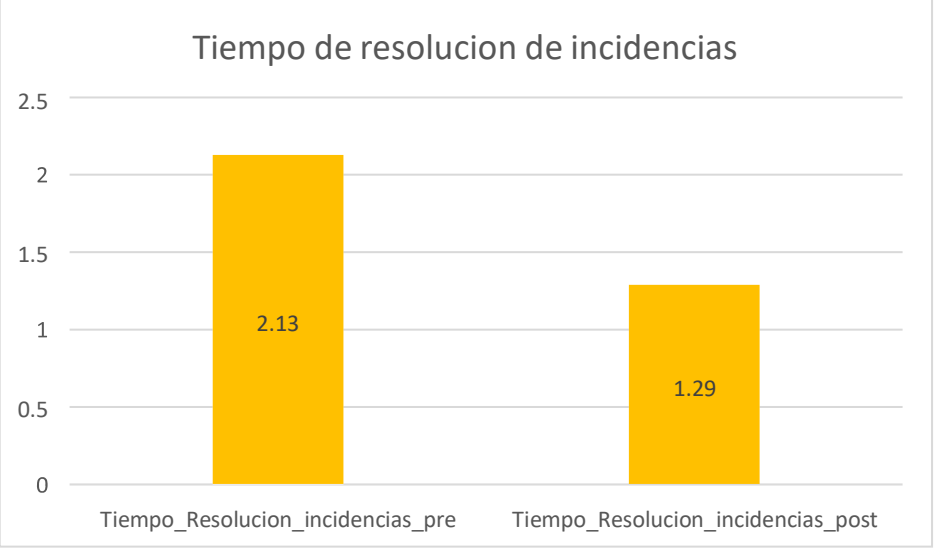
Tabla 14 Comparativo de los resultados de tiempo de resolución de incidencias

Estadísticos descriptivos

	N	Mínimo	Máximo	Media	Desv. Desviación
Tiempo_resolucion_incidencias_pre	20	1,08	3,33	2,1370	,52127
Tiempo_resolucion_incidencias_post	20	,83	2,23	1,2900	,34026
N válido (por lista)	20				

Nota: Elaboración propia

Figura 10 Comparativo de los resultados de tiempo de resolución de incidencias



Nota: Elaboración propia

5.2 Prueba de normalidad

A continuación, se utiliza la prueba de normalidad para determinar cómo se distribuyen los resultados. Cuando el tamaño de la muestra es menor a 50 individuos, el autor aconseja utilizar la prueba de Shapiro-Wilk. En cambio, si el tamaño de la muestra es superior a 50 individuos, se usan los resultados de la prueba de Kolmogorov-Smirnov. Según este criterio, la distribución se considera normal si el nivel de significación es mayor o igual a 0,05. En caso contrario, se considera que la distribución no es normal si los niveles de significancia no satisfacen esta estipulación.

Vulnerabilidades corregidas

Los resultados de la prueba de normalidad para el indicador de vulnerabilidad actualizado se muestran en la tabla siguiente. En este caso, se evaluaron un total de 30 registros, lo que sugiere que, de acuerdo con el criterio mencionado, deben utilizarse los resultados de la prueba de Shapiro-Wilk en lugar de los resultados del autor de Kolmogorov.

Los resultados obtenidos para el primer tiempo fueron de 0.970, mientras que para el segundo tiempo fueron de 0.172. Estos valores validan que ambos sean mayores a 0.05, lo cual indica que la distribución del indicador de porcentaje de eficiencia es normal o paramétrica.

En visto que los resultados indican una distribución normal, se utilizará la prueba de t-student para la prueba de hipótesis.

Tabla 15 Resultados de la prueba de normalidad para el indicador vulnerabilidades corregidas

Pruebas de normalidad

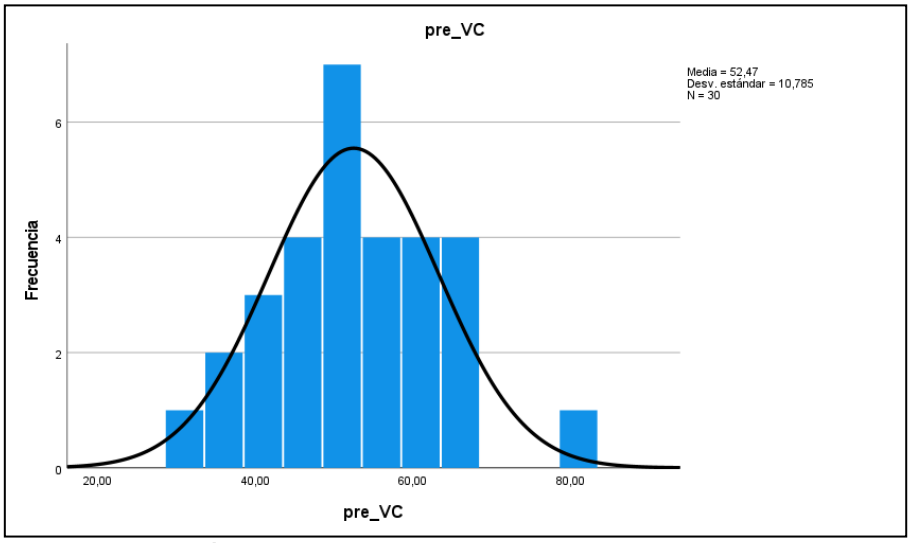
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
pre_VC	,076	30	,200*	,987	30	,970
post_VC	,158	30	,055	,950	30	,172

*. Esto es un límite inferior de la significación verdadera.

a. Corrección de significación de Lilliefors

Nota: Elaboración propia

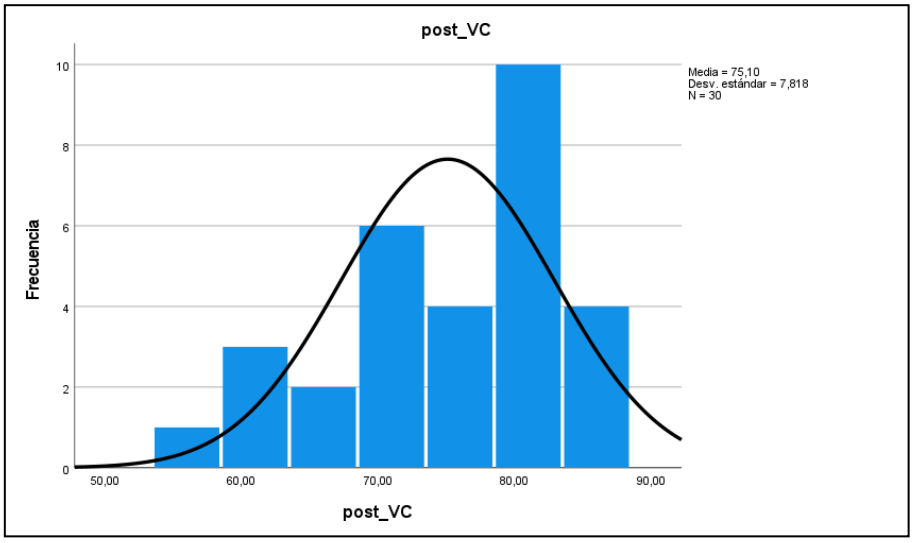
Figura 11 Distribución de los resultados del pre test de vulnerabilidades corregidas



Nota: Elaboración propia

En la anterior figura se representa la distribución de los resultados del pre Test para el indicador vulnerabilidades corregidas. En aquella figura, se visualiza que el promedio obtenido fue de 52.47, con una desviación estándar de 10.785, basado en un total de 30 objetos de estudio.

Figura 12 Distribución de los resultados del post test de vulnerabilidades corregidas



Nota: Elaboración propia

En la anterior figura se representa la distribución de los resultados del pre Test para el indicador vulnerabilidades corregidas. En dicha figura, se visualiza que el promedio obtenido fue de 75.10, con una desviación estándar de 7.818, basado en un total de 30 objetos de estudio.

Vulnerabilidades no corregidas

La prueba de normalidad realizada para el indicador de vulnerabilidad no corregido se muestra en la tabla siguiente. En este caso, se evaluaron un total de 30 registros, lo que sugiere que, de acuerdo con el criterio mencionado, deben utilizarse los resultados de la prueba de Shapiro-Wilk en lugar de los resultados del autor de Kolmogorov.

Los resultados obtenidos para el primer tiempo fueron de 0.973, mientras que para el segundo tiempo fueron de 0.126. Estos valores validan que ambos sean mayores a 0.05, lo cual refiere que la distribución del indicador de porcentaje de eficiencia es normal o paramétrica.

En vista que los resultados indican una distribución normal, se utilizará la prueba de t-student para la prueba de hipótesis.

Tabla 16 Resultados de la prueba de normalidad para el indicador vulnerabilidades corregidas

Pruebas de normalidad

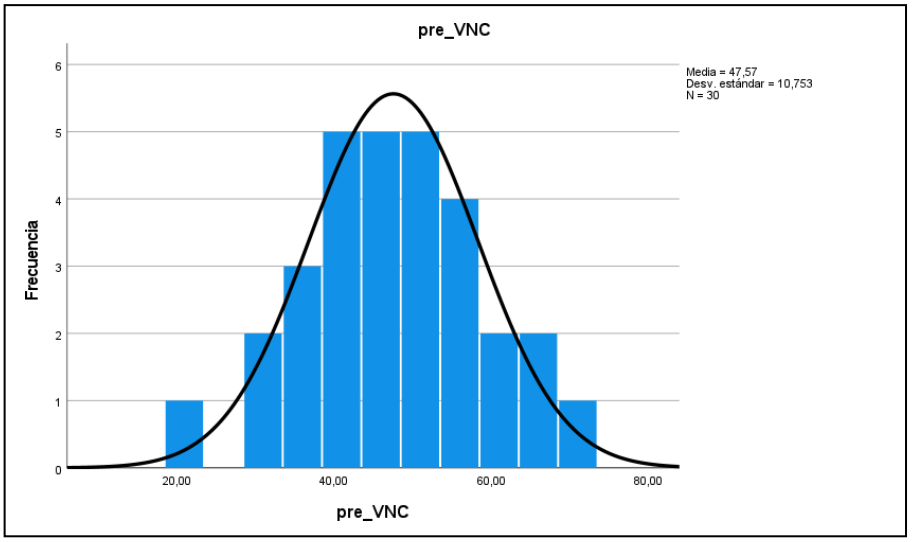
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
pre_VNC	,077	30	,200*	,988	30	,973
post_VNC	,158	30	,053	,945	30	,126

*. Esto es un límite inferior de la significación verdadera.

a. Corrección de significación de Lilliefors

Nota: Elaboración propia

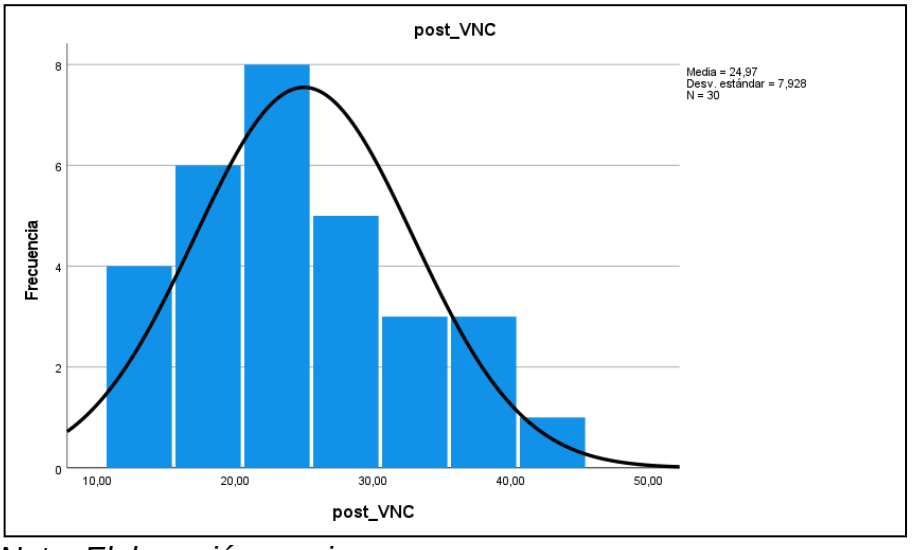
Figura 13 Distribución de los resultados del pre test de vulnerabilidades no corregidas



Nota: Elaboración propia

En la anterior figura se representa la repartición de los resultados del pre Test para el indicador vulnerabilidades corregidas. En dicha figura, se visualiza que el promedio obtenido fue de 47.57, con una desviación estándar de 10.753, basado en un total de 30 objetos de estudio.

Figura 14 Distribución de los resultados del post test de vulnerabilidades no corregidas



Nota: Elaboración propia

En la figura anterior se representa la distribución de los resultados del pre Test para el indicador vulnerabilidades corregidas. En esta figura, se visualiza que el

promedio obtenido fue de 24.97, con una desviación estándar de 7.928, basado en un total de 30 objetos de estudio

Nivel de incidencias atendidas

La prueba de normalidad realizada para la indicación del nivel de incidentes atendidos se muestra en la tabla siguiente. En este caso, se evaluó un total de 20 registros, lo que sugiere utilizar las evidencias de la prueba de Shapiro-Wilk en lugar de los resultados del autor de Kolmogorov, de acuerdo con el criterio mencionado.

Los resultados obtenidos para el primer tiempo fueron de 0.781, mientras que para el segundo tiempo fueron de 0.939. Estos valores validan que ambos sean mayores a 0.05, lo cual revela que la distribución del indicador de porcentaje de eficiencia es normal o paramétrica.

Dado que los resultados indican una distribución normal, se utilizará la prueba de t-student para la prueba de hipótesis.

Tabla 17 Resultados de la prueba de normalidad para el indicador nivel de incidencias atendidas

Pruebas de normalidad

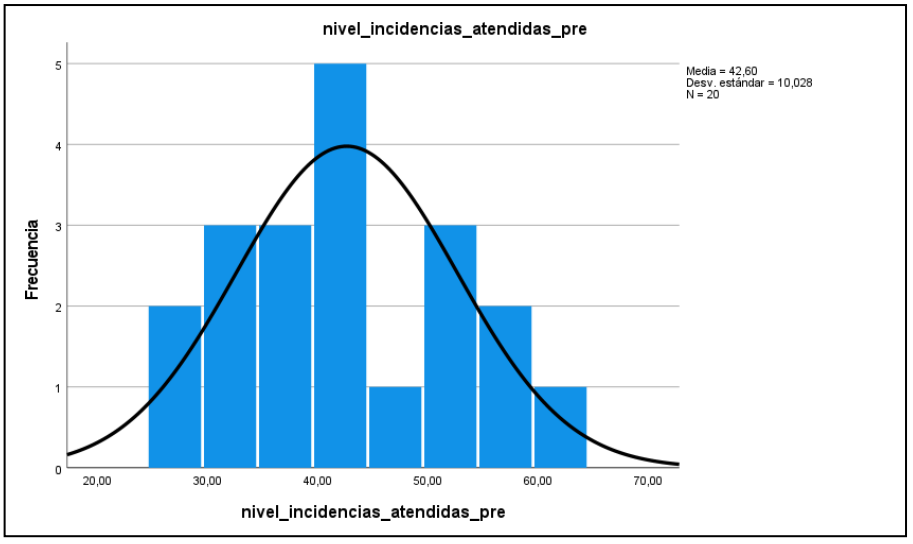
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
nivel_incidencias_atendidas_pre	,134	20	,200*	,971	20	,781
nivel_incidencias_atendidas_post	,129	20	,200*	,980	20	,939

*. Esto es un límite inferior de la significación verdadera.

a. Corrección de significación de Lilliefors

Nota: Elaboración propia

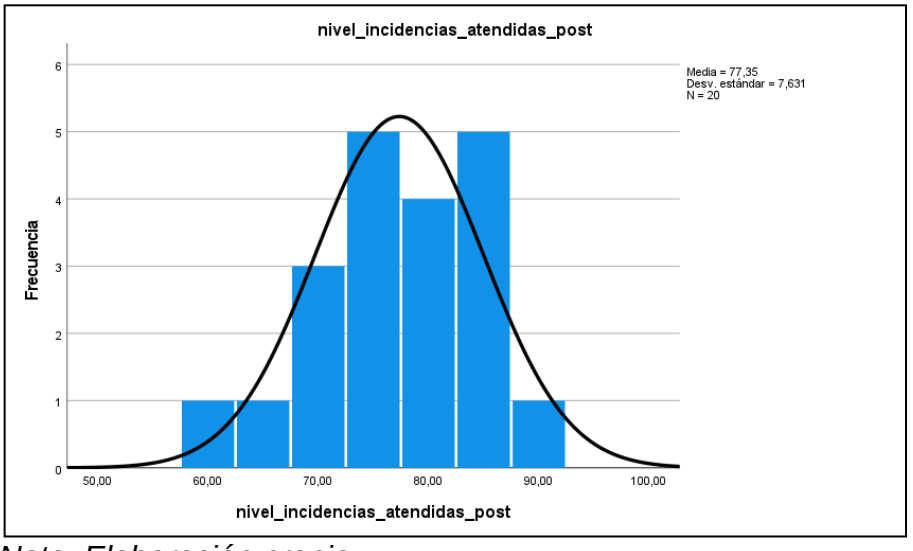
Figura 15 Distribución de los resultados del pre test de Nivel de incidencias atendidas



Nota: Elaboración propia

En la figura anterior se representa la distribución de los resultados del pre Test para el indicador vulnerabilidades corregidas. En esta figura, se visualiza que el promedio obtenido fue de 42.60, con una desviación estándar de 10.028, basado en un total de 20 objetos de estudio.

Figura 16 Distribución de los resultados del post test de Nivel de incidencias atendidas



Nota: Elaboración propia

En la figura anterior se representa la distribución de los resultados del pre Test para el indicador vulnerabilidades corregidas. En esta figura, se visualiza que el promedio obtenido fue de 77.35, con una desviación estándar de 7.631, basado en un total de 20 objetos de estudio.

Tiempo de resolución de incidencias

La prueba de normalidad realizada para el indicador del nivel de incidentes atendidos se muestra en la tabla siguiente. El hecho de que en este caso se hayan analizado 20 registros en total sugiere que, de acuerdo con el criterio mencionado, se utilicen los resultados de la prueba de Shapiro-Wilk en lugar de los resultados del autor de Kolmogorov.

Los resultados obtenidos para el primer tiempo fueron de 0.774, mientras que para el segundo tiempo fueron de 0.066. Estos valores validan que ambos sean mayores a 0.05, lo cual revela que la distribución del indicador de porcentaje de eficiencia es normal o paramétrica.

Dado que los resultados indican una distribución normal, se utilizará la prueba de t-student para la prueba de hipótesis.

Tabla 18 Resultados de la prueba de normalidad para el indicador Tiempo de resolución de incidencias

Pruebas de normalidad

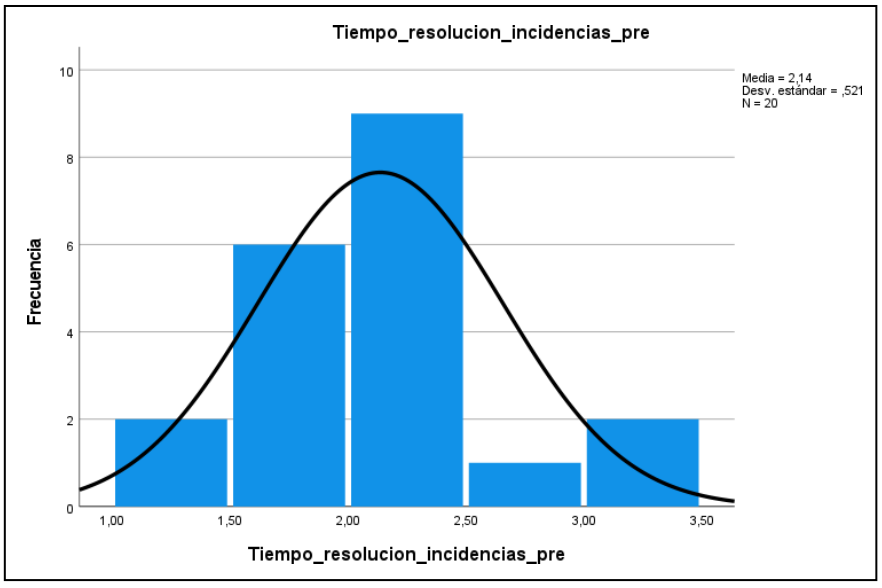
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Tiempo_resolucion_incidencias_pre	,122	20	,200*	,971	20	,774
Tiempo_resolucion_incidencias_post	,157	20	,200*	,911	20	,066

*. Esto es un límite inferior de la significación verdadera.

a. Corrección de significación de Lilliefors

Nota: Elaboración propia

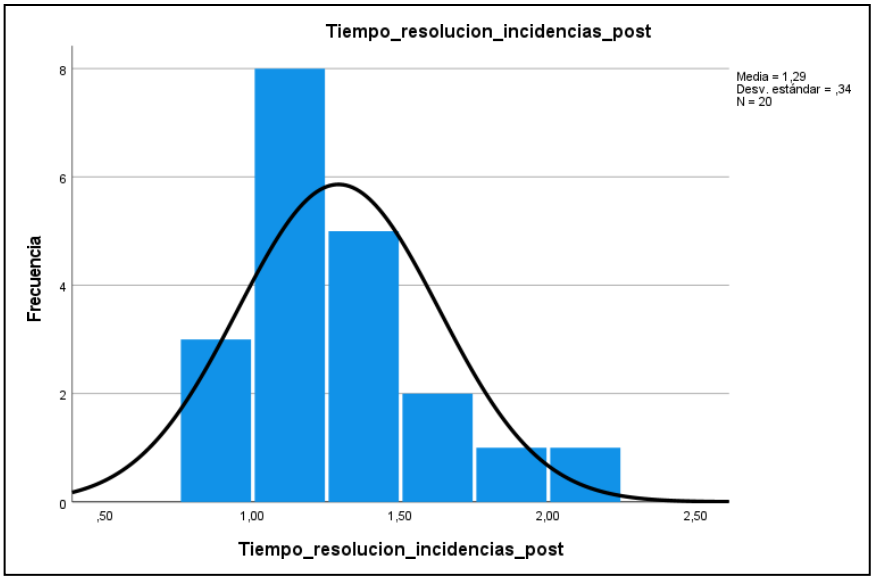
Figura 17 Distribución de los resultados del pre test de Tiempo de resolución de incidencias



Nota: Elaboración propia

En la anterior figura se representa la distribución de los resultados del pre Test para el indicador vulnerabilidades corregidas. En esta figura, se visualiza que el promedio obtenido fue de 2.14, con una desviación estándar de 0.521, basado enun total de 20 objetos de estudio.

Figura 18 Distribución de los resultados del post test de Tiempo de resolución de incidencias



Nota: Elaboración propia

En la anterior figura se representa la distribución de los resultados del pre Test para el indicador vulnerabilidades corregidas. En dicha figura, se observa que el promedio obtenido fue de 1.29, con una desviación estándar de 0.34, basado en un total de 20 objetos de estudio.

5.3 Prueba de hipótesis

A continuación, se lleva a cabo la prueba de hipótesis con el propósito de establecer la región de rechazo y la región de aceptación, para así poder rechazar la hipótesis nula y aceptar la hipótesis alternativa.

Vulnerabilidades corregidas

La evaluación mediante los resultados de la prueba t-student para dos muestras relacionadas se muestra en la tabla siguiente. Los resultados exponen quese obtuvo una media de -22,5 con una desviación típica de 12,53. El valor t estimadofue de -9,864, el valor de los grados de libertad (gl) fue de 29 y se tuvo en cuenta el nivel de confianza del 95%.

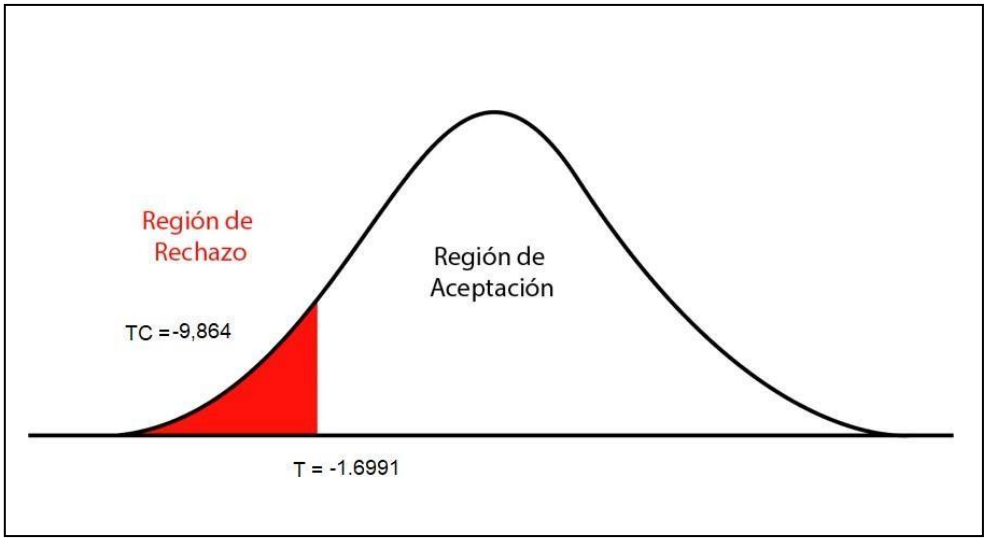
Tabla 19 Prueba t-student para el indicador vulnerabilidades corregidas

Prueba de muestras emparejadas						
		Media	Desviación estándar	t	gl	Sig. (bilateral)
Par 1	Indice_vulnerabilidades_corregidas_pre - Indice_vulnerabilidades_corregidas_post	-22,56733	12,53063	-9,864	29	,000

Nota: Elaboración propia

El valor crucial de la tabla t-student, que se define por la intersección del grado de libertad (gl) y el nivel de confianza establecido, se compara con el valor Tproducido. En este caso, el valor crucial fue -1,6991. Se rechaza la hipótesis nula al observar que el valor de T es menor que el valor crítico.

Figura 19 Zona de rechazo para el indicador vulnerabilidades corregidas



Nota: Elaboración propia

Por todo lo anterior se puede llegar a la conclusión que una aplicación de seguridad aumenta las vulnerabilidades corregidas en la Seguridad Informática en una organización de servicios de tecnología.

Vulnerabilidades no corregidas

La evaluación mediante los resultados de la prueba t-student para dos muestras conexas se muestra en la tabla siguiente. Según los resultados, la media adquirida fue de 22,6 y la desviación standar de 12,49. El valor t estimado fue de -9,909 con un grado de libertad (gl) de 29 y un nivel de confianza del 95%.

Tabla 20 Prueba t-student para el indicador vulnerabilidades corregidas

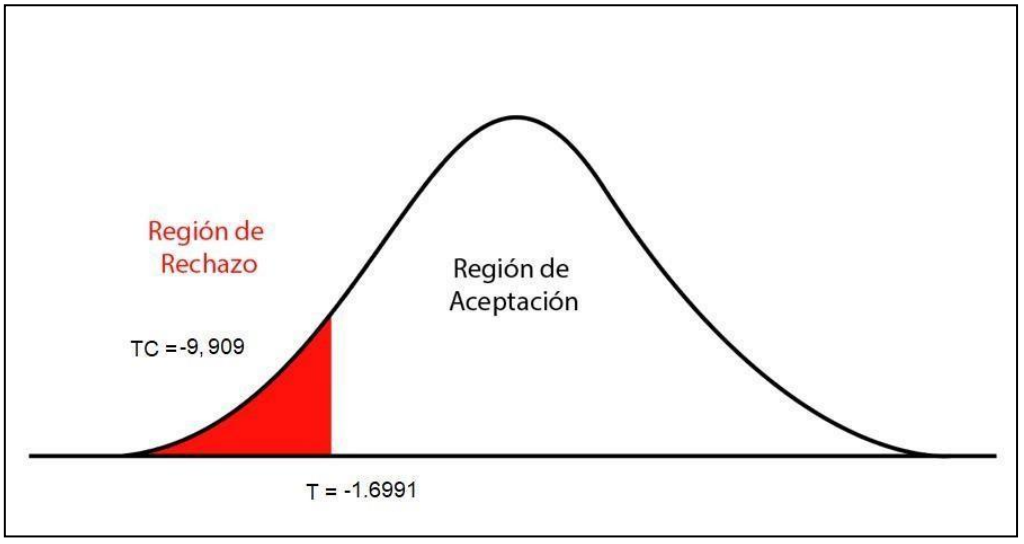
Prueba de muestras emparejadas						
		Media	Desviación estándar	t	gl	Sig. (bilateral)
Par 1	pre_VNC - post_VNC	22,60000	12,49165	-9,909	29	,000

Nota: Elaboración propia

El valor crucial de la tabla t-student, que se define por la intersección del grado de libertad (gl) y el nivel de confianza establecido, se compara con el valor T producido.

En este caso, el valor crucial fue -1,6991. Se rechaza la hipótesis nula al observar que el valor de T es menor que el valor crítico.

Figura 20 Zona de rechazo para el indicador vulnerabilidades corregidas



Nota: Elaboración propia

Por todo lo anterior se puede concluir que una aplicación de seguridad disminuye las vulnerabilidades no corregidas en la Seguridad Informática en una organización de servicios de tecnología.

Nivel de incidencias atendidas

La tabla siguiente muestra el análisis utilizando los resultados de la prueba t-student para 2 muestras vinculadas. Los resultados indican que se obtuvo una media de -34,75 con una desviación típica de 11,72. El valor t estimado fue de -13,25, con un grado de libertad (gl) de 19 y un nivel de confianza del 95%.

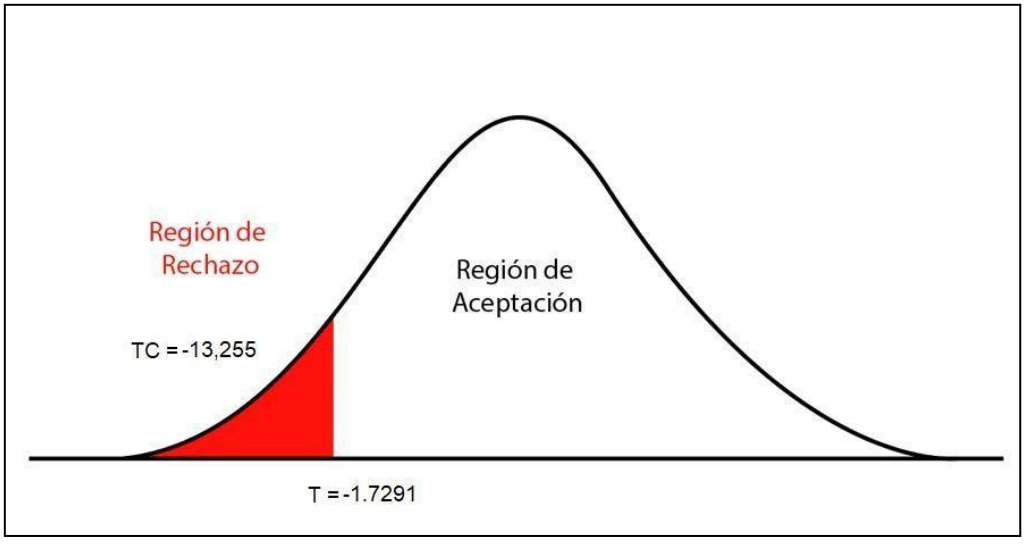
Tabla 21 Prueba t-student para el indicador Nivel de incidencias atendidas

Prueba de muestras emparejadas						
		Media	Desviación estándar	t	gl	Sig. (bilateral)
Par 1	nivel_incidencias_atendidas_pre - nivel_incidencias_atendidas_post	-34,75000	11,72436	-13,255	19	,000

Nota: Elaboración propia

El valor crucial de la tabla t-student, que se define por la intersección del grado de libertad (gl) y el nivel de confianza establecido, se compara con el valor T producido. En este caso, el valor crucial fue -1,7291. La hipótesis nula se rechaza al observar que el valor de T es menor que el valor crítico.

Figura 21 Zona de rechazo para el indicador Nivel de incidencias atendidas



Nota: Elaboración propia

Por todo lo anterior se puede concluir que una aplicación de seguridad aumenta el nivel de incidencias atendidas en la Seguridad Informática en una empresa de servicios de tecnología.

Tiempo de resolución de incidencias

La evaluación mediante los resultados de la prueba t-student para dos muestras conexas se muestra en la tabla siguiente. Los resultados indican que la media obtenida fue de 0,84 con una desviación típica de 0,56. Suponiendo un nivel de confianza del 95%, el valor t calculado fue de -6,762, con un grado de libertad (gl) de 19.

Tabla 22 Prueba t-student para el indicador Nivel de incidencias atendidas

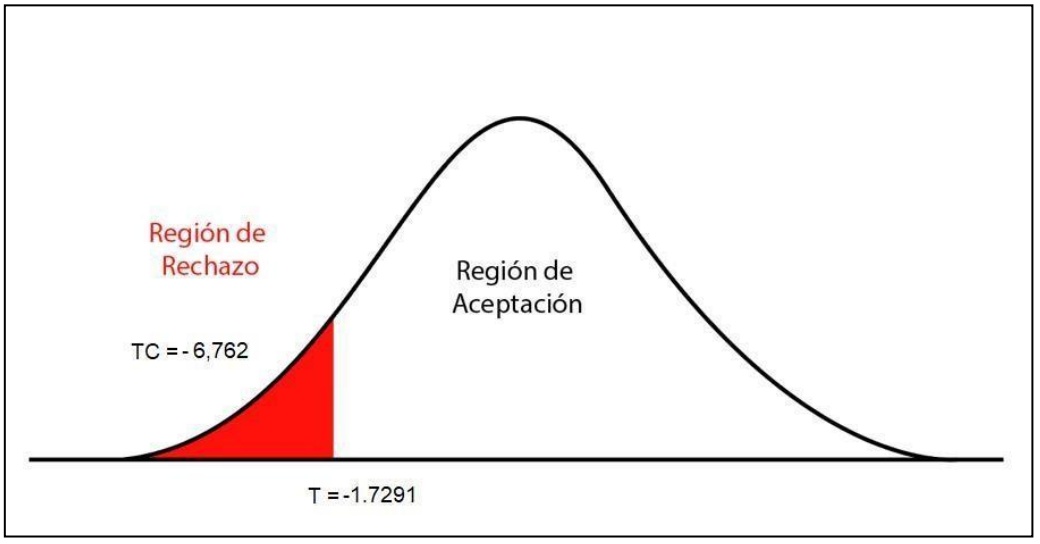
Prueba de muestras emparejadas

		Media	Desviación estándar	t	gl	Sig. (bilateral)
Par 1	Tiempo_resolucion_incidencias_pre - Tiempo_resolucion_incidencias_post	,84700	,56016	6,762	19	,000

Nota: Elaboración propia

El valor crucial de la tabla t-student, que se define por la intersección del grado de libertad (gl) y el nivel de confianza establecido, se compara con el valor T producido. En este caso, el valor crucial fue -1,7291. La hipótesis nula se rechaza al observar que el valor de T es menor que el valor crítico.

Figura 22 Zona de rechazo para el indicador Nivel de incidencias atendidas



Nota: Elaboración propia

Por todo lo anterior se puede concluir que una aplicación de seguridad acrecienta el nivel de incidencias atendidas en la Seguridad Informática en una organización de servicios de tecnología.

VI. DISCUSIÓN

Índice de vulnerabilidades corregidas: La mejora en el índice de vulnerabilidades corregidas, desde un 52.44% en el pre test hasta un 75.01% en el pos test, revela un avance significativo en la gestión de vulnerabilidades. Esta mejora demuestra el compromiso de la organización en abordar las debilidades y fortalecer su postura de seguridad. El índice de vulnerabilidades reparadas no debe considerarse un indicador aislado, sino más bien un componente de una estrategia de seguridad global que abarque la prevención de amenazas y la detección precoz.

Índice de vulnerabilidades no corregidas: La reducción del índice de vulnerabilidades no corregidas, desde un 47.56% en el pre test hasta un 24.99% en el pos test, es una señal positiva de que la organización ha tomado medidas para abordar las vulnerabilidades identificadas. Esta disminución refleja un enfoque más efectivo en la gestión de vulnerabilidades y una mayor capacidad para cerrar las brechas de seguridad. Sin embargo, es esencial continuar monitoreando y abordandode manera proactiva las nuevas vulnerabilidades que puedan surgir, ya que la seguridad informática es un desafío constante.

Asistencia a incidentes: El salto en la asistencia a incidentes del 43% en la pre-test al 77% en el post-test es un signo significativo de que la empresa se ha vuelto más hábil a la hora de identificar, abordar y resolver problemas de seguridad. Este incremento refleja una mayor eficiencia en la gestión de incidentes y una respuesta más rápida y efectiva. Sin embargo, es importante evaluar la calidad de la respuesta a las incidencias, asegurándose de que se sigan los procedimientos adecuados y se realicen análisis exhaustivos para comprender las causas subyacentes y prevenir futuras incidencias similares.

Tiempo de resolución de incidencias: La reducción del tiempo de resolución de incidencias, desde un promedio de 2.14 horas en el pre test a 1.29 horas en el pos

test, es un logro significativo. Una resolución más rápida de las incidencias permite minimizar el impacto y la exposición a riesgos de seguridad. Sin embargo, es importante evaluar la calidad de la resolución, no solo el tiempo. Asegurarse de que se realicen investigaciones adecuadas, se identifiquen las causas raíz y se implementen medidas correctivas efectivas puede ayudar a prevenir la recurrencia de las incidencias y fortalecer la seguridad general de la organización.

VII. CONCLUSIONES

La conclusión de medir el índice de vulnerabilidades corregidas en incidencias en la seguridad informática es que esta métrica proporciona una medida efectiva para evaluar y mejorar la actitud de seguridad de una empresa. Al monitorear y medir regularmente el número de vulnerabilidades identificadas y corregidas en incidentes de seguridad, se puede valorar la eficacia de ls revisiones de seguridadimplementados y determinar si las medidas tomadas son adecuadas para proteger los activos de información.

Al aumentar el índice de vulnerabilidades corregidas, se reducen los riesgos potenciales para la organización, ya que se disminuye la probabilidad de que los atacantes exploten las vulnerabilidades conocidas. Esto puede llevar a una mejora significativa en la seguridad global de los sistemas informáticos y ayudar a prevenir brechas de seguridad y pérdida de datos confidenciales.

En conclusión, la ejecución de medidas para corregir las vulnerabilidades en la seguridad informática ha demostrado ser efectiva, como se evidencia por el incremento significativo en el índice de vulnerabilidades corregidas. El pre test reveló un índice inicial de vulnerabilidades corregidas del 52.44%, mientras que el pos test mostró un aumento notable al alcanzar un índice del 75.01%.

Este incremento en el índice de vulnerabilidades corregidas refleja elcompromiso de la organización en abordar las debilidades y fortalecer su postura de seguridad. Al corregir activamente las vulnerabilidades identificadas, la organización ha logrado reducir los riesgos y minimizar las oportunidades de explotación por parte de los atacantes.

La conclusión de medir el índice de vulnerabilidades no corregidas en incidencias en la seguridad informática es que esta métrica proporciona una perspectiva importante sobre las debilidades persistentes en los sistemas y la efectividad de los esfuerzos de seguridad de una organización. Al identificar y cuantificar las vulnerabilidades que no han sido corregidas, se puede evaluar el alto nivel de riesgos al que está sometida la organización y la urgencia de tomar medidas correctivas.

Un alto índice de vulnerabilidades no corregidas indica que existen debilidades conocidas en los sistemas que aún no han sido abordadas. Esto representa una amenaza significativa, ya que los atacantes pueden aprovechar estas vulnerabilidades para infiltrarse en los sistemas y comprometer la seguridad de la organización, robar información confidencial o causar daños significativos.

La priorización de las medidas de seguridad y la asignación de recursos adecuados para resolver las principales vulnerabilidades pueden realizarse con la ayuda de la medición de la tasa de vulnerabilidades no corregidas. Esto permite a la organización centrarse en las áreas más vulnerables y tomar medidas para solucionar las debilidades existentes, fortaleciendo así la postura de seguridad general.

En conclusión, el índice de vulnerabilidades no corregidas ha experimentado una disminución significativa, lo que indica un progreso notable en la gestión de las debilidades de seguridad. En el pre test, se identificó que el 47.56% de las vulnerabilidades detectadas no habían sido corregidas, mientras que en el pos test este número se redujo significativamente a solo el 24.99%.

Esta reducción en el índice de vulnerabilidades no corregidas refleja los esfuerzos y la eficacia de la organización para abordar y resolver las vulnerabilidades conocidas. La implementación de acciones correctivas, como la aplicación de parches, actualizaciones de software y medidas de seguridad adicionales, ha permitido cerrar las brechas y minimizar los riesgos de explotación por parte de los atacantes.

Conclusión: Medir el número de incidentes de seguridad informática gestionados permite evaluar la eficacia de una organización a la hora de identificar, responder y resolver incidentes de seguridad. La eficiencia de las medidas de seguridad y la

madurez del programa de seguridad de la organización pueden evaluarse controlando la cantidad y el calibre de los incidentes gestionados.

Un alto nivel de incidencias atendidas indica que la organización está implementando medidas efectivas para detectar y responder a posibles incidentes de seguridad. Esto demuestra una capacidad de respuesta rápida y una gestión adecuada de los incidentes, lo que ayuda a reducir el impacto y el tiempo transcurrido de los incidentes, reduciendo así el riesgo y los posibles daños a los activos de información.

La medición del nivel de incidencias atendidas también puede revelar patrones o tendencias en los tipos de incidentes que ocurren con mayor frecuencia, lo que permite a la organización identificar las áreas de mayor vulnerabilidad y tomar medidas para mejorar la seguridad en esas áreas específicas.

En conclusión, el nivel de incidencias atendidas ha experimentado un aumento sustancial, lo que se lee como una mejora relevante en la capacidad de la organización para detectar, responder y resolver las incidencias de seguridad. En el pre test, se atendió aproximadamente el 43% de las incidencias detectadas, mientras que en el pos test este número aumentó notablemente a un 77%.

Este incremento en el nivel de incidencias atendidas demuestra un enfoque más efectivo en la gestión de incidencias de seguridad. La organización ha mejorado su capacidad para identificar y priorizar las incidencias, asignar recursos adecuados y llevar a cabo acciones de respuesta de manera oportuna.

Conclusión: Medir el tiempo de resolución de incidentes en seguridad informática es importante porque proporciona datos importantes sobre la rapidez y eficacia con que se gestionan los incidentes de seguridad. El tiempo de resolución de incidentes es un parámetro crucial para evaluar el rendimiento de una organización para identificar, investigar, contener y resolver rápidamente los incidentes de seguridad.

Un tiempo de resolución de incidencias rápido es deseable, ya que indica una capacidad efectiva de respuesta ante incidentes. Una respuesta ágil y rápida puede ayudar a reducir el impacto de los incidentes, limitar la propagación de amenazas y minimizar el tiempo de exposición a riesgos de seguridad. Esto es especialmente

importante en un entorno en constante evolución, donde las amenazas cibernéticas pueden propagarse rápidamente y causar daños significativos si no se abordan de manera oportuna.

En conclusión, el tiempo de resolución de incidencias ha experimentado una reducción significativa, lo que indica una mejora notable en la eficiencia y rapidez con la que la organización responde y resuelve los incidentes de seguridad. En el pre test, el tiempo promedio de resolución por incidencia era de aproximadamente 2.14 horas, mientras que en el pos test este tiempo se redujo a tan solo 1.29 horas por incidencia.

Esta reducción del tiempo de resolución de incidentes es el resultado de la mejora de los procedimientos de gestión de incidencias de seguridad y del aumento de la capacidad de respuesta. Para reducir el efecto y la duración de los problemas, la organización ha puesto en marcha procedimientos e innovaciones para acelerar la detección, investigación, contención y resolución de los problemas.

La disminución en el tiempo de resolución de incidencias indica una mayor eficiencia en la identificación y aplicación de soluciones, así como una mejor coordinación y colaboración entre los equipos de respuesta a incidentes. Esto se traduce en una capacidad mejorada para restaurar la normalidad operativa rápidamente y minimizar cualquier interrupción o daño causado por los incidentes.

VIII. RECOMENDACIONES

Basándome en el contexto actual se presentan las siguientes recomendaciones

Implementar un enfoque proactivo: No esperes a que ocurran incidentes de seguridad para tomar medidas. Establece un programa de seguridad integral que incluya evaluaciones regulares de vulnerabilidades, actualizaciones de software y parches, así como una monitorización constante de los sistemas para detectarposibles amenazas.

Establecer un proceso de gestión de vulnerabilidades sólido: Desarrolla un enfoque sistemático para identificar, evaluar y corregir las vulnerabilidades detectadas. Prioriza las vulnerabilidades según su nivel de riesgo y aplica soluciones rápidamente para mitigar las posibles brechas de seguridad.

Cree una estrategia exhaustiva de respuesta a incidentes con funciones y responsabilidades definidas y pasos para la detección, evaluación, contención y resolución de problemas para mejorar la respuesta a incidentes. Asegúrate de que todos los miembros involucrados están preparados y formados para actuar conrapidez en cualquier situación.

Automatizar y agilizar los procesos de respuesta a incidentes: Utiliza herramientas y tecnologías avanzadas para automatizar tareas repetitivas y acelerar la respuesta a incidentes. La automatización puede ayudar a identificar y contener rápidamente amenazas, reduciendo así el tiempo de resolución.

Establecer un sistema de seguimiento y métricas: Implementa un sistema para rastrear y medir las incidencias de seguridad, el tiempo de resolución, el nivel de incidencias atendidas y el índice de vulnerabilidades corregidas. Esto proporcionará información valiosa para identificar áreas de mejora, establecer metas y realizar un seguimiento del progreso a lo largo del tiempo.

Todos los empleados deben recibir formación sobre las mejores prácticas de seguridad, incluido el desarrollo de claves seguras, la identificación de correos phishing y la seguridad de datos privados. Fomente en el trabajo una cultura que valore la seguridad.

Mantenerse actualizado con las últimas amenazas y soluciones de seguridad: Establece canales de información confiables para mantenerse al tanto de las últimas tendencias y amenazas en seguridad informática. Mantén actualizados los sistemas y aplicaciones con los últimos parches y actualizaciones de seguridad.

Deben realizarse auditorías y evaluaciones de seguridad periódicas para detectar posibles fallos en los sistemas y procedimientos. Las evaluaciones de seguridad pueden ayudar a detectar áreas problemáticas y ofrecer sugerencias para reforzar la infraestructura de seguridad.

Referencias Bibliográficas

Álaba, K. Basurto, W. y Tóala, R. (2022). VULNERABILIDADES EN LOS SISTEMAS INFORMÁTICOS OWASP TOP 10: REVISIÓN BIBLIOGRÁFICA. 3(2), 1-8. https://revistas.uleam.edu.ec/index.php/business_science/article/view/221/308

Albós, A. (2019). Fundamentos de seguridad informática. 1-64 PID_00269891 https://openaccess.uoc.edu/bitstream/10609/148532/1/FundamentosDeSeguridadInformatica.pdf

Alcaldía Municipal Ibagué (2019). GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION. 1-38 https://www.ibague.gov.co/portal/admin/archivos/publicaciones/2019/22994-DOC-20190207.pdf

Alqahtani, S., & Zou, X. (2021). Vulnerability assessment in cybersecurity: An overview. In Proceedings of the 2021 International Conference on Artificial Intelligence and Cybersecurity (AICS) (pp. 1-6). IEEE.

Alshammari, F. H. (2023). Design of capability maturity model integration with cybersecurity risk severity complex prediction using bayesian-based machine learning models. Service Oriented Computing and Applications, 17(1), 59-72. doi:10.1007/s11761-022-00354-4

Alvarez, A. (2020). Clasificación de las Investigaciones. Universidad de Lima https://repositorio.ulima.edu.pe/bitstream/handle/20.500.12724/10818/Nota%20Acad%C3%A9mica%202C%20%20Clasificaci%C3%B3n%20de%20Investigaciones.pdf?sequence=4&isAllowed=y

Amin, M. R., & Bhowmik, T. (2022). Existing vulnerability information in security requirements elicitation. Paper presented at the *Proceedings of the IEEE International Conference on Requirements Engineering,* 220-225. doi:10.1109/REW56159.2022.00049

Arispe, C. Yangali, J. Guerrero, M. Lozada, O. Acuña, L. y Arellano, C. (2020). LA INVESTIGACIÓN CIENTÍFICA. Una aproximación para los estudios de posgrado.

Universidad Internacional del Ecuador. https://repositorio.uide.edu.ec/bitstream/37000/4310/1/LA%20INVESTIGACI%C3%93N%20CIENT%C3%8DFICA.pdf

ARIZMENDI, F. (2019) Fundamentos de Fundamentos de Estadística y Probabilidades con aplicaciones, Editorial Yo Publico. Disponible en: https://books.google.com.pe/books?id=SZ_MDwAAQBAJ&pg=PR11&dq=estadistica+poblacion&hl=es-419&sa=X&ved=2ahUKEwj5lM-epNjzAhUVIrkGHTR5DDsQ6AF6BAgFEAI#v=onepage&q=estadistica%20poblacion&f=false

Bernal, A. E., Monterrubio, S. M. M., Fuente, J. P., Crespo, R. G., & Verdu, E. (2021). Methodology for computer security incident response teams into IoT strategy. *KSII Transactions on Internet and Information Systems, 15*(5), 1909- 1928. doi:10.3837/tiis.2021.05.018

Briceño, J. (2018). ANÁLISIS DE RIESGOS DE LOS SISTEMAS DE SEGURIDAD INFORMÁTICA DE LA EMPRESA KAPPA10 LTDA. [Trabajo de grado, Universidad Nacional Abierta y a Distancia - UNAD] https://repository.unad.edu.co/bitstream/handle/10596/27822/%20%09jcbricenoo.pdf?sequence=1&isAllowed=y

Cáceres, C. (2019). Desarrollo de un modelo de gestión de incidentes basado en Itil v3.0 para el área de Facilities Management de la empresa Tgestiona [Tesis de titulación, Universidad Peruana de Ciencias Aplicadas] https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/625703/c%c3%a1ceres_cc.pdf?sequence=1&isAllowed=y

Cai, D., Sun, Y., Su, X., & Cao, Y. (2022). Research on security defect assessment technology for java source code. Paper presented at the Proceedings of SPIE - the International Society for Optical Engineering, ,12474 doi:10.1117/12.2653742 Retrieved from www.scopus.com

Cobit Control Objectives 3erd Edition, ISACA 2000 http://www.isaca.org/Template.cfm?Section=Downloads5&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=63&ContentID=13742#COBIT

Cárdenas, M. (2020). Análisis de vulnerabilidades en la seguridad informática de las empresas peruanas. Revista de Investigación Académica, 22(1), 1-12.

CASAS, J. (2020) Inferencia estadística para Economía, Editorial. Ramon arieces , [Consultado 22 de abril del 2022] Disponible en: https://books.google.com.pe/books?id=f8BjDwAAQBAJ&pg=PP1&dq=estadistica&hl=es-419&sa=X&ved=2ahUKEwjsoey058T3AhVLCbkGHcfAAY4Q6AF6BAgEEAI#v=onepage&q=estadistica&f=false

Celis Reategui, R. D. (2021). Aplicación del marco de trabajo de ITIL v3 y su influencia en la gestión de incidencias en la Unidad de Informática del PEDAMAALC. https://explore.openaire.eu/search/publication?articleId=od_____9504::0fc2adeaafda980326fbda62b842024d

Centro Nacional de Incidentes de Seguridad de la Información del Perú (CENSI). (2020). Informe Anual de Incidentes de Seguridad de la Información 2020. Recuperado de

Cerrón, D. y Vite, C. (2023). Buenas prácticas de ITIL v4 para la gestión de incidencias en un centro médico privado, Lima 2022 [Tesis de titulación, Universidad Norbert Wiener] https://repositorio.uwiener.edu.pe/bitstream/handle/20.500.13053/8790/T061_75414480_47935063_T.pdf?sequence=1&isAllowed=y

Chicano, E. (2023). Gestión de incidentes de seguridad informática. IFCT0109. IC Editorial https://www.google.com.pe/books/edition/Gesti%C3%B3n_de_incidentes_de_seguridad_info/rxPLEAAAQBAJ?hl=es&gbpv=0

Condori Fernandez, M. M. (2018). Gestión de incidencias aplicando ITIL v3 en una empresa de telecomunicaciones.

Department for Digital, C. M. (2020). Cyber Security Breaches Survey 2020. https://www.gov.uk/government/statistics/cyber-security-breachessurvey-2020/cyber-security-breaches-survey-2020: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachm

e
nt_data/file/893399/Cyber_Security_Breaches_Survey_2020_Statistical_Release_180 620.pdf

Elizabeth Conde-Zhingre, L., Alejandro Quezada-Sarmiento, P., & Hernandez, W. (2019). Propuesta de Arquitectura de mesa de servicios tecnológicos basado en el marco de referencia ITIL V 3.0. CISTI (Iberian Conference on Information Systems & Technologies / Conferência Ibérica de Sistemas e Tecnologias de Informação) Proceedings, 1–6.

ESET. (2020). Security Report Latinoamérica 2020. Argentina: ESET. https://www.welivesecurity.com/wp-content/uploads/2020/08/ESETSecurity-Report-LATAM_2020.pdf

Fajardo, J. (2017). Análisis de vulnerabilidades en sistemas de información. Seguridad y Defensa, 25(2), 107-114.

Flores Carrillo, J. A. (2023). Desarrollo de un modelo de gestión de incidencias para el departamento de Soporte TI y Redes basado en ITIL V4 para la empresa Red Animation Studios ; Development of an incident management model for the Department of it support and networks based on Itil v4 for the Company Red Animation Studio [Universidad Peruana de Ciencias Aplicadas (UPC)]. In Universidad Peruana de Ciencias Aplicadas (UPC); Repositorio Académico - UPC. http://hdl.handle.net/10757/667936

Fouz, C. (2021). Introducción a las vulnerabilidades. 2-40 PID_00274038 https://materials.campus.uoc.edu/daisy/Materials/PID_00274038/pdf/PID_00274038.pdf

Francisco Xavier, L. R. (2020). Estudio para fortalecer la atención de incidencias en una empresa de telecomunicaciones. https://explore.openaire.eu/search/publication?articleId=od 3056::0d2ae1e7319c9687b8db28baabfa1977 http://repositorio.ug.edu.ec/handle/redug/51477

García, V. Riaño, J. y Estrada, L.(2021) Lesson learned management model for solving incidents. 10.23919/CISTI.2017.7975789

Hernández, C. y Carpio N. (2019) Introducción a los tipos de muestreo. Alerta. 2019;2(1):75-79. DOI: 10.5377/alerta. v2i1.7535

Hernández, R. (2018). METODOLOGÍA DE LA INVESTIGACIÓN: LAS RUTAS CUANTITATIVA, CUALITATIVA Y MIXTA, 3-753 http://repositorio.uasb.edu.bo:8080/handle/54000/1292

Joya, Trejos y Dorado (2019). GESTIÓN DE INCIDENTES EN SEGURIDAD DE LA INFORMACIÓN TEVEANDINA LTDA. – CANAL TRECE. 3-15 https://canaltrece.com.co/uploads/file_uploads/Manual_de_gestion_de_incidentes_V0.pdf

Katsadouros, E., & Patrikakis, C. (2022). A survey on vulnerability prediction using GNNs. Paper presented at the *ACM International Conference Proceeding Series,* 38-43. doi:10.1145/3575879.3575964

KnowledgeHut Tutorial (2019, Agosto 27). ITIL 4 Four Dimension Model | Concepts with Real-Time Examples. https://www.knowledgehut.com/tutorials/itil4-tutorial/itil-four-dimensions-it-service-management

Laghrissi, F., Douzi, S., Douzi, K., & Hssina, B. (2021). Intrusion detection systems using long short-term memory (LSTM). Journal of Big Data, 8(65). doi:10.1186/s40537-021-00448-4

Leveraging ISO 17799 to Achieve Security Management Best Practices de Evan Tegethoff http://www.forsythe.com/Forsythe/itriskman/security/security_leveragingiso.jsp

Loayza, E. (2021). El fichaje de investigación como estrategia para la formación de competencias investigativas. Educare et Comunicare, 9 (1), 67-77. https://www.aacademica.org/edward.faustino.loayza.maturrano/22.pdf

Lozano Triana, C. J., & Motavita Ramirez, A. (2022). Formulación de un plan de mejora al proceso de gestión de incidencias de la mesa de servicio del área de tecnología de la empresa Symplifica sede Bogotá D.C utilizando ITIL V4 e ISO 27001.https://doi.org/20.500.12494/46464

Mishra, S., Alotaibi, W. B., Alshehri, M., & Saxena, S. (2022). Cyber-attacks visualisation and prediction in complex multi-stage network. *International Journal of Computer Applications in Technology, 68*(4), 345-356. doi:10.1504/ijcat.2022.125180

Peña, T. (2022). Etapas del análisis de la información documental. Revista Interamericana de Bibliotecología, 45(3), e340545. https://doi.org/10.17533/udea.rib.v45n3e340545 http://www.scielo.org.co/pdf/rib/v45n3/2538-9866-rib-45-03-e4.pdf

Postigo, A. (2020). Seguridad informática (Edición 2020). Ediciones Paraninfo, S.A https://www.google.com.pe/books/edition/Seguridad_inform%C3%A1tica_Edici%C3%B3n_2020/UCjnDwAAQBAJ?hl=es&gbpv=0

Puentes Figueroa, C. E., & Maestre-Gongora, G. (2019). Plan estrategico basado en ITIL para mipymes en el departamento de Arauca-Colombia. Lampsakos, 68. https://doi.org/10.21501/21454086.3280

PwC Perú. (2020). Encuesta de Seguridad de la Información 2020. Recuperado de

Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, M. A., Amir, A., . . . Sarwat, A. I. (2023). Impact, vulnerabilities, and mitigation strategies for cyber-secure critical infrastructure. Sensors, 23(8) doi:10.3390/s23084060

Robledo, C. (2010) Técnicas y Proceso de Investigación Científica. Disponible en: https://investigar1.files.wordpress.com/2010/05/fichas-de-trabajo.pdf

Sahin, A., Ozkaya, M., & Ekici, E. (2021). A systematic literatur review on security incident response management. Journal of Network and Computer Applications, 177, 102947.

Sánchez, F. & Valles, M. (2021). Influence of ITIL V3 in incident management of a Peruvian municipality. Revista Cubana de Ciencias Informáticas, 15(3), 1-19. Epub 01 de septiembre de 2021. Recuperado en 29 de julio de 2023, de

http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S222718992021000300001&lng=es&tlng=en.

Thapa, N., Liu, Z., Shaver, A., Esterline, A., Gokaraju, B., & Roy, K. (2021). Secure cyber defense: An analysis of network intrusion-based dataset ccd-idsv1 with machine learning and deep learning models. Electronics (Switzerland), 10(1747). doi:10.3390/electronics10151747

Touloumis, K., Michalitsi-Psarrou, A., Georgiadou, A., & Askounis, D. (2022). A tool for assisting in the forensic investigation of cyber-security incidents. Paper presented at the *Proceedings - 2022 IEEE International Conference on Big Data, Big Data 2022,* 2630-2636. doi:10.1109/BigData55660.2022.10020208

Valencia Balladares, I. A., & Tapia Chichande, A. P. (2020). Seguridad informatica aplicada a la defensa y seguridad basada en principios Juridicos. Revista Alternativas, 21(2). https://doi.org/10.23878/alternativas.v21i2.335

Vasquez Vasquez, R. (2020). Aplicación para la gestión de incidencias de TI bajo la perspectiva ITIL y el enfoque Open Source para Departamento de TI de la Caja Rural de Ahorro y Crédito Cajamarca S.A. https://explore.openaire.eu/search/publication?articleId=od 3056::b80d2e1ca73eeb3d2ee08e6c2383a459

VEGAS-CAPRISTAN, N., & SOTO-ALARCÓN, A. (2022). La eficiencia de la gestión de incidencias en Cloud Services. Revista Campus, 27(34), 197–208. https://doi.org/10.24265/campus.2022.v27n34.03

Xu, D., Chen, T., Tan, Z., Wu, F., Gao, J., & Yang, Y. (2022). Web vulnerability detection analyzer based on python. *International Journal of Digital Crime and Forensics, 14*(2) doi:10.4018/IJDCF.302875

Yurivilca, E. (2019). Mejora de la gestión de incidentes en el sistema de gestión de flotas vehiculares mediante Itil en la Empresa Mine Sense Solutions – Sociedad Minera El Brocal – Pasco, 2019. [Tesis de titulación, UNIVERSIDAD NACIONAL DEL CENTRO DEL PERÚ]

https://repositorio.uncp.edu.pe/bitstream/handle/20.500.12894/5435/T010_72441412_T.pdf?sequence=1&isAllowed=y

Anexo 1

Tabla 5 Operacionalización de variables

Tipo	Variable	Definición Conceptual	Definición Operacional	Dimensión	Indicador	Escala de Medición
Independiente	Análisis de Vulnerabilidades en la seguridad informática	Las vulnerabilidades en seguridad de la información son fallos, debilidades o defectos en el diseño, implementación o funcionamiento de los sistemas informáticos, que pueden ser explotados por los atacantes paracomprometer la confiabilidad, integridad o disponibilidad de los datos y sistemas (Alqahtani & Zou, 2021, p. 1).	Las vulnerabilidades informáticas son debilidades o defectos en los sistemas, redes o programas que pueden ser explotados por personas malintencionadas o utilizados accidentalmente por los usuarios sin intención de causar daño. Estas vulnerabilidades podrían permitir el acceso no autorizado, la manipulación de datos, la interrupción del funcionamiento normal del sistema o la ejecución de código malicioso.	Vulnerabilidades técnicas	Índice de Vulnerabilidades corregidas	Razón
					Índice de vulnerabilidades no corregidas	Razón
Dependiente	Incidencias de seguridad informática	Una incidencia de seguridad informática es cualquier suceso que compromete la confiabilidad, integridad o disponibilidad de los datos o sistemas informáticos (Sahin et al., 2021, p. 38).	Los incidentes relacionados con la seguridad informática pueden ser cosas que ocurren o circunstancias que afectan a la seguridad de los sistemas, redes o datos en un entorno informático. Estos sucesos pueden ser indicadores de rendimiento, errores, fallos de calidad o características de los factores, y pueden suponer un riesgo para la privacidad, la precisión o la velocidad de los datos.	Monitoreo y mejora	Tiempo de Resolución de Incidencias	Razón
					Nivel de incidencias atendidas	Razón

Nota: *Elaboración propia*

Anexo 2: Instrumentos de recolección de datos

Índice de Vulnerabilidades corregidas Pre test

Fecha de Registro				
Investigador	Jose Luis Sanchez	**Tipo de Prueba**		Pre Test
Empresa investigada	CRATE E.I.R.L.			
Motivo de Investigación	Índice de Vulnerabilidades corregidas			
Fecha Inicio	3-Abr	**Fecha fin**		30-Abr
Investigación	**Indicador**	**Medida**	**Fórmula**	
Análisis de vulnerabilidades o incidencias en la Seguridad Informática	Índice de Vulnerabilidades corregidas	Porcentaje	IVC=NVC/NTVC * 100	
Item	**Proyecto**	**Número de vulnerabilidades corregidas**	**Número total de vulnerabilidades conocidas**	**Indice de vulnerabilidades corregidas**
1	Proyecto 1	8	14	57.14%
2	Proyecto 2	10	15	66.67%
3	Proyecto 3	5	16	31.25%
4	Proyecto 4	5	14	35.71%
5	Proyecto 5	9	15	60.00%
6	Proyecto 6	6	14	42.86%
7	Proyecto 7	8	16	50.00%
8	Proyecto 8	7	14	50.00%
9	Proyecto 9	9	15	60.00%
10	Proyecto 10	8	16	50.00%
11	Proyecto 11	9	14	64.29%
12	Proyecto 12	9	15	60.00%
13	Proyecto 13	6	13	46.15%
14	Proyecto 14	7	13	53.85%
15	Proyecto 15	8	12	66.67%
16	Proyecto 16	8	15	53.33%
17	Proyecto 17	9	16	56.25%
18	Proyecto 18	11	14	78.57%
19	Proyecto 19	6	15	40.00%
20	Proyecto 20	10	16	62.50%
21	Proyecto 21	9	14	64.29%
22	Proyecto 22	6	15	40.00%
23	Proyecto 23	7	16	43.75%
24	Proyecto 24	8	14	57.14%
25	Proyecto 25	8	15	53.33%
26	Proyecto 26	7	15	46.67%
27	Proyecto 27	5	14	35.71%
28	Proyecto 28	8	16	50.00%
29	Proyecto 29	7	16	43.75%
30	Proyecto 30	8	15	53.33%

Índice de Vulnerabilidades corregidas Post test

Fecha de Registro				
Investigador	Jose Luis Sanchez	Tipo de Prueba		Pre-Test
Empresa investigada	CRATI E.I.R.L.			
Motivo de investigación	Índice de Vulnerabilidades corregidas			
Fecha Inicio	1-Mar	Fecha fin		30-Mar
Investigación	Indicador	Medida	Fórmula	
Análisis de vulnerabilidades o incidencias en la Seguridad Informática	Índice de Vulnerabilidades corregidas	Porcentaje	IVC=NVC/NTVC * 100	
Item	Proyecto	Número de vulnerabilidades corregidas	Número total de vulnerabilidades conocidas	Indice de vulnerabilidades corregidas
1	Proyecto 1	11	14	78.57%
2	Proyecto 2	12	15	80.00%
3	Proyecto 3	9	16	56.25%
4	Proyecto 4	10	14	71.43%
5	Proyecto 5	11	15	73.33%
6	Proyecto 6	12	14	85.71%
7	Proyecto 7	11	16	68.75%
8	Proyecto 8	12	14	85.71%
9	Proyecto 9	10	15	66.67%
10	Proyecto 10	13	16	81.25%
11	Proyecto 11	12	14	85.71%
12	Proyecto 12	10	15	66.67%
13	Proyecto 13	8	13	61.54%
14	Proyecto 14	10	13	76.92%
15	Proyecto 15	9	12	75.00%
16	Proyecto 16	11	15	73.33%
17	Proyecto 17	10	16	62.50%
18	Proyecto 18	11	14	78.57%
19	Proyecto 19	12	15	80.00%
20	Proyecto 20	12	16	75.00%
21	Proyecto 21	11	14	78.57%
22	Proyecto 22	12	15	80.00%
23	Proyecto 23	13	16	81.25%
24	Proyecto 24	10	14	71.43%
25	Proyecto 25	11	15	73.33%
26	Proyecto 26	13	15	86.67%
27	Proyecto 27	11	14	78.57%
28	Proyecto 28	10	16	62.50%
29	Proyecto 29	12	16	75.00%
30	Proyecto 30	12	15	80.00%

Índice de Vulnerabilidades no corregidas Pre test

Fecha de Registro			
Investigador	Jose Luis Sanchez	Uso de Prueba	Pre Test
Empresa investigada	CRATI E.I.R.L.		
Motivo de Investigación	Índice de vulnerabilidades no corregidas		
Fecha Inicio	3-Abr	Fecha fin	30-Abr
Investigación	Indicador	Medida	Fórmula
Análisis de vulnerabilidades e incidencias en la Seguridad Informática	Índice de Vulnerabilidades no corregidas	Porcentaje	IVNC=NVNC/NTVC * 100

Ítem	Proyecto	Número de vulnerabilidades no corregidas	Número total de vulnerabilidades conocidas	Ipuesta de vulnerabilidades no corregidas
1	Proyecto 1	6	14	42.86%
2	Proyecto 2	5	15	33.33%
3	Proyecto 3	11	16	68.75%
4	Proyecto 4	9	14	64.29%
5	Proyecto 5	6	15	40.00%
6	Proyecto 6	8	14	57.14%
7	Proyecto 7	8	16	50.00%
8	Proyecto 8	7	14	50.00%
9	Proyecto 9	6	15	40.00%
10	Proyecto 10	8	16	50.00%
11	Proyecto 11	5	14	35.71%
12	Proyecto 12	6	15	40.00%
13	Proyecto 13	7	13	53.85%
14	Proyecto 14	6	13	46.15%
15	Proyecto 15	4	12	33.33%
16	Proyecto 16	7	15	46.67%
17	Proyecto 17	7	16	43.75%
18	Proyecto 18	3	14	21.43%
19	Proyecto 19	9	15	60.00%
20	Proyecto 20	6	16	37.50%
21	Proyecto 21	5	14	35.71%
22	Proyecto 22	9	15	60.00%
23	Proyecto 23	9	16	56.25%
24	Proyecto 24	6	14	42.86%
25	Proyecto 25	7	15	46.67%
26	Proyecto 26	8	15	53.33%
27	Proyecto 27	9	14	64.29%
28	Proyecto 28	8	16	50.00%
29	Proyecto 29	9	16	56.25%
30	Proyecto 30	7	15	46.67%

Índice de Vulnerabilidades no corregidas Post test

Fecha de Registro				
Investigador	Jose Luis Sanchez	Tipo de Prueba		Pos-Test
Empresa investigada	CRATI E.I.R.L.			
Motivo de Investigación	Índice de vulnerabilidades no corregidas			
Fecha Inicio	3-Abr	Fecha fin		30-Abr
Investigación	Indicador	Medida	Fórmula	
Análisis de vulnerabilidades e incidencias en la Seguridad Informática	Índice de Vulnerabilidades no corregidas	Porcentaje	IVNC=NVNC/NTVC * 100	
Item	Proyecto	Número de vulnerabilidades no corregidas	Número total de vulnerabilidades corregidas	Indice de vulnerabilidades no corregidas
1	Proyecto 1	3	14	21.43%
2	Proyecto 2	3	15	20.00%
3	Proyecto 3	7	16	43.75%
4	Proyecto 4	4	14	28.57%
5	Proyecto 5	4	15	26.67%
6	Proyecto 6	2	14	14.29%
7	Proyecto 7	5	16	31.25%
8	Proyecto 8	2	14	14.29%
9	Proyecto 9	5	15	33.33%
10	Proyecto 10	3	16	18.75%
11	Proyecto 11	2	14	14.29%
12	Proyecto 12	5	15	33.33%
13	Proyecto 13	5	13	38.46%
14	Proyecto 14	3	13	23.08%
15	Proyecto 15	3	12	25.00%
16	Proyecto 16	4	15	26.67%
17	Proyecto 17	6	16	37.50%
18	Proyecto 18	3	14	21.43%
19	Proyecto 19	3	15	20.00%
20	Proyecto 20	4	16	25.00%
21	Proyecto 21	3	14	21.43%
22	Proyecto 22	3	15	20.00%
23	Proyecto 23	3	16	18.75%
24	Proyecto 24	4	14	28.57%
25	Proyecto 25	4	15	26.67%
26	Proyecto 26	2	15	13.33%
27	Proyecto 27	3	14	21.43%
28	Proyecto 28	6	16	37.50%
29	Proyecto 29	4	16	25.00%
30	Proyecto 30	3	15	20.00%

Nivel de Incidencias atendidas Pre test

Ficha de Registro				
Investigador	Jose Luis Sanchez	**Tipo de Prueba**		Pre Test
Empresa investigada	CRATI E.I.R.L.			
Motivo de investigación	Nivel de incidencias atendidas			
Fecha Inicio	3-Abr	**Fecha fin**		30-Abr
Investigación	Indicador	**Medida**	**Fórmula**	
Análisis de vulnerabilidades e incidencias en la Seguridad Informática	Nivel de incidencias atendidas	Porcentaje	NIAT=NIA/TIR x 100	
Item	**Fecha**	**Número de incidencias atendidas**	**Total de incidencias registradas**	**Nivel de incidencias atendidas**
1	3-Abr	8	14	57%
2	4-Abr	7	14	50%
3	5-Abr	6	11	55%
4	6-Abr	5	16	31%
5	7-Abr	4	15	27%
6	10-Abr	6	14	43%
7	11-Abr	7	13	54%
8	12-Abr	6	14	43%
9	13-Abr	5	12	42%
10	14-Abr	5	14	36%
11	17-Abr	6	14	43%
12	18-Abr	5	13	38%
13	19-Abr	4	12	33%
14	20-Abr	6	13	46%
15	21-Abr	7	11	64%
16	24-Abr	6	15	40%
17	25-Abr	6	12	50%
18	26-Abr	5	13	38%
19	27-Abr	5	15	33%
20	28-Abr	4	14	29%

Nivel de incidencias atendidas Post test

Ficha de Registro				
Investigador	Jose Luis Sanchez	**Tipo de Prueba**		Post test
Empresa investigada	CRATI E.I.R.L.			
Motivo de investigación	Nivel de incidencias atendidas			
Fecha inicio	2-May	**Fecha fin**		30-May
Investigación	Indicador	**Medida**	**Fórmula**	
Análisis de vulnerabilidades e incidencias en la Seguridad Informática	Nivel de incidencias atendidas	Porcentaje	NIAT=NIA/TIR x 100	
Item	**Fecha**	**Número de incidencias atendidas**	**Total de incidencias registradas**	**Nivel de incidencias atendidas**
1	2-May	10	13	0.77
2	3-May	11	12	0.92
3	4-May	12	14	0.86
4	5-May	9	12	0.75
5	8-May	10	13	0.77
6	9-May	11	14	0.79
7	10-May	9	15	0.60
8	11-May	10	15	0.67
9	12-May	11	16	0.69
10	15-May	10	12	0.83
11	16-May	11	13	0.85
12	17-May	9	12	0.75
13	18-May	10	14	0.71
14	19-May	11	14	0.79
15	22-May	12	14	0.86
16	23-May	10	12	0.83
17	24-May	9	13	0.69
18	25-May	12	15	0.80
19	26-May	11	14	0.79
20	29-May	9	12	0.75

Tiempo de resolución de Incidencias Pre test

Ficha de Registro					
Investigador	Jose Luis Sanchez	**Tipo de Prueba**			Pre Test
Empresa investigada	CRATI E.I.R.L.				
Motivo de investigación	Tiempo de Resolución de Incidencias				
Fecha inicio	3-Abr	**Fecha fin**			30-Abr
Investigación	Indicador	**Medida**	**Fórmula**		
Análisis de vulnerabilidades e incidencias en la Seguridad Informática	Tiempo de Resolución de Incidencias	Porcentaje		TRI=TRI/NTI x 100	
Dias	**Fecha**	**Tiempo de resolucion de Incidencias (horas)**	**Número de Incidencias atendidas**	**Número total de Incidencias**	**Tiempo de resolucion de Incidencias (horas)**
1	3-Abr	15.3	8	14	1.91
2	4-Abr	23.3	7	14	3.33
3	5-Abr	14.3	6	11	2.38
4	6-Abr	15.3	5	16	3.06
5	7-Abr	8.3	4	15	2.08
6	10-Abr	13.4	6	14	2.23
7	11-Abr	12.3	7	13	1.76
8	12-Abr	11.3	6	14	1.88
9	13-Abr	9.3	5	12	1.86
10	14-Abr	11.2	5	14	2.24
11	17-Abr	12.33	6	14	2.06
12	18-Abr	13.4	5	13	2.68
13	19-Abr	6.4	4	12	1.60
14	20-Abr	8.3	6	13	1.38
15	21-Abr	15.4	7	11	2.20
16	24-Abr	13.4	6	15	2.23
17	25-Abr	11.8	6	12	1.97
18	26-Abr	5.4	5	13	1.08
19	27-Abr	12.3	5	15	2.46
20	28-Abr	9.4	4	14	2.35

Tiempo de resolución de incidencias Post test

Ficha de Registro					
Investigador	Jose Luis Sanchez	**Tipo de Prueba**			Pre Test
Empresa investigada	CRATI E.I.R.L.				
Motivo de investigación	Tiempo de Resolución de Incidencias				
Fecha Inicio	3-Abr	**Fecha fin**			30-Abr
Investigación	Indicador	**Medida**	**Fórmula**		
Análisis de vulnerabilidades e incidencias en la Seguridad Informática	Tiempo de Resolución de Incidencias	Porcentaje			TRI=TRI/NTI_x 100
Dias	**Fecha**	**Tiempo de resolucion de incidencias (horas)**	**Número de incidencias atendidas**	**Número total de incidencias**	**Tiempo de resolucion de incidencias (horas)**
1	3-Abr	18.2	10	13	1.82
2	4-Abr	17.3	11	12	1.57
3	5-Abr	14.3	12	14	1.19
4	6-Abr	15.3	9	12	1.70
5	7-Abr	8.3	10	13	0.83
6	10-Abr	13.4	11	14	1.22
7	11-Abr	12.3	9	15	1.37
8	12-Abr	11.3	10	15	1.13
9	13-Abr	9.3	11	16	0.85
10	14-Abr	11.2	10	12	1.12
11	17-Abr	12.33	11	13	1.12
12	18-Abr	13.4	9	12	1.49
13	19-Abr	22.3	10	14	2.23
14	20-Abr	12.3	11	14	1.12
15	21-Abr	15.4	12	14	1.28
16	24-Abr	13.4	10	12	1.34
17	25-Abr	11.8	9	13	1.31
18	26-Abr	11.4	12	15	0.95
19	27-Abr	12.3	11	14	1.12
20	28-Abr	9.4	9	12	1.04

Anexo 3: Matriz Evaluación por juicio de expertos, formato UCV

Evaluación por juicio de expertos

Respetado juez. Usted ha sido seleccionado para evaluar el instrumento "Fichaje Índice de vulnerabilidades y Fichaje tiempo de resolución de incidencias". La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente, aportando al quehacer psicológico. Agradecemos su valiosa colaboración.

1. Datos generales del juez

Nombre del juez:	Marlon Acuña Benites
Grado profesional:	Maestría ( ) Doctor (X)
Área de formación académica:	Clínica ( ) Social ( ) Educativa (X) Organizacional ( )
Áreas de experiencia profesional:	Educación Universitaria
Institución donde labora:	Universidad César Vallejo
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (X)
Experiencia en Investigación Psicométrica: (si corresponde)	Trabajo(s) psicométricos realizados Título del estudio realizado.

2. Propósito de la evaluación:
Validar el contenido del instrumento, por juicio de expertos.

3. Soporte teórico
(describir en función al modelo teórico)

Escala/ÁREA	Subescala (dimensiones)	Definición

4. Presentación de instrucciones para el juez:
A continuación a usted le presento el cuestionario Evaluación por Juicio de Expertos elaborado por José Luis Sánchez Ruda en el año 2023 De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
	1. totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.

COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana con la dimensión.
	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de Acuerdo (alto nivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente

1 No cumple con el criterio
2. Bajo Nivel
3. Moderado nivel
4. Alto nivel

Dimensiones del instrumento:

- Primera dimensión: Alcance del análisis
- Objetivos de la Dimensión: Calcular

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Número de vulnerabilidades	4	4	4	4	
Severidad de las vulnerabilidades	2	3	3	4	
Tiempo de respuesta para resolver	3	4	4	4	
Cobertura del análisis	4	3	4	3	
Mejoras implementadas	5	3	3	3	

- Segunda dimensión: Vulnerabilidades técnicas
- Objetivos de la Dimensión: Identificar las vulnerabilidades y el tiempo de resolución para las incidencias presentadas.

INDICADORES	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Índice de Vulnerabilidades	1	4	3	4	
Tiempo de Resolución de Incidencias	2	4	4	4	

Dr. Marlon Acuña Benites
DNI: 42097456
Ing. de Sistemas / Investigador

Firma del evaluador
DNI

Pd.: el presente formato debe tomar en cuenta:
Williams y Webb (1994) así como Powell (2003), mencionan que no existe un consenso respecto al número de expertos a emplear. Por otra parte, el número de jueces que se debe emplear en un juicio depende del nivel de experticia y de la diversidad del conocimiento. Así, mientras Gable y Wolf (1993), Grant y Davis (1997), y Lynn (1986) (citados en McGartland et al. 2003) sugieren un rango de **2 hasta 20 expertos**, Hyrkäs et al. (2003) manifiestan que **10 expertos** brindarán una estimación confiable de la validez de contenido de un instrumento (cantidad mínimamente recomendable para construcciones de nuevos instrumentos). Si un 80 % de los expertos han estado de acuerdo con la validez de un ítem éste puede ser incorporado al instrumento (Voutilainen & Liukkonen, 1995, citados en Hyrkäs et al. (2003).
Ver : https://www.revistaespacios.com/cited2017/cited2017-23.pdf entre otra bibliografía

Anexo 2

Evaluación por juicio de expertos

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento "Fichaje Índice de vulnerabilidades y Fichaje tiempo de resolución de incidencias". La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de este sean utilizados eficientemente; aportando al quehacer psicológico. Agradecemos su valiosa colaboración.

1. Datos generales del juez

Nombre del juez:	ARIANA MAYBEE ORUÉ MEDINA
Grado profesional:	Maestría (X) Doctor ( )
Área de formación académica:	Clínica ( ) Social ( ) Educativa ( ) Organizacional ( )
Áreas de experiencia profesional:	INGENIERÍA DE SISTEMAS
Institución donde labora:	MUNICIPALIDAD PROVINCIAL CALLAO
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (X)
Experiencia en Investigación Psicométrica: (si corresponde)	Trabajo(s) psicométricos realizados Título del estudio realizado.

2. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

3. Soporte teórico

(Describir en función al modelo teórico)

Escala/ÁREA	Subescala (dimensiones)	Definición
Razón	Vulnerabilidades técnicas	Las vulnerabilidades en seguridad de la información son fallos, debilidades o defectos en el diseño, implementación o funcionamiento de los sistemas informáticos, que pueden ser explotados por los atacantes para comprometer la confidencialidad, integridad o disponibilidad de los datos y sistemas (Alcántara & Cruz, 2021, p. 1).
Razón	Monitoreo y mejora	Una incidencia de seguridad informática es cualquier suceso que comprometa la confidencialidad, integridad o disponibilidad de los datos o sistemas informáticos (Quispe et al., 2021, p. 38).

4. Presentación de instrucciones para el juez:

A continuación a usted le presento el cuestionario evaluación de juicio de expertos elaborado por Jose Luis Sanchez Quispe el año 2023 De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, es	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.

decir, su sintáctica y semántica son adecuadas.	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA. El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana con la dimensión.
	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de Acuerdo (alto nivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA. El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente

1 No cumple con el criterio
2. Bajo Nivel
3. Moderado nivel
4. Alto nivel

Dimensiones del instrumento:

- Primera dimensión: Vulnerabilidades técnicas
- Objetivos de la Dimensión: Calcular

Indicadores	**Ítem**	**Claridad**	**Coherencia**	**Relevancia**	**Observaciones/ Recomendaciones**
Índice de Vulnerabilidades corregidas	30	4	3	4	
Índice de vulnerabilidades no corregidas	30	4	3	4	

- Segunda dimensión: Monitoreo y mejora
- Objetivos de la Dimensión: Identificar las vulnerabilidades y el tiempo de resolución para las incidencias presentadas.

INDICADORES	**Ítem**	**Claridad**	**Coherencia**	**Relevancia**	**Observaciones/ Recomendaciones**
Tiempo de Resolución de Incidencias	20	4	3	4	
Nivel de incidencias atendidas	20	4	3	4	

MG . ARIANA MAYBEE ORUÉ MEDINA
DNI 48164963

Pd.: el presente formato debe tomar en cuenta:

Williams y Webb (1994) así como Powell (2003), mencionan que no existe un consenso respecto al número de expertos a emplear. Por otra parte, el número de jueces que se debe emplear en un juicio depende del nivel de experticia y de la diversidad del conocimiento. Así, mientras Gable y Wolf (1993), Grant y Davis (1997), y Lynn (1986) (citados en McGartland et al. 2003) sugieren un rango de **2** hasta **20 expertos**, Hyrkäs et al. (2003) manifiestan que **10 expertos** brindarán una estimación confiable de la validez de contenido de un instrumento (cantidad mínimamente recomendable para construcciones de nuevos instrumentos). Si un 80 % de los expertos han estado de acuerdo con la validez de un ítem éste puede ser incorporado al instrumento (Voutilainen & Liukkonen, 1995, citados en Hyrkäs et al. (2003).

Ver : https://www.revistaespacios.com/cited2017/cited2017-23.pdf entre otra bibliografía

Anexo 2

Evaluación por juicio de expertos

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento "Fichaje Índice de vulnerabilidades y Fichaje tiempo de resolución de incidencias". La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente; aportando al quehacer psicológico. Agradecemos su valiosa colaboración.

1. Datos generales del juez

Nombre del juez:	Dr. BEKER MARAZA VILCANQUI
Grado profesional:	Maestría ( ) Doctor (X)
Área de formación académica:	Clínica ( ) Social ( ) Educativa ( ) Organizacional ( )
Áreas de experiencia profesional:	INGENIERÍA
Institución donde labora:	MUNICIPALIDAD DE UCAYALI
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (x)
Experiencia en investigación Psicométrica: (si corresponde)	Trabajo(s) psicométricos realizados Título del estudio realizado.

2. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

3. Soporte teórico

(describir en función al modelo teórico)

Escala/ÁREA	Subescala (dimensiones)	Definición
Razón	Vulnerabilidades técnicas	Las vulnerabilidades en seguridad de la información son fallos, debilidades o defectos en el diseño, implementación o funcionamiento de los sistemas informáticos, que pueden ser explotados por los atacantes para comprometer la confiabilidad, integridad o disponibilidad de los datos y sistemas (Alqahtani & Zou, 2021, p. 1).
Razón	Monitoreo y mejora	Una incidencia de seguridad informática es cualquier suceso que compromete la confiabilidad, integridad o disponibilidad de los datos o sistemas informáticos (Sahu et al., 2021, p. 38).

4. Presentación de instrucciones para el juez:

A continuación a usted le presento el cuestionario evaluación de juicio de expertos elaborado por Jose Luis Sanchez Bardales el año 2023 De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, es	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.

decir, su sintáctica y semántica son adecuadas.	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. Totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana con la dimensión.
	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de Acuerdo (alto nivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente

1 No cumple con el criterio
2. Bajo Nivel
3. Moderado nivel
4. Alto nivel

Dimensiones del instrumento:

- Primera dimensión: Vulnerabilidades técnicas
- Objetivos de la Dimensión: Calcular

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Indice de Vulnerabilidades corregidas	30	4	4	4	
Indice de vulnerabilidades no corregidas	30	4	4	4	

- Segunda dimensión: Monitoreo y mejora
- Objetivos de la Dimensión: Identificar las vulnerabilidades y el tiempo de resolución para las incidencias presentadas.

INDICADORES	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Tiempo de Resolución de Incidencias	20	4	4	4	
Nivel de incidencias atendidas	20	4	3	3	

Dr. Boker Maraza Yllanqui
DNI 01343336

Pd.: el presente formato debe tomar en cuenta:

Williams y Webb (1994) así como Powell (2003), mencionan que no existe un consenso respecto al número de expertos a emplear. Por otra parte, el número de jueces que se debe emplear en un juicio depende del nivel de experticia y de la diversidad del conocimiento. Así, mientras Gable y Wolf (1993), Grant y Davis (1997), y Lynn (1986) (citados en McGartland et al. 2003) sugieren un rango de **2** hasta **20 expertos**, Hyrkäs et al. (2003) manifiestan que **10 expertos** brindarán una estimación confiable de la validez de contenido de un instrumento (cantidad mínimamente recomendable para construcciones de nuevos instrumentos). Si un 80 % de los expertos han estado de acuerdo con la validez de un ítem éste puede ser incorporado al instrumento (Davis & Larrabee, 1988, citados en Hyrkäs et al. (2003).

Ver : http://www.revistaespacios.com/a18v39n07/a18v39n07p23.pdf entre otra bibliografía