UNIVERSIDAD NACIONAL DEL CALLAO

FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

UNIDAD DE INVESTIGACIÓN DE LA FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS

"IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE VULNERABILIDADES PARA MEJORAR LA PRODUCTIVIDAD EN LA EMPRESA CONTACTA HABILIDAD S.A.C., LIMA – 2024"

TESIS PARA OPTAR ELTÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

AUTOR/ES:
FLORES HUANCA MARÍA INÉS

NUÑEZ ZEGARRA FIORELLA ARACELI

VILLEGAS PACHECO ANDREA GIULIANA

ASESOR: OSMART MORALES CHALCO

LÍNEA DE INVESTIGACIÓN: **INGENIERÍA Y TECNOLOGÍA**

Callao, 2024
PERÚ

HOJA DE REFERENCIA DEL JURADO Y APROBACIÓN

MIEMBROS DEL JURADO DE SUSTENTACIÓN:

- MG. FARFÁN AGUILAR JOSÉ ANTONIO — PRESIDENTA
- MG. ANGELINO ABAD RAMOS CHOQUEHUANCA — SECRETARIA
- DR. ANIVAL ALFREDO TORRE CAMONES — MIEMBRO
- DR. RUIZ NIZAMA JOSE LEONOR — SUPLENTE

ASESOR: Osmart Morales Chalco

Nº de Libro: …N° 001……..

N° de Folio: …N° 28……

Nº de Acta: …005-2024-II-CTT-IS

Fecha de Aprobación de la tesis: 18-05-2024

Resolución de Sustentación: Nº 361-2024-CF-FIIS

INFORMACIÓN BÁSICA

FACULTAD: Facultad de Ingeniería Industrial y de Sistemas.

UNIDAD DE INVESTIGACIÓN: Automatización

ESCUELA PROFESIONAL: Escuela profesional de Ingeniería De Sistemas.

TÍTULO: "IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE VULNERABILIDADES PARA MEJORAR LA PRODUCTIVIDAD EN LA EMPRESA CONTACTA HABILIDAD S.A.C., LIMA – 2024"

AUTORES:

MARÍA INÉS FLORES HUANCA
CÓDIGO ORCID: 0009-0002-7489-7319
DNI:77174623

FIORELLA ARACELI NUÑEZ ZEGARRA
CÓDIGO ORCID: 0009-0002-3527-8937
DNI: 77096692

ANDREA GIULIANA VILLEGAS PACHECO
CÓDIGO ORCID: 0009-0003-6931-6759
DNI:73684340

ASESOR: OSMART MORALES CHALCO - 09900421 - 0000-0002-5850-4899

LUGAR DE EJECUCIÓN: LIMA

UNIDAD DE ANÁLISIS: ACTIVOS DE TECNOLOGÍA DE INFORMACIÓN DE LA EMPRESA CONTACTA HABILIDAD S.A.C.

TIPO DE INVESTIGACIÓN: APLICADA

ENFOQUE: CUANTITATIVO

DISEÑO DE INVESTIGACIÓN: EXPERIMENTAL

TEMA OCDE: OTRAS INGENIERÍAS Y TECNOLOGÍAS

ACTA DE SUSTENTACIÓN

ACTA DE SUSTENTACION POR MODALIDAD DE CICLO TALLER DE TESIS PARA LA OBTENCIÓN DEL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

ACTA Nº 005-2024-II-CTT-IS

Siendo las 16:30 horas del día 18 de Mayo del año 2024, encontrándose reunidos en el Auditorio de la FIIS, el **DR. ENRIQUE GARCÍA TALLEDO,** en representación de la Rectora de la UNAC; el **JURADO DE SUSTENTACIÓN DE TESIS** (designado por resolución **361-2024-CF-FIIS**)de la Facultad Ingeniería Industrial y de Sistemas de la Universidad Nacional del Callao, para la evaluación de las Tesis que conllevan a la obtención del Título Profesional de **INGENIERO DE SISTEMAS**, el que se encuentra conformado por los siguientes docentes ordinarios:

PRESIDENTE	**MG. FARFÁN AGUILAR JOSÉ ANTONIO**
SECRETARIO	**MG. ANGELINO ABAD RAMOS CHOQUEHUANCA**
VOCAL	**DR. ANIVAL ALFREDO TORRE CAMONES**
SUPLENTE	**DR. RUIZ NIZAMA JOSE LEONOR**

Con el quórum reglamentario de ley y de conformidad con lo establecido por el Reglamento de Grados y Títulos vigente se dio inicio al Acto de Sustentación de la Tesis de las Bachilleres: **NUÑEZ ZEGARRA FIORELLA ARACELI, VILLEGAS PACHECO ANDREA** y **FLORES HUANCA MARÍA INÉS;** quienes, habiendo cumplido con los requisitos para optar el Título Profesional de **INGENIERO DE SISTEMAS**, sustentan la tesis titulada **"IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE VULNERABILIDADES PARA MEJORAR LA PRODUCTIVIDAD EN LA EMPRESA CONTACTA HABILIDAD S.A.C, LIMA-2024",** cumpliendo con la sustentación en acto público, de manera presencial.

Luego de la exposición, y de la absolución de las preguntas formuladas por el Jurado de Sustentación y efectuadas las deliberaciones pertinentes, **SE ACORDÓ**: Dar por **APROBADO** con la escala de calificación cuantitativa **(16)** y calificación cualitativa **(Muy Bueno)** a la presente tesis, conforme a lo dispuesto en el Art. 24 del Reglamento de Grados y Títulos de la UNAC, aprobado por Resolución de Consejo Universitario N° 150-2023-CU del 15 de junio del 2023.

Se dio por concluida la Sesión a las 17:00 horas del día 18 de Mayo del 2024.

MG. FARFÁN AGUILAR JOSÉ ANTONIO
Presidente

MG. ANGELINO ABAD RAMOS CHOQUEHUANCA
Secretario

DR. ANIVAL ALFREDO TORRE CAMONES
Vocal

DR. JOSE LEONOR RUIZ NIZAMA
Suplente

INFORME Nº 005-2024-JS-II-CTT-IS

PARA : **DR. PAUL GREGORIO PAUCAR LLANOS**
DECANO FIIS

DE : **JURADO DE SUSTENTACIÓN DEL II CICLO TALLER DE TESIS DE INGENIERÍA DE SISTEMAS**

ASUNTO : **INFORME FAVORABLE DEL JURADO DE SUSTENTACIÓN**

FECHA : **Callao, 18 de Mayo del 2024**

Los miembros del Jurado de Sustentación designados por **Resolución Nº 361-2024-CF-FIIS** y de acuerdo al Reglamento de Grados y Títulos, aprobado por Resolución 150-2023-CU del 15 de junio de 2023 Art. 71, visto el Acta de Sustentación **Nº 005-2024-II-CTT-IS** de Tesis Titulada: **"IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE VULNERABILIDADES PARA MEJORAR LA PRODUCTIVIDAD EN LA EMPRESA CONTACTA HABILIDAD S.A.C, LIMA-2024"**

Presentado por:
NUÑEZ ZEGARRA FIORELLA ARACELI
VILLEGAS PACHECO ANDREA
FLORES HUANCA MARÍA INÉS

Para obtener Título de Profesional de **INGENIERO DE SISTEMAS,** por modalidad de Tesis con Ciclo Taller de Tesis, habiendo obtenido nota aprobatoria de (16) dieciséis, Muy Bueno.

En tal sentido, los miembros del Jurado de Sustentación informan que no existe observación alguna a dicha Tesis por lo que se da la **CONFORMIDAD,** lo cual se debe comunicar a los interesados.

Sin otro particular reiteramos los sentimientos y estima personal.

MG. FARFAN AGUILAR JOSÉ ANTONIO
Presidente

MG. ANGELINO ABAD RAMOS CHOQUEHUANCA
Secretario

DR. ANIVAL ALFREDO TORRE CAMONES
Vocal

DR. JOSE LEONOR RUIZ NIZAMA
Suplente

1A, NUÑEZ ZEGARRA, VILLEGAS PACHECO, FLORES HUANCA-TESIS PREGRADO-2024

17% Textos sospechosos

17% Similitudes
2% similitudes entre comillas
0% entre las fuentes mencionadas
< 1% Idiomas no reconocidos

Nombre del documento: 1A, NUÑEZ ZEGARRA, VILLEGAS PACHECO, FLORES HUANCA-TESIS PREGRADO-2024.docx
ID del documento: 55c674f67c4b6a195ed87c69cbecebdcac6d8ca5
Tamaño del documento original: 1,21 MB

Depositante: FIIS PREGRADO UNIDAD DE INVESTIGACION
Fecha de depósito: 6/5/2024
Tipo de carga: interface
fecha de fin de análisis: 6/5/2024

Número de palabras: 11.403
Número de caracteres: 78.938

Ubicación de las similitudes en el documento:

Fuentes de similitudes

Fuentes principales detectadas

N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	**repositorio.unac.edu.pe** https://repositorio.unac.edu.pe/bitstream/handle/20.500.12952/8536/TESIS - CHAVEZ-FLORES-ROBL...	3%		Palabras idénticas: **3%** (405 palabras)
2	**qasrepositorio.esan.edu.pe** https://qasrepositorio.esan.edu.pe/bitstream/handle/20.500.12640/3432/2023_MADTI_19-2_05_TI.p... **20 fuentes similares**	2%		Palabras idénticas: **2%** (204 palabras)
3	**dspace.utb.edu.ec** http://dspace.utb.edu.ec/bitstream/49000/6872/6/E-UTB-FAFI-SIST-00017.pdf.txt **1 fuente similar**	2%		Palabras idénticas: **2%** (196 palabras)
4	**repositorio.upse.edu.ec** https://repositorio.upse.edu.ec/bitstream/46000/5754/1/UPSE-TTI-2021-0007.pdf **1 fuente similar**	1%		Palabras idénticas: **1%** (180 palabras)
5	**repositorio.unne.edu.ar** https://repositorio.unne.edu.ar/bitstream/handle/123456789/28453/RIUNNE_FACENA_TM_Cossio Ci...	1%		Palabras idénticas: **1%** (156 palabras)

Fuentes con similitudes fortuitas

N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	**repositorio.continental.edu.pe** | Repositorio Continental: Tesis https://repositorio.continental.edu.pe/handle/20.500.12394/258	< 1%		Palabras idénticas: **< 1%** (40 palabras)
2	**repositorio.ucv.edu.pe** | Implementación de un sistema de ciberseguridad para la... https://repositorio.ucv.edu.pe/handle/20.500.12692/70776?show=full	< 1%		Palabras idénticas: **< 1%** (34 palabras)
3	**www.alearningcenter.com** | Auditor Líder ISO 27001:2022 | Advanced Learning Ce... https://www.alearningcenter.com/auditor-lider-27001/	< 1%		Palabras idénticas: **< 1%** (32 palabras)
4	**repositorio.unac.edu.pe** https://repositorio.unac.edu.pe/bitstream/handle/20.500.12952/8734/TESIS - LLANOS-MAMANI-NAP...	< 1%		Palabras idénticas: **< 1%** (25 palabras)
5	**1A, SUÁREZ RODRÍGUEZ CHRISTIAN JESÚS-INFORME FINAL-2024.pdf** | 1... #7b61da El documento proviene de mi biblioteca de referencias	< 1%		Palabras idénticas: **< 1%** (21 palabras)

DEDICATORIA

Dedicamos esta investigación a Dios, a nuestras familias y a nuestros profesores por su apoyo incondicional y orientación invaluable durante todo el proceso.

Que este trabajo sea un testimonio de nuestro compromiso colectivo con la excelencia académica y contribuya al avance del conocimiento en nuestra área de estudio.

AGRADECIMIENTO

Agradecemos principalmente a Dios, por ser nuestra guía y fortaleza durante este viaje académico.

A nuestras familias, cuyo amor y apoyo incondicional han sido nuestra mayor motivación y respaldo.

A nuestra querida Universidad Nacional del Callao por proporcionarnos las herramientas y conocimientos necesarios para nuestro desarrollo profesional.

Sin su apoyo, este logro no habría sido posible.

ÍNDICE

ÍNDICE DE TABLAS DE CONTENIDO

ÍNDICE DE FIGURAS

RESUMEN

La gestión de vulnerabilidades es un desafío para la empresa Contacta Habilidad S.A.C., quienes a menudo se encuentran con dificultades al intentar identificar, priorizar y remediar eficazmente las vulnerabilidades en sus activos de Tecnología de la Información por lo que involucra un alto nivel operativo en esta gestión.

Con la implementación de un Sistema de Gestión de Vulnerabilidades se busca mejorar la productividad, reducir costos y esfuerzos de los equipos responsables adoptando las mejores prácticas e incluyendo la priorización basada en riesgos.

Se realizó un análisis exhaustivo de las vulnerabilidades existentes en los servidores y aplicaciones web de toda la empresa y se implementó un software especializado para facilitar la gestión y la remediación automática de estas vulnerabilidades. Se utilizó el Framework Gartner como guía para el proceso de gestión de vulnerabilidades que define este proceso como el ciclo para encontrar, evaluar, remediar y mitigar las debilidades de seguridad en los activos de Tecnología de la Información.

Los resultados obtenidos proporcionaron evidencia sólida de que la implementación del Sistema de Gestión de Vulnerabilidades contribuyó significativamente a mejorar la eficiencia y la eficacia en la empresa, lo que llevó a una reducción de vulnerabilidades y esfuerzos en la etapa de remediación.

Implementar un sistema de gestión de vulnerabilidades es esencial para elevar la seguridad y la eficiencia operativa de la empresa, además de reducir riesgos potenciales tal como se muestra en los resultados obtenidos en esta investigación.

Palabras clave: gestión, vulnerabilidades, productividad, riesgos, sistemas, implementación**.**

ABSTRACT

The management of vulnerabilities is a challenge for Contacta Habilidad S.A.C., as they often face difficulties when trying to identify, prioritize, and effectively remediate vulnerabilities in their Information Technology assets, which is why they involve a high operational level in this management.

With the implementation of a Vulnerability Management System, the aim is to improve productivity, reduce costs, and efforts of the responsible team by adopting best practices and including risk-based prioritization.

A comprehensive analysis of existing vulnerabilities in the company's servers and web applications was conducted, and specialized software was implemented to facilitate the management and automatic remediation of these vulnerabilities. The Gartner Framework was used as a guide for the vulnerability management process, which defines this process as the cycle for finding, assessing, remediating, and mitigating security weaknesses in Information Technology assets.

The results obtained provided solid evidence that the implementation of the Vulnerability Management System significantly contributed to improving efficiency and effectiveness in the company, leading to a reduction in vulnerabilities and efforts in the remediation stage.

Implementing a vulnerability management system is essential to enhance the security and operational efficiency of the company, as well as to reduce potential risks, as shown in the results obtained in this research.

Keywords: management, vulnerabilities, system, implementationKeywords: management, vulnerabilities, productivity, risks, systems, implementation.

INTRODUCCIÓN

La presente investigación abordó los desafíos que enfrenta la empresa en la gestión de vulnerabilidades de sus activos de Tecnología de la Información el cual tiene un impacto negativo en la productividad de la empresa Contacta Habilidad S.A.C.

El propósito de esta investigación fue implementar un sistema de gestión de vulnerabilidades que permita mejorar la productividad basándose en las directrices del Framework de Gartner y la implementación de un software que facilite la remediación automática de vulnerabilidades con el fin de mejorar la eficiencia y eficacia en la organización.

En el capítulo I se examina la problemática central, exponiendo el dilema a investigar y proponiendo soluciones mediante establecimiento de objetivos generales y específicos.
En el capítulo II se centra en proporcionar las bases teóricas necesarias y antecedentes estudiados, ofreciendo una visión general de los temas abordados mediante una explicación detallada.
En el capítulo III se dedica a formular las hipótesis generales y específicas de la investigación, así como a describir las variables de estudio empleadas para la misma.
En el capítulo IV se detalla la metodología empleada en la investigación, se identifican los problemas a resolver y se determina cómo se llevará a cabo la medición de la propuesta, delineando las estrategias utilizadas y validando las hipótesis propuestas.
En el capítulo V se presentan los resultados de la investigación, especialmente de forma descriptiva, mostrando los reportes en acción hacia la propuesta planteada en este trabajo de investigación.
En el capítulo VI se analiza los resultados obtenidos para luego proceder a la elaboración de las conclusiones extraídas del trabajo realizado.

En el capítulo VII se exponen las conclusiones derivadas de la investigación, haciendo hincapié en la validación de la propuesta inicial y comparando los aspectos positivos y negativos de los resultados obtenidos.

En el capítulo VIII se presentan recomendaciones que podrían complementar la propuesta definida en este trabajo y permite analizarla desde diferentes perspectivas para su posible implementación.

I. PLANTEAMIENTO DEL PROBLEMA

1.1 Descripción de la realidad problemática

A nivel global la creciente interconectividad ha llevado a un aumento exponencial de los ciberataques. Las organizaciones de todos los rubros enfrentan desafíos significativos en la protección de sus activos digitales. Según "Internet Security Threat Report" de Symantec (2020), se observó un incremento del 12% en las brechas de seguridad reportadas en comparación con el año anterior, con más de 4,1 mil millones de registros expuestos. Este incremento subraya la necesidad urgente de soluciones robustas para la gestión de vulnerabilidades, ya que la ciberseguridad se ha convertido en una prioridad crítica para mantener la integridad y confidencialidad de los datos.

A nivel Latinoamérica la situación es igualmente preocupante. El ESET Security Report (2020) reveló que el 60% de las empresas latinoamericanas reportaron al menos un incidente de seguridad durante el año. Entre estos incidentes, la infección por códigos maliciosos es el caso más común, afectando al 33% de las empresas. Este alto porcentaje de incidentes destaca la vulnerabilidad de las organizaciones en la región y la necesidad de fortalecer sus defensas cibernéticas. La falta de implementación de sistemas de gestión de vulnerabilidades eficientes deja a muchas empresas expuestas a amenazas que podrían haberse prevenido con medidas adecuadas.

A nivel nacional, En Perú, la situación es igualmente crítica. Según el Diario Gestión (2018), las pymes peruanas muestran un notable desinterés en la ciberseguridad, reflejado en una baja inversión en esta área y en los 21,800 ataques cibernéticos registrados en el país, equivalentes a 60 ataques diarios. Este desinterés se evidenció en una encuesta de Optical Networks, donde solo el 30% de las pymes realizaron un diagnóstico sobre las vulnerabilidades de sus sistemas informáticos. La falta de conciencia y acción en ciberseguridad no solo expone a estas empresas a riesgos significativos, sino que también amenaza su continuidad operativa y su capacidad para competir en el mercado.

Contacta Habilidad S.A.C. se especializa en proporcionar plataformas inteligentes de negocio bidireccionales y autoadministrables que facilitan la comunicación entre empresas y clientes. Su sistema integral está diseñado para agilizar la toma de decisiones, maximizar la efectividad de la comunicación y ofrecer servicios como mensajería instantánea, evaluación de campañas en tiempo real y configuración de llamadas con prioridad. A pesar de estas fortalezas, la empresa enfrenta serios desafíos en la identificación y resolución oportuna de vulnerabilidades en su infraestructura tecnológica.

La ausencia de un sistema de gestión de vulnerabilidades eficiente no solo expone a Contacta Habilidad S.A.C. a riesgos constantes de ataques cibernéticos y pérdida de datos, sino que también afecta directamente su productividad y eficacia operativa. Esta situación genera interrupciones no planificadas en las operaciones, lo que impacta negativamente en la productividad y la efectividad del personal. Además, la falta de una respuesta ágil y eficiente ante incidentes de seguridad contribuye a prolongar los tiempos de inactividad y aumentar los costos operativos.

La gestión inadecuada del tiempo de atención a las vulnerabilidades también incide en la eficiencia de la empresa. Sin directrices claras para priorizar y resolver las vulnerabilidades de manera rápida y efectiva, se produce una utilización ineficiente de los recursos, tanto humanos como tecnológicos. Esto se traduce en una disminución en la capacidad de respuesta ante situaciones críticas y en una menor eficacia en la protección de los activos de información.

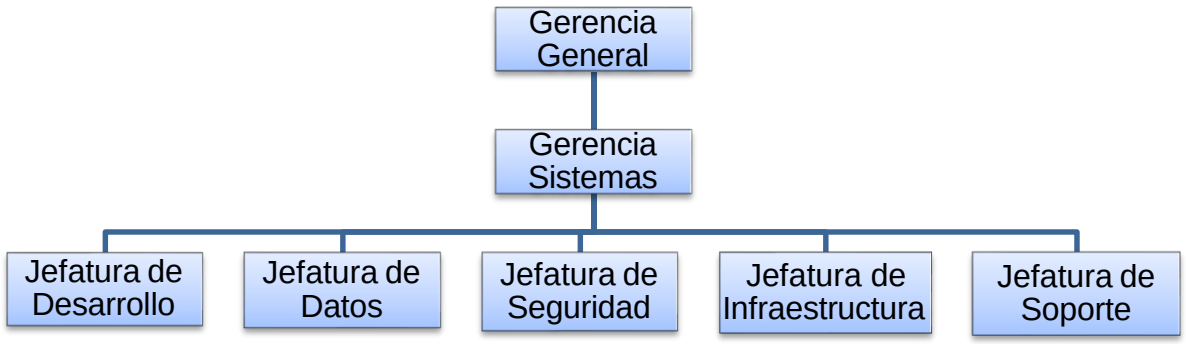
Este análisis FODA proporciona una visión clara de las fortalezas, oportunidades, debilidades y amenazas de Contacta Habilidad S.A.C. antes de la implementación del sistema de gestión de vulnerabilidades, resaltando la importancia y el potencial impacto positivo de nuestra investigación.

Tabla N° 1: *FODA Contacta Habilidad S.A.C.*

FORTALEZAS	DEBELIDADES
• Contacta Habilidad SAC se destaca por ofrecer plataformas inteligentes que facilitan la comunicación bidireccional y autoadministrable entre empresas y clientes. • Su sistema integral está diseñado para agilizar la toma de decisiones y maximizar la efectividad de la comunicación empresarial. • Capacidad de adaptación rápida a las necesidades del mercado y de los clientes, proporcionando soluciones personalizadas y efectivas.	• Los procesos manuales pueden resultar en un tiempo de respuesta más lento para identificar y mitigar vulnerabilidades. • La ausencia de herramientas avanzadas de escaneo y mitigación de vulnerabilidades puede limitar la capacidad de la empresa para manejar amenazas complejas. • Los costos asociados a la implementación de nuevas tecnologías y sistemas de gestión de vulnerabilidades pueden ser significativos y representar un desafío financiero.
OPORTUNIDADES	**AMENAZAS**
• La creciente necesidad de soluciones de comunicación empresarial ofrece oportunidades para expandir la base de clientes. • La implementación de un sistema de gestión de vulnerabilidades puede mejorar significativamente la seguridad de las aplicaciones y servidores y la eficiencia operativa, reduciendo riesgos y optimizando recursos. • La automatización de la identificación y mitigación de vulnerabilidades puede reducir la dependencia del trabajo manual, aumentando la eficiencia y precisión.	• La rápida evolución de las amenazas cibernéticas requiere una vigilancia constante y la capacidad de adaptación rápida. • La existencia de vulnerabilidades no descubiertas puede poner en riesgo la seguridad de la información. • El incumplimiento de las normativas de seguridad puede resultar en sanciones y daños a la reputación de la empresa. • La creciente cantidad de empresas en el sector de soluciones de comunicación empresarial aumenta la competencia, lo que puede afectar la cuota de mercado y presionar los márgenes de beneficio.

Fuente: Elaboración Propia

Figura N° 1: *Organigrama de la empresa Contacta Habilidad S.A.C*



Fuente: Elaboración Propia

1.2 Formulación del Problema

1.2.1 Problema General

¿De qué manera la implementación de un Sistema de Gestión de Vulnerabilidades mejora la productividad en la empresa Contacta Habilidad S.A.C., Lima - 2024?

1.2.2 Problemas Específicos

- ¿De qué manera la implementación de un Sistema de Gestión de Vulnerabilidades mejora la eficiencia en la empresa Contacta Habilidad S.A.C., Lima - 2024?

- ¿De qué manera la implementación de un Sistema de Gestión de Vulnerabilidades mejora la eficacia en la empresa Contacta Habilidad S.A.C., Lima - 2024?

1.3 Objetivos

1.3.1 Objetivo General

Determinar de qué manera la implementación de un Sistema de Gestión de Vulnerabilidades mejora la productividad en la empresa Contacta Habilidad S.A.C., Lima - 2024.

1.3.2 Objetivos Específicos

- Determinar de qué manera la implementación de un Sistema de Gestión de Vulnerabilidades mejora la eficiencia en la empresa Contacta Habilidad S.A.C., Lima - 2024

- Determinar de qué manera la implementación de un Sistema de Gestión de Vulnerabilidades mejora la eficacia en la empresa Contacta Habilidad S.A.C., Lima - 2024

1.4 Justificación

1.4.1 Justificación Teórica

El proyecto de tesis radica en la necesidad de contribuir al corpus de conocimiento existente en el ámbito de la gestión de vulnerabilidades, específicamente en relación con su impacto en la productividad en el área de seguridad de las organizaciones, cuyos resultados podrán sistematizarse en una propuesta, para ser incorporado como conocimiento al área de seguridad, ya que se estaría demostrando que la gestión de vulnerabilidades mejora la productividad en el área de seguridad.

1.4.2 Justificación Metodológica

El proyecto de tesis se justifica metodológicamente debido a que se realizó un análisis a nuestras variables, tanto dependiente como independiente, lo que nos ayudó a examinar de manera sistemática y objetiva la relación entre la implementación del sistema de gestión de vulnerabilidades y la mejora de la productividad.

El análisis cuantitativo permitió aumentar la validez y la fiabilidad de los resultados obtenidos, mismos que podrán ser utilizados en otros proyectos de tesis y pequeñas empresas.

1.4.3 Justificación Práctica

Al centrarse en la implementación de un sistema de gestión de vulnerabilidades y su impacto en la productividad en la empresa Contacta Habilidad S.A.C., este estudio busca proporcionar resultados tangibles que puedan ser utilizados para mejorar la eficiencia y la eficacia en la gestión de vulnerabilidades ofreciendo soluciones concretas y aplicables a una problemática real en el ámbito empresarial.

1.5 Delimitantes de la investigación

Con el propósito de hacer viable la propuesta de este proyecto de investigación se establecieron criterios que delimitan el alcance del proyecto. Las cuales se dividen en teórico, espacial y temporal.

1.5.1 Teórico

La propuesta de la implementación de un sistema de gestión de vulnerabilidades se desarrolla utilizando habilidades teóricas metodológicas, terminología y enfoques que han demostrado mejorar la productividad, para esto existen múltiples herramientas que permiten identificar, priorizar, mitigar y validar la correcta gestión de vulnerabilidades de acuerdo a los requerimientos que influyen

para mejorar la productividad en una pequeña empresa, generando información de los avances y teorías desarrollados en el primer trimestre del año 2024.

1.5.2 Temporal

La obtención de resultados para validar la relación de un sistema de gestión de vulnerabilidades y la productividad del área de la empresa CONTACTA HABILIDAD S.A.C. comenzará en el último trimestre del año 2023 y finalizará en el primer trimestre del año 2024.

1.5.3 Espacial

La propuesta del proyecto de investigación se delimitará en todos los activos de Tecnología de Información de la empresa CONTACTA HABILIDAD S.A.C. Específicamente en los servidores y aplicaciones que forman parte de la operativa de la organización.

II. MARCO TEÓRICO

2.1 Antecedentes

2.1.1. Antecedentes Internacionales

Catuto Pilar (2021), en su estudio “Análisis de amenazas y vulnerabilidades informáticas basado en la Norma ISO 27002, en el proceso de citas del servidor web de una Institución Santa Elena, 2021”, el objetivo es analizar los posibles riesgos, amenazas del sistema informático de citas, consultas e historiales, mediante la norma ISO 27002 para mejorar la confiabilidad en las áreas de la clínica. Se realizó un estudio investigativo de tipo exploratorio ya que se llevará a cabo las diferentes técnicas de recopilación de información, consultar los problemas a los que se enfrenta la institución ya que anteriormente no se ha realizado un análisis de amenazas y vulnerabilidades informática en la institución. Con los resultados de los riesgos existentes y de los activos que se involucran antes las pérdidas de información, se espera minimizar los riesgos empleando controles de seguridad de la norma ISO 27002 lo cual ayuda a fortalecer tres aspectos importantes: la confidencialidad, integridad y disponibilidad de la información que corresponda a las necesidades de seguridad informática, de esta forma tendremos una protección de los datos, una vez aplicada políticas de seguridad informática mejorando los niveles de seguridad de la información de los procesos de la clínica. (Catuto, 2021)

Cuesta Morante (2019), en su investigación “Análisis de Amenazas y Vulnerabilidades dentro del Sistema de Gestión del Voluntariado en la Cruz Roja ubicada en la Ciudad de Babahoyo, Ecuador 2019”, el objetivo de este estudio es hacer el análisis al sistema corregir estas vulnerabilidades para evitar o minimizar los riesgos de fuga de información, para este estudio se utilizó el método cuantitativo ya que la información fue obtenida a través de encuestas realizadas a los voluntarios de la cruz roja, recopilando datos concretos estructurados y estadísticos para el desarrollo y respaldo del estudio de caso. El presente estudio de caso logra demostrar que el sistema de gestión del voluntariado de la cruz roja

presenta varias fallas de seguridad que pueden poner en peligro la integridad de los datos y de su infraestructura tecnológica. La utilización de herramientas como “Nessus” que permiten analizar el sistema para encontrar vulnerabilidades, proporciona información que puede ser utilizada para corregir y mejorar el funcionamiento para tener un mayor grado de seguridad en la información sensible de la organización. Los resultados obtenidos en el análisis al sistema informático permiten identificar brechas de seguridad las cuales pueden ser aprovechadas por piratas informáticos para fines no éticos, el objetivo de hacer el análisis al sistema es corregir estas vulnerabilidades para evitar o minimizar los riesgos de fuga de información. (Morante,2019)

Cedeño Zambrano (2021), en su investigación “Detección de vulnerabilidades mediante pruebas de penetración a la red de servidores y servicios del Instituto Superior Tecnológico Sucre Cohorte, 2021”, cuyo objetivo desarrollar un plan de mejoras que permita mitigar vulnerabilidades identificadas mediante la ejecución de pruebas de penetración en la red de servidores y servicios del Instituto Superior Tecnológico Sucre. Se utilizó la metodología de investigación cualitativa con un enfoque exploratorio, empleando además una investigación de campo mediante la realización de entrevistas, la observación, listas de cotejo y la ejecución de pruebas de penetración externas de caja negra sobre la red de servidores y servicios del Instituto Superior Tecnológico Sucre. Las pruebas de penetración se las realizó siguiendo un proceso de fases, tal es el caso, que en primer lugar se ejecutó una fase de reconocimiento y recopilación de información a través del uso de herramientas para analizar el dominio, página web y direcciones IP proporcionadas por el Instituto, para posteriormente realizar una fase de análisis para detectar y obtener las vulnerabilidades que afectan dichas aplicaciones y servicios, lo cual permitió además conocer el nivel de criticidad de cada vulnerabilidad; con estos datos se pudo ejecutar la fase de explotación de las vulnerabilidades críticas que afectan a dichos servicios. Con la ejecución adecuada de las pruebas de penetración se logró detectar de forma eficiente las vulnerabilidades que afectan a la red de servidores y servicios del Instituto Superior Tecnológico Sucre, lo cual, permitió además, desarrollar un plan de

mejora que contiene las recomendaciones de las acciones que el Instituto Superior Tecnológico Sucre debe implementar para mitigar las vulnerabilidades que afectan a su red y así minimizar los riesgos a los que su infraestructura se encuentra expuesta, garantizando así cumplir con lo dispuesto en la Norma ISO 27001 en cuanto a asegurar en todo momento la integridad, disponibilidad y confidencialidad de la información. (Cedaño,2021)

Borbor Toala (2022), en su investigación “Estudio de la Seguridad Informática a los servidores de una cooperativa de Transporte de la Provincia de Santa Elena, Ecuador 2022”, Este estudio tiene como finalidad el estudio de la seguridad informática en los servidores de una cooperativa de transporte de la provincia de Santa Elena, ya que se considera uno de los activos de información más importantes para dicha empresa, este estudio se centra en la obtención de vulnerabilidades y busca contrarrestar los futuros riesgos a los que pueden estar sometidos a través de la propuesta de soluciones para poner fin a dichas vulnerabilidades. La metodología de investigación diagnóstica es la interpretación de una realidad, por ello expresa y explica las características de su funcionamiento y evolución. La metodología de investigación exploratoria tiene por objeto definir o clarificar conceptos, conocer el problema con mayor profundidad y generar hipótesis o propuestas explicativas relacionadas con el fenómeno objeto de estudio. Con los resultados obtenidos de este análisis podremos establecer medidas de seguridad que nos permitan minimizar riesgos en la operatividad de la organización evitando así la fuga de información sensible lo que puede desencadenar en daños incalculables. (Borbos,2022)

Oscar Cossio (2022)**,** en su estudio “Vulnerabilidades de Ciberseguridad en Sistema de Control Industrial y accesibilidad a través de redes públicas”, el objetivo de este trabajo es obtener información sobre las características y la prevalencia de las principales vulnerabilidades de ciberseguridad en redes de control industrial, sistemas de control industrial, protocolos de comunicación de dispositivos de campo y SCADA., la metodología que se usó fue de tipo experimental como resultado de este trabajo se evidencio que existe un enorme

trabajo a realizar para asegurar que tanto las compañías industriales como los servicios públicos de infraestructura estén protegidos de la mejor manera posible contra el riesgo permanentemente y creciente de brechas de ciberseguridad que vulnera los entornos de control industrial. A pesar de la toma de conciencia y la supuesta preparación por parte de las organizaciones, a menudo son subestimados tanto la fuente como el alcance de estos incidentes. Es esencial que se lleven a cabo los pasos necesarios para identificar los riesgos a los entornos de sistemas de control industriales, con políticas y procesos rigurosos y bien definidos para administrar el riesgo de manera tal que la organización esté en la mejor posición posible para asegurar su tecnología operacional.

2.1.2. Antecedentes Nacionales

Aliaga Yupanqui (2021), en su estudio titulado "Implementación de un Sistema de Ciberseguridad para la prevención de los ataques cibernéticos en la Empresa Radiadores Fortaleza, 2021", se buscó aplicar un sistema de ciberseguridad con el fin de mitigar los ataques cibernéticos en dicha empresa. Este trabajo se enmarca en un estudio de tipo aplicado, con un diseño preexperimental, y tuvo como muestra a 50 empleados de la empresa Radiadores Fortaleza. Los resultados del análisis, reflejados en una diferencia significativa entre las medias del pretest y postest, respaldados por una prueba de Student con un valor de -46.680 y un p valor de 0,000, menor al nivel de significancia establecido ($p<0,05$), llevaron al rechazo de la hipótesis nula (Ho) y la aceptación de la hipótesis general (Ha) planteada en la investigación. La implementación del modelo de ciberseguridad demostró ser efectiva, evidenciando una mejora en la defensa contra ataques informáticos y una reducción en las vulnerabilidades, lo que se tradujo en un mejor desempeño del negocio para la empresa Radiadores Fortaleza (Aliaga, 2021).

Davila Angeles y colaboradores (2021), en su estudio titulado "Propuesta de una Implementación de un programa de Gestión de Vulnerabilidades de Seguridad Informática para mitigar los siniestros de la información en el policlínico de salud

AMC alineado a la NTP-ISO/IEC 27001:2014 en la ciudad de Lima - 2021", se busca implementar un programa de Gestión de Vulnerabilidades con el objetivo de mejorar el nivel de Seguridad Informática en el Policlínico AMC. El enfoque metodológico empleado fue descriptivo, centrado en la recopilación de información de la organización mencionada para fundamentar el estudio. Se privilegiaron las fuentes de información como la documentación y registros de la empresa, entre otros, para orientar la investigación según los hallazgos obtenidos. Como conclusión, se destaca la importancia de diseñar e implementar un programa de Gestión de Vulnerabilidades en el Policlínico AMC como una medida necesaria y efectiva para gestionar adecuadamente las vulnerabilidades en su entorno informático. Los resultados obtenidos señalan la urgencia de abordar las vulnerabilidades de severidad crítica/alta en el menor tiempo posible. Se determinó que la incorporación de controles conforme a la normativa NTP-ISO 27001 garantizará una gestión adecuada de la operación, el control de activos y la gestión de las vulnerabilidades técnicas detectadas, así como la mejora continua del proceso (Davila Angeles et al., 2021).

Huaman Mauricio y colaboradores (2022), en su investigación titulada "Propuesta de implementación de políticas de seguridad basado en CISCO ISE (Identity Services Engine) en la red LAN de Caja Huancayo", se buscó elaborar una propuesta de políticas de seguridad para la Red LAN de Caja Huancayo, basada en la tecnología informática Cisco ISE (Identity Services Engine). Para lograr este objetivo, se empleó una investigación cualitativa de tipo descriptiva. Se aplicó la metodología PPDIOO de Cisco, que comprende las etapas de preparar, planear, diseñar, implementar, operar y optimizar para su respectiva simulación, con el fin de identificar la causa, el problema y el efecto de un riesgo, y así implementar medidas para mitigar amenazas, proteger y asegurar los datos e información. En resumen, se espera reducir los riesgos de accesos no autorizados mediante una simulación con ISE, siempre y cuando se garantice el acceso únicamente a recursos necesarios y se autentifiquen los equipos. Se sugiere el uso de herramientas que faciliten la identificación de posibles amenazas o

vulnerabilidades para corregirlas y prevenir ataques informáticos (Huaman Mauricio et al., 2022).

Avalos Mendoza y colaboradores (2023), en su estudio titulado "Diseño de un modelo de Gestión en Seguridad Digital para la aplicación en entidades peruanas del Sector Público", se propuso diseñar un modelo de Gestión de Seguridad Digital aplicable a las entidades del sector público peruano, con el fin de fortalecer sus capacidades de prevención y respuesta en materia de seguridad digital. Este modelo se basaría en estándares, normativas, mejores prácticas y marcos relacionados con la Seguridad Digital, alineados con la normativa vigente. Para alcanzar este objetivo, se empleó una investigación cualitativa, ya que era necesario examinar el estado actual de las entidades estatales en cuanto a los estándares y marcos de seguridad digital existentes. Basándose en el análisis de los resultados de una encuesta realizada y en fuentes secundarias, se decidió tomar como referencia el marco de ciberseguridad NIST, COBIT, así como el ISO/IEC 27001:2014, como parte del diseño del modelo de gestión de seguridad digital. Este enfoque busca fortalecer las capacidades de prevención y respuesta en materia de seguridad digital en las instituciones públicas peruanas (Avalos Mendoza et al., 2023).

Huara Mere (2019), en su investigación titulada "Gestión de riesgos de seguridad de la información para empresas del sector de las telecomunicaciones", se planteó como objetivo determinar la influencia de la gestión de riesgos de seguridad de la información basada en la norma NTP ISO/IEC 31000 en el control de riesgos en empresas del sector de las telecomunicaciones. Este estudio se enmarca en la investigación no experimental. Como resultado de la investigación, se concluyó que la implementación de una gestión de riesgos de seguridad de la información basada en el estándar internacional NTP ISO/IEC 31000 efectivamente influye en el control de riesgos en las empresas del sector de las telecomunicaciones. Además, este enfoque permite establecer normas para analizar de manera coherente los riesgos, proporcionar indicadores y métricas de gestión que reflejen

el panorama actual de la empresa, y servir como un respaldo continuo para la Alta Dirección (Huara, 2019).

2.2 Bases Teóricas

Son el conocimiento teórico de los problemas que permiten investigarlos a través de la exposición y el análisis de aquellas teorías o enfoques teóricos que se relacionan con el tema de investigación.
Considerando las leyes, principios, y teorías científicas que sirven de base o fundamento para el cuerpo del conocimiento científico del informe final de investigación. (Creswell, 2017).

a) Bases Metodológicas

ISO/IEC 27001:2013

Es una norma internacional que establece los requisitos para un sistema de gestión de seguridad de la información (SGSI).
La ISO/IEC 27001 se centra en la identificación y gestión de los riesgos de seguridad de la información a través de un enfoque basado en riesgos, el ciclo PDCA, un enfoque basado en procesos y controles de seguridad de la información. Esta norma proporciona un marco sólido para establecer, implementar, operar, monitorear, revisar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información en una organización. (ISO/IEC, 2023)

ISO/IEC 27002:2013

La norma ISO/IEC 27002 proporciona un marco completo de controles de seguridad de la información que las organizaciones pueden implementar para proteger sus activos de información y garantizar la confidencialidad, integridad y disponibilidad de la información.

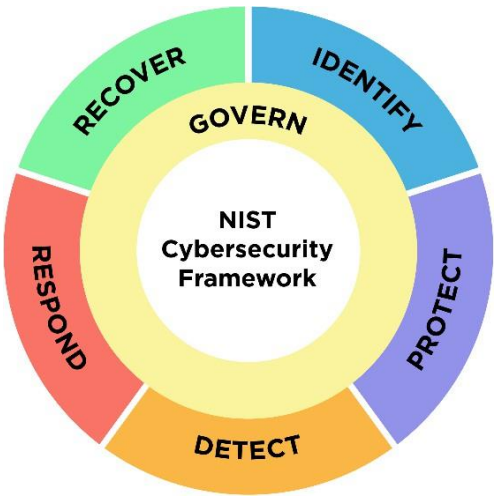
Aborda la protección de los activos de información contra amenazas físicas y ambientales, incluye la gestión de accesos de usuarios, control de contraseñas, autenticación, autorización y control de accesos remotos para garantizar que solo las personas autorizadas tengan acceso a los recursos de información. (ISO/IEC 27002, 2013)

NIST Cybersecurity Framework:

El Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos ha desarrollado el Marco de Ciberseguridad del NIST (NIST Cybersecurity Framework), que proporciona un conjunto de estándares, pautas y mejores prácticas para mejorar la ciberseguridad de las organizaciones.

El marco aborda la ciberseguridad de manera integral, considerando aspectos como la prevención, detección, respuesta y recuperación de incidentes de seguridad. Esto permite a las organizaciones desarrollar una estrategia de ciberseguridad completa que aborde todos los aspectos de la gestión de riesgos de ciberseguridad. (NIST, 2018)

Figura N° 2: *Ciclo NIST Cybersecurity Framework*

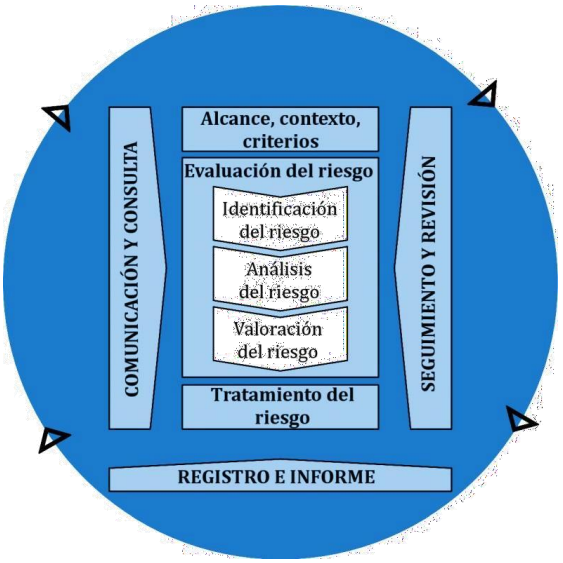


Fuente: NIST Cybersecurity Framework

ISO 31000:2018

Es una norma internacional que establece los principios y directrices para la gestión del riesgo en organizaciones. La norma proporciona un marco para evaluar los riesgos, que incluye la identificación de los riesgos existentes y potenciales, la evaluación de su probabilidad e impacto, y la determinación de las medidas de control apropiadas.

Figura N° 3: *Proceso Gestión de Riesgos*



Fuente: ISO/IEC:2018

b) Bases de la Seguridad de la Información

Esta teoría aborda la protección de la confidencialidad, integridad y disponibilidad de la información en una organización. Examina principios, prácticas y tecnologías para prevenir, detectar y responder a las amenazas a la seguridad. (Whitman & Mattord, 2019).

Gestión de Riesgos en Tecnología de Información

Este enfoque se basa en el análisis sistemático de posibles amenazas y vulnerabilidades, así como en la evaluación de su impacto potencial en los objetivos del negocio. La gestión de Riesgos en Tecnología de Información lica la implementación de procesos y controles para reducir la probabilidad de ocurrencia de eventos adversos y minimizar su impacto en caso de que ocurran (Chapple, 2017).

c) Bases de Gestión de Vulnerabilidades

Este enfoque se apoya en procesos estructurados y metodologías específicas diseñadas para gestionar proactivamente las amenazas a la seguridad de la información, implica la identificación temprana de posibles puntos débiles en los sistemas, la evaluación de su impacto potencial y la implementación de medidas correctivas para reducir o eliminar los riesgos asociados. Este enfoque se basa en el uso de herramientas tecnológicas como escáneres de vulnerabilidades y sistemas de gestión de parches, así como en la integración con otros procesos de seguridad de la información. (Park Foreman, 2019).

2.3 Marco Conceptual

Comprende los principales conceptos en base a los avances o evolución del conocimiento científico-tecnológico y su estado relacionado con el área de investigación. Es obligatoria la presentación y citación de la bibliografía de libros, revistas, papers especializados en el área o tema de investigación. (Wayne Booth, 2008)

Framework Gartner

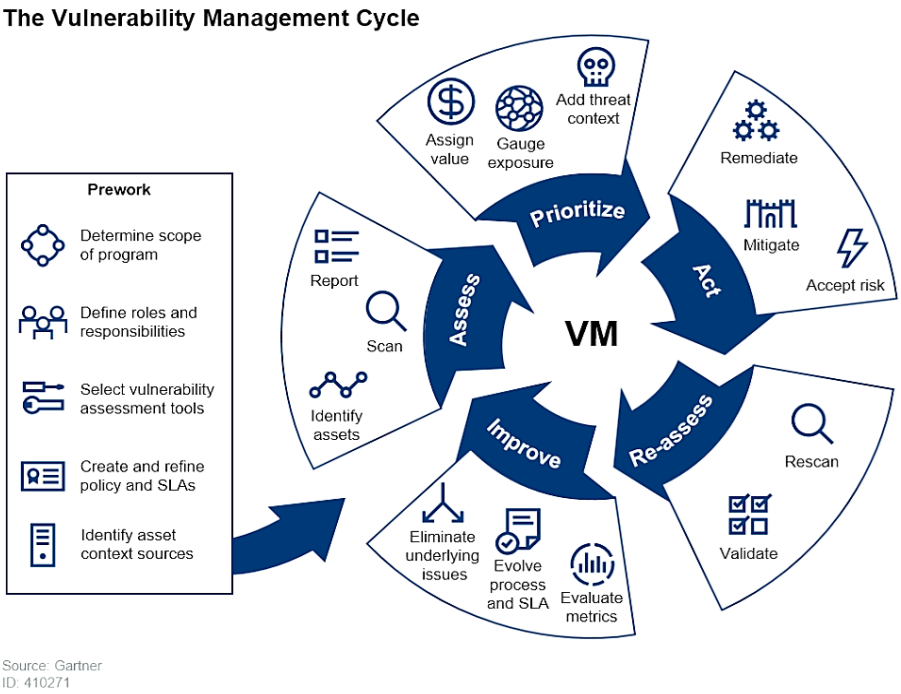
El Framework Gartner proporciona una estructura conceptual sólida que ayuda a las organizaciones a establecer y mantener programas efectivos de gestión de vulnerabilidades. Al seguir este enfoque, las organizaciones pueden mejorar su

capacidad para identificar, priorizar y remediar las vulnerabilidades de manera proactiva, lo que contribuye a fortalecer su postura de seguridad y proteger sus activos críticos de información. (Gartner, 2021)

Ciclo de vida de la Gestión de Vulnerabilidades

El marco de Gartner establece un proceso estructurado que abarca desde la identificación inicial de vulnerabilidades hasta la implementación de medidas correctivas y el seguimiento continuo. Este ciclo de vida ayuda a garantizar que las organizaciones aborden de manera completa y sistemática las amenazas potenciales a la seguridad de sus sistemas. (Gartner, 2021)

Figura N° 4: *Proceso de Gestión de Vulnerabilidades*



Fuente: Framework Gartner

Gestión del Ciclo de Vulnerabilidades

Ciclo o proceso utilizado para administrar y abordar las vulnerabilidades de seguridad en una organización, siguiendo las mejores prácticas recomendadas por Gartner, se mencionan las fases:

a) **Identificación:** Esta fase implica la identificación proactiva de vulnerabilidades en los sistemas y redes de la organización, utilizando herramientas de escaneo de vulnerabilidades, análisis de seguridad y otros métodos de evaluación de vulnerabilidades. (Gartner, 2021)

b) **Priorización:** Una vez identificadas las vulnerabilidades, se deben priorizar según su criticidad y el impacto potencial en la organización. Las vulnerabilidades más críticas y urgentes deben abordarse primero para mitigar los riesgos más importantes. En esta etapa, se realiza un análisis más detallado de las vulnerabilidades identificadas, evaluando su impacto potencial en los activos de información y los sistemas de la organización, así como la probabilidad de explotación y los posibles efectos adversos. (Gartner, 2021)

c) **Remediación:** Basándose en los resultados del análisis de riesgos, se desarrollan y aplican medidas correctivas y soluciones para abordar las vulnerabilidades identificadas, que pueden incluir parches de seguridad, actualizaciones de software, cambios de configuración y otras acciones correctivas. (Gartner, 2021)

d) **Validación:** Una vez implementadas las soluciones de remediación, es importante verificar la efectividad de las medidas correctivas implementadas. Después de aplicar las correcciones o soluciones recomendadas, se vuelve a realizar un escaneo de vulnerabilidades para verificar si las vulnerabilidades identificadas previamente han sido correctamente remediadas. (Gartner, 2021)

e) **Mejora Continua:** La gestión de vulnerabilidades es un proceso continuo y en evolución. Se requiere monitoreo constante, evaluación de nuevas amenazas y actualización de políticas y controles de seguridad para garantizar la protección continua de los activos de información de la organización. (Gartner, 2021)

Integración de Procesos de Tecnología de Información

El marco de Gartner promueve la integración de la gestión de vulnerabilidades con otros procesos de tecnología de la información, como la gestión de cambios, la gestión de configuraciones y la gestión de incidentes. Esta integración ayuda a garantizar una respuesta coherente y coordinada a las vulnerabilidades en toda la organización. (Gartner, 2021)

Automatización y Herramientas Tecnológicas

El framework reconoce la importancia de la automatización y el uso de herramientas tecnológicas para mejorar la eficiencia de la gestión de vulnerabilidades. Esto puede incluir el uso de escáneres de vulnerabilidades, sistemas de gestión de parches y plataformas de inteligencia de amenazas. (Gartner, 2021)

2.4 Definiciones de términos básicos

Según Smith y Jones (2022) define la clarificación de términos como el proceso esencial de establecer y delinear con precisión los significados de los términos utilizados en un estudio particular. Este proceso busca garantizar un consenso común en cuanto a la interpretación y aplicación de estos términos entre los investigadores y lectores.

Vulnerabilidad:

Una vulnerabilidad en el contexto de la seguridad de la información es una debilidad en un sistema, proceso o protocolo que puede ser explotada por una amenaza para comprometer la seguridad de la información. Las vulnerabilidades pueden existir en cualquier aspecto de un sistema, desde el software y hardware hasta los procedimientos operativos. Identificar y mitigar estas vulnerabilidades es crucial para proteger la integridad, confidencialidad y disponibilidad de los activos de información de una organización (Schneider, 2014).

Eficiencia

La eficiencia se refiere a la capacidad de realizar tareas o producir resultados utilizando la menor cantidad de recursos posibles, minimizando el desperdicio y maximizando la producción, implica la mejora continua y la capacidad de adaptación a cambios en el entorno empresarial, asegurando así la sostenibilidad a largo plazo. Las organizaciones eficientes son aquellas que pueden responder rápidamente a las demandas del mercado y ajustarse a nuevas condiciones sin incurrir en costos excesivos ni desperdiciar recursos. Richter (2018),

La eficiencia en la gestión de vulnerabilidades incluye la implementación de procesos automatizados y herramientas de escaneo que permiten a las organizaciones detectar y corregir vulnerabilidades de manera rápida y precisa. El estudio destaca que las empresas eficientes en este ámbito son capaces de reducir significativamente el tiempo de respuesta a las amenazas y disminuir la cantidad de recursos necesarios para gestionar la seguridad. Esto implica optimizar el uso del tiempo, personal, y tecnologías disponibles para minimizar los riesgos de seguridad de manera rentable y efectiva. (Humphreys, 2018)

Eficacia

La eficacia se define como la capacidad de lograr sus objetivos estratégicos y operativos de manera efectiva, utilizando de manera óptima sus recursos

humanos y tecnológicos. Se ve impulsada por la capacidad de adaptación al cambio, la innovación continua y la alineación de los procesos internos con los objetivos de la organización. La eficacia subraya la importancia de la implementación de sistemas de gestión del rendimiento y de la evaluación continua para asegurar que todas las actividades de la organización estén orientadas hacia la consecución de sus metas. (Lopez,2023).

La eficacia en la gestión de vulnerabilidades se refiere a la capacidad de una organización para alcanzar sus objetivos de seguridad, asegurando que las vulnerabilidades sean adecuadamente identificadas, priorizadas y mitigadas para proteger los activos críticos de la organización. La eficacia en este contexto implica no solo la implementación de controles y medidas de seguridad adecuadas, sino también la alineación de las estrategias de seguridad con los objetivos generales de la organización. (Shameli-Sendi, 2018).

Gestión Empresarial

La gestión empresarial se refiere al conjunto de actividades y procesos destinados a dirigir y administrar una empresa para lograr sus objetivos. Esto incluye la planificación estratégica, la toma de decisiones, la asignación de recursos y la supervisión de operaciones. La gestión empresarial abarca áreas como la gestión financiera, la gestión de recursos humanos, la gestión de operaciones y la gestión de marketing (Robbins & Coulter, 2017).

Seguridad de la Información

La seguridad de la información se refiere al conjunto de medidas y controles diseñados para proteger la confidencialidad, integridad y disponibilidad de la información contra amenazas como el acceso no autorizado, la manipulación o la destrucción.

La seguridad de la información involucra la implementación de políticas, procedimientos y tecnologías para proteger los activos de información de una organización (Whitman & Mattord, 2016).

III. HIPÓTESIS Y VARIABLES

3.1 Hipótesis

3.1.1 Hipótesis General

La implementación de un sistema de gestión de vulnerabilidades mejora la productividad en la empresa Contacta Habilidad S.A.C - LIMA en el primer trimestre del año 2024.

3.1.2 Hipótesis Específicas

- La implementación de un sistema de gestión de vulnerabilidades mejora la eficiencia en la empresa Contacta Habilidad S.A.C. - LIMA 2024

- La implementación de un sistema de gestión de vulnerabilidades mejora la eficacia en la empresa Contacta Habilidad S.A.C. - LIMA 2024

3.2 Operacionalización de Variables

3.2.1 Definición conceptual de las variables

Para realizar este trabajo se identificaron dos variables de estudio que sirvieron para conducir la investigación. Se identificó como variable independiente Sistema de Gestión de Vulnerabilidades y como variable dependiente la Productividad.

Sistema de Gestión de Vulnerabilidades

La gestión de vulnerabilidades es el proceso de remediar y encontrar las vulnerabilidades de softwares con el propósito de mantener los riesgos del Sistema de Información en un nivel aceptable. Todos los sistemas y aplicaciones de Tecnología de Información tienen vulnerabilidades. Una vulnerabilidad es una debilidad que permite a un atacante reducir las características fundamentales de los Sistemas de Información. (Dávila, et al, 2021)

De acuerdo con nuestro análisis, sistema de gestión de vulnerabilidades es una herramienta diseñada para identificar, priorizar, remediar, validar y mejora continua de vulnerabilidades, la cual permite automatizar el proceso de encontrar, gestionar y solucionar vulnerabilidades en las aplicaciones e infraestructura con el fin de mantener la integridad, disponibilidad y confidencialidad de los datos y recursos informáticos en una organización.

Productividad

La productividad se define como la relación entre la producción obtenida y los recursos utilizados para obtenerla. En otras palabras, representa la eficiencia con la que se utilizan los recursos para generar resultados tangibles. Esta definición enfatiza la capacidad de una organización para maximizar la producción utilizando la menor cantidad de recursos posibles. La capacidad de una empresa para mantener altos niveles de productividad puede influir significativamente en su posición en el mercado y su capacidad para adaptarse a los cambios en el entorno empresarial. (García et al, 2022)

Para demostrar y comprobar nuestra propuesta de investigación se procedió a operacionalizar las variables, se consideró hacer el estudio de las características o dimensiones, así como sus indicadores correspondientes, partiendo desde lo más general hasta lo más específico, dicha demostración se encuentra en la Tabla N°2.

Tabla N° 2: *Operacionalización de las variables*

Variable	Definición Conceptual	Definición Operacional	Dimensión	Indicador	Escala de Medición
Variable Independiente: Sistema de Gestión de Vulnerabilidades	La gestión de vulnerabilidades es el proceso de remediar y encontrar las vulnerabilidades de softwares con el propósito de mantener los riesgos del Sistema de Información en un nivel aceptable. Todos los sistemas y aplicaciones de Tecnología de Información tienen vulnerabilidades. Una vulnerabilidad es una debilidad que permite a un atacante reducir las características fundamentales de los Sistemas de Información. (Dávila, et al, 2021)	Se define un Sistema de Gestión de Vulnerabilidades es un enfoque integral y sistemático para identificar, clasificar y gestionar las vulnerabilidades en los sistemas de información de una organización. Este enfoque implica la implementación de procesos estructurados para la evaluación continua de las amenazas, la priorización de las vulnerabilidades y la aplicación de controles de seguridad adecuados para mitigar los riesgos asociados (White, et al,2016)	Identificación. Priorización Remediación Validación Mejora Continua	NC== Ejecutado/Planificado	Razón

Variable	Definición Conceptual	Definición Operacional	Dimensión	Indicador	Escala de Medición
Variable Dependiente: Productividad	La productividad se define como la relación entre la producción obtenida y los recursos utilizados para obtenerla. En otras palabras, representa la eficiencia con la que se utilizan los recursos para generar resultados tangibles. Esta definición enfatiza la capacidad de una organización para maximizar la producción utilizando la menor cantidad de recursos posibles. La capacidad de una empresa para mantener altos niveles de productividad puede influir significativamente en su posición en el mercado y su capacidad para adaptarse a los cambios en el entorno empresarial. (García et al, 2022)	Se define la productividad en el ámbito de la ciberseguridad puede entenderse como la eficiencia con la que una organización gestiona y responde a las vulnerabilidades de seguridad en sus sistemas de información. Se relaciona directamente con la capacidad de la organización para mantener un entorno tecnológico seguro y protegido, garantizando al mismo tiempo la continuidad operativa y minimizando los riesgos de incidentes de seguridad. (Aghajani,et al, 2017)	Eficiencia	Eficiencia en la Gestión de Vulnerabilidades: Número de vulnerabilidades remediadas automáticamente / Total de Vulnerabilidades corregidas x 100%	Razón
			Eficacia	Eficacia de vulnerabilidades mitigadas: Número de vulnerabilidades críticas o de alta de severidad mitigadas/ Total de vulnerabilidades críticas o de alta de severidad comprometidas x 100%	

Fuente: Elaboración propia

IV. METODOLOGÍA DEL PROYECTO

4.1 Diseño Metodológico

Tipo de Investigación

Este estudio se categorizó de la siguiente manera:

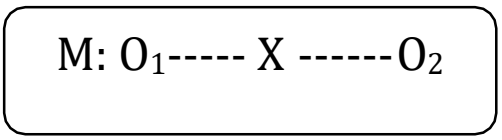
Se trató de un estudio aplicado, ya que su propósito fue investigar, examinar y hallar soluciones a los problemas actuales dentro de la empresa, con el fin de mejorar la productividad empresarial y de esa forma potenciar la competitividad y oportunidades comerciales. En términos de su enfoque en la comprensión orientada al cálculo, se especifica que este estudio adoptó una perspectiva cuantitativa y de nivel explicativo. Esto se debe a que se llevó a cabo un minucioso análisis y recopilación de datos para comprender los pormenores del estudio.

Diseño de la Investigación:

Hernández Sampieri (2014) El diseño Pretest - postest es una estrategia de investigación en la que se realiza una medición inicial de la variable dependiente antes de la aplicación de un tratamiento o intervención (pretest), seguida de una medición posterior después de la implementación del tratamiento. Este diseño permite comparar los niveles de la variable dependiente antes y después del tratamiento para evaluar su efectividad.

El estudio se caracterizó por tener un diseño experimental de tipo pre experimentado que incluye pruebas previas y posteriores. Su propósito radica en la manipulación de una variable independiente particular para examinar su influencia en la variable dependiente "productividad". Este enfoque implica la aplicación de un estímulo tras una prueba inicial en un grupo específico, seguido de una evaluación posterior tras la intervención.

Esto se muestra en el siguiente diagrama:



Donde:

M: Representa la muestra en la que realizamos el estudio.

O_1: N° de observaciones previos al programa educativo (pre- test).

X: Programa educativo (Intervención).

O_2: N° de observaciones post taller (post – test).

4.2 Método de Investigación

El método de esta investigación es deductivo con enfoque cuantitativo.

4.3 Población y Muestra

4.3.1 Población

Según Neuman (2019), la población se refiere al conjunto completo de unidades de análisis que son objeto de estudio en una investigación. Estas unidades pueden ser personas, grupos, organizaciones o cualquier otro tipo de entidad que comparta una característica común y sea relevante para los objetivos de la investigación.

La población objetivo para este estudio comprende el estudio de los activos de tecnología de información de la empresa Contacta Habilidad S.A.C., empresa especializada en brindar soluciones de pago a clientes utilizando herramientas digitales que favorecen la contabilidad.

Esta población incluye tanto los servidores como las aplicaciones utilizadas por la empresa para llevar a cabo sus operaciones comerciales y de gestión.

4.3.2 Muestra de Estudio

Para este estudio, se ha seleccionado una muestra representativa de los activos de Tecnología de la información de la empresa Contacta Habilidad S.A.C.

La muestra es la misma que la población, la cual incluye el estudio de 16 servidores y 6 aplicaciones, de los ambientes de producción y desarrollo, los cuales se consideran críticos para la operación y seguridad de la empresa.

4.4 Lugar de estudio y período desarrollado

El lugar donde se realizó el presente trabajo de investigación fue en la sede principal de la empresa Contacta Habilidad S.A.C., en la Av. Javier Prado Este 228-501, Lima - Perú. El periodo de estudio comprendió el primer trimestre del año 2024.

4.5 Técnicas e Instrumentos de Recolección de Datos

Según Hernández Sampieri (2014): Las técnicas de recolección de datos son procedimientos específicos utilizados por el investigador para obtener información sobre las variables de interés en su estudio. Estas técnicas pueden incluir entrevistas, cuestionarios, observación directa, análisis documental, entre otras.

Para la recolección de datos, se utilizaron técnicas de análisis de vulnerabilidades, que incluyeron escaneos de seguridad y pruebas de penetración. Se emplearon herramientas especializadas de seguridad informática, como escáneres de vulnerabilidades y software de evaluación de seguridad, para identificar y catalogar las vulnerabilidades presentes en los servidores y aplicaciones seleccionadas.

Herramientas de Escaneo Automatizado

Uso de herramientas de escaneo automatizado utilizadas para identificar y analizar vulnerabilidades en los activos de información de la empresa.

a) **Nessus**

   Es una herramienta de escaneo de vulnerabilidades desarrollada por Tenable Network Security. Funciona mediante la realización de escaneos automáticos en la red objetivo y la identificación de vulnerabilidades conocidas en los sistemas y aplicaciones escaneados.

Nessus realiza escaneos automatizados en la red objetivo utilizando una variedad de técnicas de escaneo, como escaneos de puertos, detección de servicios y análisis de vulnerabilidad

b) Qualys

Es una herramienta de escaneo de vulnerabilidades que funciona de manera similar a Nessus. Es una solución basada en la nube que ofrece una amplia gama de funcionalidades de seguridad, lo que significa que los escaneos se ejecutan desde los servidores de Qualys en la nube, esto permite realizar escaneos de manera remota sin necesidad de instalar software adicional en el sistema objetivo.

Pruebas de Penetración

Las pruebas de penetración, también conocidas como pentesting, son una técnica avanzada utilizada para evaluar la seguridad de un sistema informático mediante la simulación de ataques reales. Consisten en intentar descubrir y explotar vulnerabilidades en los sistemas, redes, aplicaciones y otros activos de información de una organización, con el objetivo de identificar áreas de debilidad que podrían ser explotadas por atacantes maliciosos.

a) Caja Negra (Black Box):

En este enfoque, el equipo de pruebas no tiene información previa sobre la infraestructura o el sistema que se está evaluando. Simula un ataque desde la perspectiva de un atacante externo que no tiene conocimiento interno del sistema. Esto permite evaluar la capacidad de detección y respuesta del sistema ante un ataque real.

b) Caja Gris (Gray Box):

En este enfoque, el equipo de pruebas tiene un conocimiento parcial del sistema que se está evaluando. Esto puede incluir información sobre la

arquitectura, la configuración o ciertos aspectos de la infraestructura. La prueba se realiza desde la perspectiva de un atacante interno o un usuario con ciertos privilegios dentro del sistema.

c) Caja Blanca (White Box):

En este enfoque, el equipo de pruebas tiene acceso completo y detallado a la infraestructura y al sistema que se está evaluando. Esto permite una evaluación exhaustiva de la seguridad del sistema, ya que el equipo puede revisar el código fuente, la configuración y otros aspectos internos del sistema. Este enfoque es útil para identificar vulnerabilidades específicas y realizar pruebas de seguridad más profundas.

Fichaje

La técnica de recolección de datos empleada en esta investigación implica registrar y monitorear activamente el comportamiento de las vulnerabilidades en todos los servidores y aplicaciones de la empresa Contacta Habilidad S.A.C. Este software desarrollado funcionó como una herramienta centralizada para registrar y analizar los datos relevantes, proporcionando una visión completa del panorama de seguridad de la empresa facilitando la identificación y priorización de las vulnerabilidades más críticas, así como la implementación de medidas de remediación adecuadas para mitigar los riesgos de seguridad.

4.6 Análisis y procesamiento de datos

En la fase de análisis y procesamiento de datos, se utilizó el software informático SPSS 26 para examinar detalladamente la información recopilada sobre las vulnerabilidades identificadas en los sistemas de la empresa Contacta Habilidad S.A.C.

Las vulnerabilidades encontradas fueron categorizadas según su gravedad y nivel de riesgo, utilizando criterios estándar de la industria de seguridad informática. Esto permitió priorizar las vulnerabilidades más críticas que

representaban una mayor amenaza para la seguridad de los activos de información de la empresa.

Con base en esta priorización, se elaboró un plan de acción integral para la corrección y mitigación de las vulnerabilidades identificadas. Este plan incluyó medidas específicas para abordar cada vulnerabilidad, con el objetivo de fortalecer la seguridad de los sistemas y reducir el riesgo de incidentes de seguridad.

El análisis y procesamiento de datos fueron fundamentales para tomar decisiones informadas y diseñar estrategias efectivas para mejorar la seguridad de la empresa logrando desarrollar los indicadores con éxito.

4.7 Aspectos Éticos en Investigación

Durante el seguimiento y elaboración de la tesis, se mantuvo un compromiso firme con los aspectos éticos en la investigación, en línea con las leyes peruanas de confidencialidad y protección de datos personales, específicamente la Ley N° 29733.

Además, se aseguró el cumplimiento de las normas de seguridad establecidas por la empresa Contacta Habilidad S.A.C., así mismo se siguieron las recomendaciones éticas de seguridad proporcionadas por la universidad considerando el Reglamento General de Investigación de la Universidad Nacional del Callao.

Se garantizó el respeto a la confidencialidad de la información recolectada, conforme a las leyes peruanas vigentes en la materia y la organización. Se protegió la privacidad de los datos de los participantes y se aseguró el consentimiento adecuado cuando correspondía. Se promovió la transparencia y la integridad en el manejo de los datos, así como la honestidad en la presentación de los resultados, cumpliendo con los estándares éticos y legales requeridos.

V. RESULTADOS

La combinación de una reducción en el número de vulnerabilidades, una mejor priorización y resolución más rápida de las mismas, junto con el cumplimiento normativo y la reducción de riesgos, respaldan la efectividad de la implementación de un sistema de Gestión de Vulnerabilidades en proteger los activos de información de la organización.

5.1 Resultados Descriptivos

Con la implementación del Sistema de Gestión de Vulnerabilidades, se ha logrado una notable mejora en la identificación y gestión de las vulnerabilidades en el sistema. Esto se evidencia claramente en los datos recopilados durante el período de prueba y después de la implementación.

Este notable cambio puede atribuirse a la mayor visibilidad proporcionada por el Sistema de Gestión de Vulnerabilidades, que integra herramientas de escaneo especializadas. Estas herramientas permiten una identificación más exhaustiva de las vulnerabilidades, lo que a su vez facilita la priorización de su atención y mitigación.

Tabla N° 3: *Resultados de Identificación de Vulnerabilidades*

PRE-TEST		**POST-TEST**	
Tiempo	Total de Vulnerabilidades	Tiempo	Total de Vulnerabilidades
OCT 2023	354	ENE 2024	1190
NOV 2023	471	FEB 2024	681
DIC 2023	492	MAR 2024	475
Sumatoria	1371	TOTAL	2346

Fuente: Elaboración propia

Tabla N° 4: *Porcentaje Resolución de Vulnerabilidades Mitigadas*

TOTAL DE VULNERABILIDADES MITIGADAS				
Tiempo / Activos	*Aplicaciones*		*Servidores*	
	N.º Vulnerabilidades	*% Resolución de Vulnerabilidades Mitigadas*	*N.º Vulnerabilidades*	*% Resolución de Vulnerabilidades Mitigadas*
oct-23	*48*	*0%*	*306*	*5%*
nov-23	*53*	*8%*	*418*	*14%*
dic-23	*55*	*8%*	*437*	*14%*
ene-24	*265*	*48%*	*925*	*60%*
feb-24	*128*	*70%*	*553*	*70%*
mar-24	*91*	*80%*	*384*	*80%*

Fuente: Elaboración propia

Tabla N° 5: *Resultados de Identificación de Vulnerabilidades*

Etiquetas de fila	Criticidad BAJO	Criticidad MEDIO	Criticidad ALTO	Criticidad CRÍTICO
2023	**376**	**305**	**320**	**316**
Trim.4	**376**	**305**	**320**	**316**
oct	104	85	88	77
nov	143	106	112	110
dic	129	114	120	129
2024	**744**	**562**	**527**	**513**
Trim.1	**744**	**562**	**527**	**513**
ene	395	310	260	225
feb	195	159	163	164

mar	154	93	104	124
Total general	**1120**	**867**	**847**	**829**

Fuente: Elaboración propia

Este resultado demuestra que la adopción de esta solución tecnológica no solo ha permitido identificar las vulnerabilidades de manera más efectiva, sino que también ha facilitado su mitigación de forma automatizada, eliminando la necesidad de realizar procesos manuales que consumen tiempo y recursos. Además, se observó un aumento significativo en el porcentaje de resolución de vulnerabilidades, un mayor porcentaje de resolución indica una reducción en la exposición a riesgos de seguridad y una mayor protección para la organización y sus activos digitales.

a) Resultados de Productividad

Tabla N° 6: *Resultados de Productividad Post-Test y Post-Test*

PRE-TEST		**POST-TEST**	
Tiempo	% Productividad	Tiempo	% Productividad
OCT 2023	0.71 %	ENE 2024	83.23 %
NOV 2023	2.11 %	FEB 2024	72.34 %
DIC 2023	2.36 %	MAR 2024	77.99 %
PROMEDIO	1.72 %	TOTAL	77.85 %

Fuente: Elaboración propia

La mejora del 76.13% en la productividad entre el pre-test y el post-test indica un progreso significativo en la capacidad de la empresa para gestionar las vulnerabilidades después de la implementación del sistema de gestión de vulnerabilidades. Este aumento considerable sugiere que el sistema ha tenido

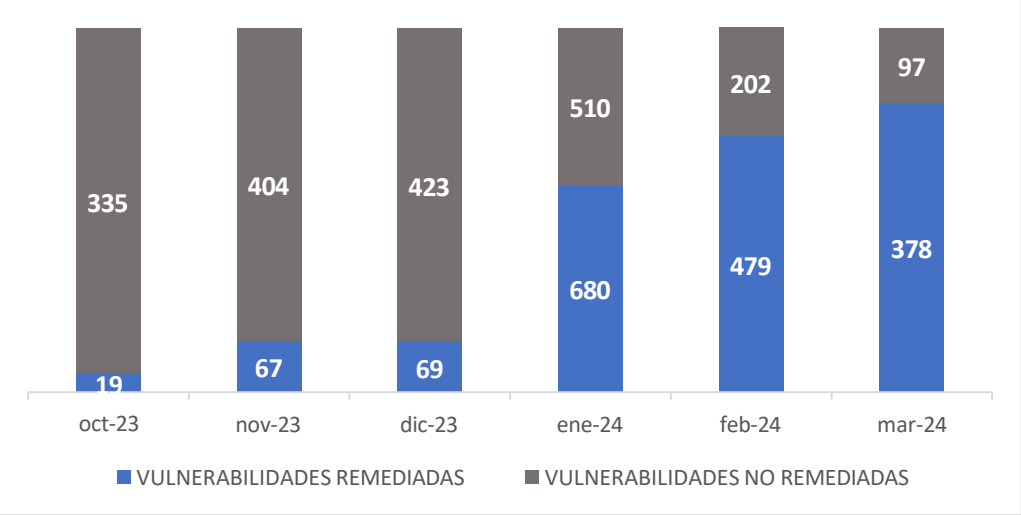
un impacto positivo en la eficiencia y eficacia de la gestión de vulnerabilidades en la empresa.

b) Resultados de la Eficiencia en la gestión de vulnerabilidades

Este indicador evalúa la capacidad de la empresa para gestionar eficientemente las vulnerabilidades identificadas calculando el porcentaje de vulnerabilidades que se han corregido de manera automática, sin necesidad de intervención manual del personal de seguridad. Un mayor porcentaje de corrección automática indica una mayor eficiencia y ahorro de esfuerzo del personal.

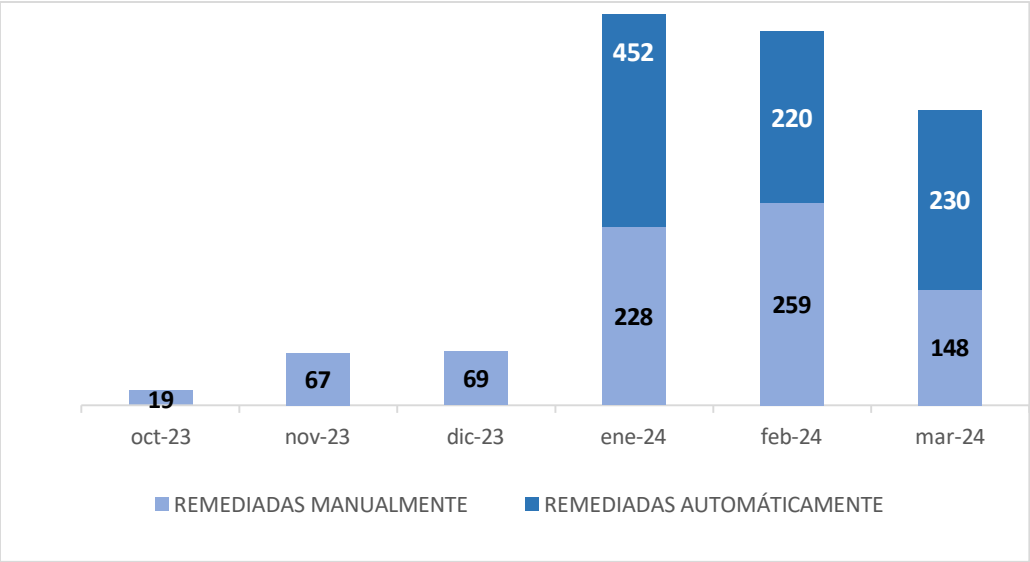
$$Eficiencia = \frac{\textbf{Número de vulnerabilidades remediadas automáticamente}}{\textbf{Total de Vulnerabilidades corregidas}} \times 100\%$$

Figura N°5: Diagrama de Vulnerabilidades Remediadas vs Vulnerabilidades no Remediadas



Fuente: Elaboración propia

Figura N°6: *Diagrama de Vulnerabilidades Remediadas Manualmente vs Vulnerabilidades Automáticamente*



Fuente: Elaboración propia

Tabla N° 7: *Resultados de Eficiencia Post-Test y Post-Test*

PRE-TEST		POST-TEST	
Tiempo	% Eficiencia	Tiempo	% Eficiencia
OCT 2023	5%	**ENE 2024**	66.47%
NOV 2023	11.5%	**FEB 2024**	45.92%
DIC 2023	10%	**MAR 2024**	60.84%
PROMEDIO	8.83%	TOTAL	57.74%

Fuente: Elaboración propia

Se observa una mejora significativa en la eficiencia después de la implementación del Sistema de Gestión de Vulnerabilidades. Antes de la implementación, en el pretest, se registró un porcentaje de eficiencia del 8.83 % en todos los meses. Sin embargo, después de la implementación, en el postest, se observa un aumento notable en la eficiencia del 48.91%.

En promedio general de eficiencia en el postest es del 57.74%, lo que indica una mejora significativa en el tiempo empleado para abordar las vulnerabilidades.

c) Eficacia de vulnerabilidades mitigadas

Este indicador calcula el porcentaje de vulnerabilidades comprometidas que se han mitigado con éxito. Un mayor porcentaje de mitigación indica una mayor eficacia en la gestión de vulnerabilidades comprometidas y una reducción en el riesgo para la empresa, lo que contribuye a una mayor productividad y ahorro de costos al evitar posibles incidentes de seguridad.

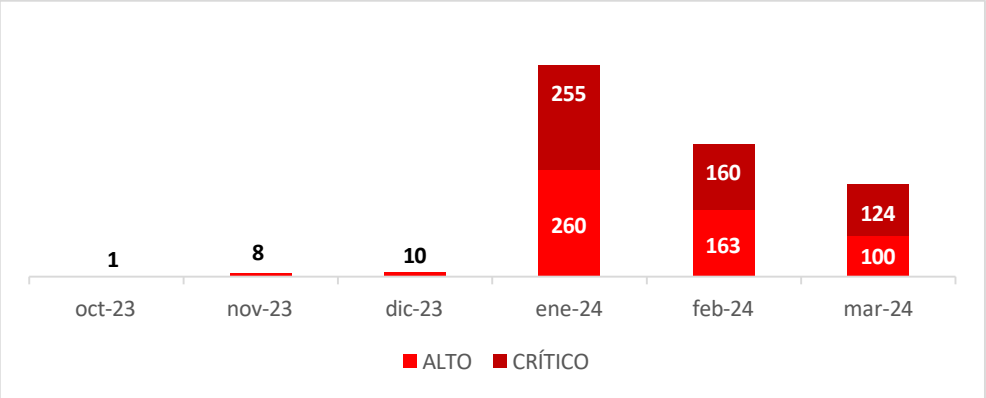
$$Eficacia = \frac{\textbf{Número de vulnerabilidades críticas y de alta de severidad mitigadas}}{\textbf{Total de vulnerabilidades críticas y de alta severidad comprometidas}} \times 100\%$$

Tabla N° 8: *Vulnerabilidades Mitigadas*

	VULNERABILIDADES REMEDIADAS DE SERVIDORES Y APLICACIONES					
CRITICIDAD	oct-23	nov-23	dic-23	ene-24	feb-24	mar-24
BAJO	15	43	34	2	12	44
MEDIO	2	16	25	163	144	90
ALTO	1	8	10	260	163	100
CRÍTICO	1	0	0	255	160	124

Fuente: Elaboración propia

Gráfico N°3: *Diagrama de vulnerabilidades altas y críticas mitigadas*



Fuente: Elaboración propia

Tabla N° 9: *Resultados de Eficacia Post-Test y Post-Test*

PRE-TEST		POST-TEST	
Tiempo	% Eficacia	Tiempo	% Eficacia
OCT 2023	1.42 %	**ENE 2024**	100 %
NOV 2023	4.23 %	**FEB 2024**	98.77 %
DIC 2023	4.72 %	**MAR 2024**	98.24 %
PROMEDIO	3.45 %	TOTAL	99 %

Fuente: Elaboración propia

Se observa una mejora significativa en la eficacia en la mitigación de vulnerabilidades altas y críticas después de la implementación del Sistema de Gestión de Vulnerabilidades. Antes de la implementación, en el pretest, se registró un porcentaje de eficacia del 3.45 % como resultado del último trimestre del 2023. Sin embargo, después de la implementación, en el postest se tiene un promedio de eficacia postest del 99%, se observa un aumento notable en la eficacia del 95.55% de vulnerabilidades altas y críticas mitigadas con respecto al compromiso del 100%.

5.2 Resultados Inferenciales

5.2.1 Resultados Inferenciales primera Hipótesis de la Variable Dependiente

Prueba de Normalidad de Variable Dependiente

En el estudio de la investigación, se optó por la prueba de normalidad de Shapiro-Wilk a causa de que el ejemplar utilizado consta menos 50 datos. Esta prueba se aplicó para evaluar las hipótesis relacionadas con la productividad, centrándose en las diferencias:

Si el valor de p (nivel de significancia) es mayor que 0.05, los datos de la notificación derivan de un suministro normal, en cuya contingencia se admite Ho.

Si el valor de p (nivel de significancia) es menor 0.05, los datos de la notificación en absoluto no proceden de un suministro normal, se admite Ha.

Tabla N° 10: *Prueba de Normalidad Variable Dependiente*

Pruebas de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Diferencia Producción	0,199	3	0	0,995	3	0,867

Fuente: Elaboración Propia

Disquisición:

De acuerdo con lo que se puede apreciar en la Tabla N°9, el valor de p obtenido mediante la muestra de significativa muestra un resultado de 0.867 el cual es mayor que 0.05. El presente resultado sugiere que los datos sometidos a esta prueba siguen una distribución normal, consolidando así la idea de que estos datos se ajustan a un perfil paramétrico. Este hallazgo refuerza la validez del enfoque estadístico empleado, confirmando que los supuestos asociados con la distribución paramétrica se cumplen de manera satisfactoria.

En lo que respecta al análisis inferencial:

Sig. (nivel de significancia) < 0.05 son datos no paramétricos, se utiliza el test Wilcoxon

Sig. (nivel de significancia) > 0.05 son datos paramétricos, se utiliza el test de T-Student

Se concluye que utilizamos T-Student por ser datos paramétricos

Validación de la primera Hipótesis de la Variable Dependiente

La implementación de un sistema de gestión de vulnerabilidades mejora la productividad en la empresa Contacta Habilidad S.A.C - LIMA en el primer trimestre del año 2024.

Ha: Hipótesis alterna.
Ho: Hipótesis nula.

Ha: La implementación de un sistema de gestión de vulnerabilidades mejora la productividad en la empresa Contacta Habilidad S.A.C - LIMA en el primer trimestre del año 2024.

Ho: La implementación de un sistema de gestión de vulnerabilidades **no** mejora la productividad en la empresa Contacta Habilidad S.A.C - LIMA en el primer trimestre del año 2024.

E= 0.05 (nivel de significancia)

Entonces, estadísticamente se halló que el p < 0.05

Si **p<0.05**, se rechaza la hipótesis nula, se acepte la hipótesis alterna

Si **p> 0.05** se acepta la hipótesis nula, se rechaza la hipótesis alterna

Tabla N° 11: *Estadísticas de Muestras Emparejadas - Productividad*

Estadísticas de muestras emparejadas					
		Media	N	Desv. Desviación	Desv. Error promedio
Par 1	Productividad Después	77,8533	3	5,44629	3,14441
	Productividad antes	1,7267	3	0,88929	0,51343

Fuente: Elaboración propia

Tabla N° 12: *Comparación pre y post muestra del Sistema de Gestión de vulnerabilidades para mejorar la productividad*

Prueba de muestras emparejadas									
		Diferencias emparejadas					t	gl	Sig. (bilateral)
		Media	Desv. Desviación	Desv. Error promedio	95% de intervalo de confianza de la diferencia				
					Inferior	Superior			
Par 1	Productividad Después - Productividad antes	76,12667	6,16004	3,55650	60,82429	91,42904	21,405	2	0,002

Fuente: Elaboración propia

Como p **0.002<0.05**, se rechaza la hipótesis nula, se acepta la hipótesis alterna

Ha: La implementación de un sistema de gestión de vulnerabilidades mejora la productividad en la empresa Contacta Habilidad S.A.C - LIMA en el primer trimestre del año 2024.

5.2.2 Resultades inferenciales de la primera Hipótesis especifica – Índice de Eficiencia

Prueba de Normalidad de la primera Hipótesis Especifica – Índice de Eficiencia

En el estudio de la investigación, se optó por la prueba de normalidad de Shapiro-Wilk a causa de que el ejemplar utilizado consta menos 50 datos. Esta prueba se aplicó para evaluar las hipótesis relacionadas con la productividad, centrándose en las diferencias:

Si el valor de p (nivel de significancia) es mayor que 0.05, los datos de la notificación derivan de un suministro normal, en cuya contingencia se admite Ho.

Si el valor de p (nivel de significancia) es menor 0.05, los datos de la notificación en absoluto no proceden de un suministro normal, se admite Ha.

Tabla N° 13: *Prueba de Normalidad de los índices de eficiencia*

Pruebas de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Diferencia Eficiencia	0,223	3	0	0,985	3	0,765

Fuente: Elaboración propia

Disquisición:

De acuerdo con lo que se puede apreciar en la Tabla N°12, el valor de p obtenido mediante la muestra de significativa muestra un resultado de 0.765 el cual es mayor que 0.05. El presente resultado sugiere que los datos sometidos a esta prueba siguen una distribución normal, consolidando así la idea de que estos datos se ajustan a un perfil paramétrico. Este hallazgo refuerza la validez del enfoque estadístico empleado, confirmando que los supuestos asociados con la distribución paramétrica se cumplen de manera satisfactoria.

En lo que respecta al análisis inferencial:

Sig. (nivel de significancia) < 0.05 son datos no paramétricos, se utiliza el test Wilcoxon

Sig. (nivel de significancia) > 0.05 son datos paramétricos, se utiliza el test de T-Student

Se concluye que utilizamos T-Student por ser datos paramétricos

Validación de la primera Hipótesis Especifica – Índice de Eficiencia

La implementación de un sistema de gestión de vulnerabilidades mejora la eficiencia en la empresa Contacta Habilidad S.A.C. - LIMA 2024.

Ha: Hipótesis alterna.
Ho: Hipótesis nula.

Ha: La implementación de un sistema de gestión de vulnerabilidades mejora la eficiencia en la empresa Contacta Habilidad S.A.C. - LIMA 2024.
Ho: La implementación de un sistema de gestión de vulnerabilidades no mejora la eficiencia en la empresa Contacta Habilidad S.A.C. - LIMA 2024.

E= 0.05 (nivel de significancia)
Entonces, estadísticamente vamos a hallar el p (nivel de significancia o SIG)
Si **p<0.05**, se rechaza la hipótesis nula, se acepte la hipótesis alterna
Si **p> 0.05** se acepta la hipótesis nula, se rechaza la hipótesis alterna

Tabla N° 14: *Estadísticas de muestras emparejadas – Eficiencia*

Estadísticas de muestras emparejadas					
		Media	N	Desv. Desviación	Desv. Error promedio
Par 1	Eficiencia después	57,7433	3	10,61921	6,13100
	Eficiencia antes	8,8333	3	3,40343	1,96497

Fuente: Elaboración propia

Tabla N° 15: *Comparación pre y post muestra de la implementación del Sistema de gestión de vulnerabilidades sobre el indicador Eficiencia*

Prueba de muestras emparejadas									
		Diferencias emparejadas					t	gl	Sig. (bilateral)
		Media	Desv. Desviación	Desv. Error promedio	95% de intervalo de confianza de la diferencia				
					Inferior	Superior			
Par 1	Productividad Después - Productividad antes	48,9100	13,62789	7,86806	15,05645	82,76355	6,216	2	0,025

Fuente: Elaboración propia

Como **p 0.025<0.05**, se rechaza la hipótesis nula, se acepte la hipótesis alterna

Ha: La implementación de un sistema de gestión de vulnerabilidades mejora la eficiencia en la empresa Contacta Habilidad S.A.C. - LIMA 2024.

5.2.3 Resultades inferenciales de la Segunda Hipótesis especifica – Índice de Eficacia

Prueba de Normalidad de la segunda Hipótesis Especifica – Índice de Eficacia

En el estudio de la investigación, se optó por la prueba de normalidad de Shapiro-Wilk a causa de que el ejemplar utilizado consta menos 50 datos. Esta prueba se aplicó para evaluar las hipótesis relacionadas con la productividad, centrándose en las diferencias:

Si el valor de p (nivel de significancia) es mayor que 0.05, los datos de la notificación derivan de un suministro normal, en cuya contingencia se admite Ho.

Si el valor de p (nivel de significancia) es menor 0.05, los datos de la notificación en absoluto no proceden de un suministro normal, se admite Ha.

Tabla N° 16: *Prueba de Normalidad de los índices de eficacia*

Pruebas de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Diferencia Eficacia	0,313	3	0	0,894	3	0,366

Fuente: Elaboración propia

Disquisición:

De acuerdo con lo que se puede apreciar en la Tabla N°15, el valor de p obtenido mediante la muestra de significativa muestra un resultado de 0.366 el cual es mayor que 0.05. El presente resultado sugiere que los datos sometidos a esta prueba siguen una distribución normal, consolidando así la idea de que estos datos se ajustan a un perfil paramétrico. Este hallazgo refuerza la validez del enfoque estadístico empleado, confirmando que los supuestos asociados con la distribución paramétrica se cumplen de manera satisfactoria.

En lo que respecta al análisis inferencial:

Sig. (nivel de significancia) < 0.05 son datos no paramétricos, se utiliza el test Wilcoxon

Sig. (nivel de significancia) > 0.05 son datos paramétricos, se utiliza el test de T-Student

Se concluye que utilizamos T-Student por ser datos paramétricos

Validación de la segunda Hipótesis Especifica – Índice de Eficacia

La implementación de un sistema de gestión de vulnerabilidades mejora la eficacia en la empresa Contacta Habilidad S.A.C. - LIMA 2024.

Ha: Hipótesis alterna.
Ho: Hipótesis nula.

Ha: La implementación de un sistema de gestión de vulnerabilidades mejora la eficacia en la empresa Contacta Habilidad S.A.C. - LIMA 2024.

Ho: La implementación de un sistema de gestión de vulnerabilidades no mejora la eficacia en la empresa Contacta Habilidad S.A.C. - LIMA 2024.

E= 0.05 (nivel de significancia)

Entonces, estadísticamente vamos a hallar el p (nivel de significancia o SIG)

Si **p<0.05**, se rechaza la hipótesis nula, se acepte la hipótesis alterna

Si **p> 0.05** se acepta la hipótesis nula, se rechaza la hipótesis alterna

Tabla N° 17: *Estadísticas de muestras emparejadas – Eficacia*

Estadísticas de muestras emparejadas					
		Media	N	Desv. Desviación	Desv. Error promedio
Par 1	Eficacia desp	99,0033	3	,90290	,52129
	Eficacia antes	3,4567	3	1,78074	1,02811

Fuente: Elaboración propia

Tabla N° 18: *Comparación pre y post muestra de la implementación del sistema de gestión de vulnerabilidades sobre el indicador de Eficacia*

Prueba de muestras emparejadas									
		Diferencias emparejadas					t	gl	Sig. (bilateral)
		Media	Desv. Desviación	Desv. Error promedio	95% de intervalo de confianza de la diferencia				
					Inferior	Superior			
Par 1	Eficacia después Eficacia antes	95,54667	2,67599	1,54498	88,89913	102,19420	61,843	2	0,000

Fuente: Elaboración propia

Como p **0.00<0.05**, se rechaza la hipótesis nula, se acepte la hipótesis alterna

Ha: La implementación de un sistema de gestión de vulnerabilidades mejora la eficacia en la empresa Contacta Habilidad S.A.C. - LIMA 2024.

VI. DISCUSIÓN DE RESULTADOS

6.1 Contrastación y demostración de la hipótesis con los resultados

a) Al contrastar y demostrar la variable dependiente, es decir, la productividad, se puede observar en la tabla N°12 resultados con un valor de significancia de 0.002, por debajo del umbral establecido de 0.05 por lo tanto, se declina la Ho y se valida Ha.

   Esta diferencia estadísticamente significativa en la productividad antes y después de la implementación del Sistema de Gestión de Vulnerabilidades indica un cambio positivo y notable en el rendimiento de la empresa. El incremento del 76.12% en la productividad post-implementación refleja la eficacia de este sistema en mejorar la eficiencia y la efectividad operativa de la organización, lo que se traduce en un impacto significativo en su desempeño general y su capacidad para alcanzar sus objetivos estratégicos.

b) Al contrastar y demostrar la dimensión de la eficiencia, se examinaron los resultados presentados en la Tabla N°15. Aquí, el valor de significancia obtenido es de 0.025, por debajo del nivel de significancia establecido.

   Esto indica que la hipótesis nula ha sido rechazada, confirmando que ha habido un cambio significativo en la eficiencia después de la implementación del Sistema de Gestión de Vulnerabilidades. El incremento del 48.91% en el índice de eficiencia subraya el impacto positivo de esta implementación en la capacidad de la empresa para utilizar sus recursos de manera más efectiva.

c) Al contrastar y demostrar la dimensión de eficacia al consultar la Tabla N°18, se observa que el valor de significancia obtenido es 0.000, situándose por debajo de 0.05. Por lo tanto, se rechaza la hipótesis nula y se valida la alternativa.

   Este hallazgo refleja una mejora significativa en la media del índice de eficacia, que ha experimentado un aumento del 95.54%. Por lo tanto, se

puede afirmar que existe una diferencia estadísticamente significativa en la productividad. La implementación del Sistema de Gestión de Vulnerabilidades para mejorar la eficacia en la empresa Contacta Habilidad S.A.C. - 2024, resulta en un marcado aumento del 95.54% en el índice de eficacia.

6.2 Contrastación de los resultados con estudios similares

En la tesis de Aliaga Yupanqui, “Implementación de un Sistema de Ciberseguridad para la prevención de los ataques cibernéticos en la Empresa Radiadores Fortaleza, 2021” se implementó un sistema de ciberseguridad que influyó de manera positiva en la prevención ataques cibernéticos en la mencionada empresa y se mejoró notablemente la defensa de los ataques informáticos y se disminuyó las vulnerabilidades la cual conllevo a un mejor desempeño del negocio. Nuestra investigación se centra en la implementación de un Sistema de Gestión de Vulnerabilidades, lo que resultó en una mejora notable del 76.12 % en la productividad y un alto nivel de aceptación post propuesta.

En la tesis de Davila Angeles y otros, “Propuesta de una Implementación de un programa de Gestión de Vulnerabilidades de Seguridad Informática para mitigar los siniestros de la información en el policlínico de salud AMC alineado a la NTP-ISO/IEC 27001:2014 en la ciudad de Lima – 2021”, se determinó que la implementación de este programa de gestión garantizará la correcta gestión de la Operación, control de activos y Gestión de las Vulnerabilidades técnicas detectadas y mejora continua del proceso. De forma similar, en nuestra investigación, se asegura una gestión adecuada, respaldada por resultados de pretest y post test que evidencian una eficacia del 95.54%. En resumen, mientras que estas tesis abordan diferentes enfoques y contextos, todas comparten el objetivo común de mejorar la seguridad informática y la gestión de vulnerabilidades en sus respectivas organizaciones.

En la tesis de Huaman Mauricio y otros “Propuesta de implementación de políticas de seguridad basado en CISCO ISE (identity services engine) en la red

LAN de Caja Huancayo cuyo objetivo es elaborar una propuesta de implementación de políticas de seguridad para la Red LAN de Caja Huancayo, basado en la tecnología informática Cisco ISE (Identity Services Engine).” En contraste con la propuesta de implementación de políticas de seguridad, nuestro enfoque se centra en mejorar la productividad mediante la implementación de un sistema de gestión de vulnerabilidades. Mientras que el estudio de Huaman Mauricio y otros se enfoca en atenuar los riesgos de accesos no autorizados mediante la simulación con ISE y la autenticación de equipos, nuestra investigación se dirige hacia la identificación y mitigación automatizada de vulnerabilidades.

Nuestro trabajo busca optimizar la eficiencia y la eficacia al gestionar las vulnerabilidades existentes, lo que se traduce en una reducción de los riesgos de pérdida de información y en una mejora continua de la seguridad informática. Al automatizar la mitigación de vulnerabilidades y garantizar una gestión más efectiva de los recursos necesarios, nuestra propuesta se alinea con el objetivo de incrementar la seguridad de la información y mantener un entorno de red seguro y protegido.

En la tesis de Avalos Mendoza y otros, en su estudio “Diseño de un modelo de Gestión en Seguridad Digital para la aplicación en entidades peruanas del Sector Público” examinó el estado actual de las entidades estatales con respecto a los estándares y marcos de seguridad digital existentes basándose en el análisis de los resultados de la encuesta realizada, así como en fuentes secundarias, el estudio decidió tomar como base al marco de ciberseguridad NIST, COBIT, así como el ISO/IEC 27001:2014, como parte del diseño del modelo de gestión de seguridad digital para la aplicación en entidades peruanas del sector público que permitió fortalecer las capacidades de prevención y respuesta en materia de seguridad digital en las instituciones públicas peruana. Nuestro enfoque estuvo dirigido hacia la mejora de la productividad mediante la implementación de dicho sistema, logrando un aumento del 76.12 % y un alto nivel de aceptación post propuesta.

Ambos estudios comparten la meta de fortalecer las capacidades de prevención y respuesta en seguridad digital, aunque lo hacen desde enfoques y estrategias diferentes. Mientras que Avalos Mendoza y su equipo se centraron en el diseño de un modelo de gestión, nuestra investigación se enfocó en la aplicación práctica de un Sistema de Gestión de Vulnerabilidades para obtener mejoras concretas en la productividad.

6.3 Responsabilidad ética

Este estudio ha sido desarrollado en estricta conformidad con las normativas y directrices tanto a nivel nacional como internacional, así como los estándares establecidos por la Universidad Nacional del Callao.

Para garantizar la integridad y fiabilidad de los resultados, se ha seguido un riguroso proceso metodológico, desde la recolección de datos hasta su análisis. Se ha prestado especial atención al respeto de los códigos de ética, asegurando que no se hayan realizado distorsiones ni alteraciones en los datos presentados. Los datos recopilados se sustentan en los resultados obtenidos mediante la aplicación del Pre-Test y Post-Test, los cuales fueron procesados utilizando el software SPSS 26, siguiendo prácticas estándar de análisis estadístico.

Además, se ha garantizado en todo momento el nivel de confidencialidad requerido por la empresa involucrada en este análisis, asegurando la protección de la información sensible y la privacidad de los participantes.

VII. CONCLUSIONES

De acuerdo con los resultados obtenidos en el trabajo de investigación se llegó a las siguientes conclusiones:

- La implementación de un Sistema de Gestión de Vulnerabilidades ha demostrado ser una estrategia efectiva para mejorar la productividad en la empresa Contacta Habilidad S.A.C. Esta conclusión se fundamenta en los resultados obtenidos, que indican que dicho sistema ha optimizado la identificación, gestión y remediación de vulnerabilidades en los activos informáticos de la organización. La mejora en la productividad se evidencia en un aumento del 76,13% en la eficiencia operacional y la eficacia en el manejo de las vulnerabilidades.

- Se demostró una mejora sustancial en la eficiencia operativa de la empresa, se reflejó en una significativa reducción en los tiempos de remediación de vulnerabilidades, así como en un aumento en la identificación efectiva de estas. Como resultado, se logró una mejora del 48.91% en el índice de eficiencia de la empresa. Este incremento en la eficiencia operativa fue efectiva para optimizar los procesos de seguridad de la empresa y mejorar su capacidad para enfrentar las nuevas vulnerabilidades en ciberseguridad.

- Se concluyó que la implementación del sistema de Gestión de Vulnerabilidades mejoró significativamente la eficacia en la mitigación de vulnerabilidades en Contacta Habilidad S.A.C. Esta mejora se reflejó en un aumento del 95.55% en el índice de eficacia, lo que indica un mayor compromiso y éxito en la mitigación de vulnerabilidades. Además, el cumplimiento del Benchmarking de ciberseguridad sugiere que la empresa ha alcanzado estándares de desempeño en la gestión de vulnerabilidades, lo que fortalece aún más su postura de seguridad.

VIII. RECOMENDACIONES

- Es fundamental centralizar todas las vulnerabilidades identificadas en un repositorio único y establecer un proceso claro y estructurado para su gestión. Esto incluye la clasificación, priorización y asignación de responsabilidades para la mitigación de cada vulnerabilidad. La centralización y gestión eficiente de las vulnerabilidades facilitará la coordinación entre los equipos de seguridad y TI, garantizando una respuesta más rápida y efectiva.

- Se sugiere investigar y evaluar software de identificación de vulnerabilidades más avanzado y especializado. Estas herramientas pueden ofrecer capacidades avanzadas de detección, análisis y correlación de amenazas, permitiendo una identificación más precisa y exhaustiva de vulnerabilidades en los sistemas de la empresa. Además, algunas soluciones pueden integrar inteligencia de amenazas y análisis de riesgos permitiendo descartar falsos positivos.

- Se recomienda enfocarse en la automatización de los procesos de mitigación de vulnerabilidades La automatización puede agilizar significativamente la respuesta a las vulnerabilidades al permitir la implementación rápida de parches, la configuración de reglas de seguridad y la aplicación de medidas correctivas de manera programada y sistemática. Esto no solo reduce el tiempo de respuesta, sino que también minimiza el riesgo de errores humanos y garantiza una respuesta consistente y eficiente ante las amenazas.

IX. REFERENCIAS BIBLIOGRÁFICAS

Catuto Pilar. (2021). Análisis de amenazas y vulnerabilidades informáticas basado en la Norma ISO 27002, en el proceso de citas del servidor web de una Institución Santa Elena. Tesis de pregrado, Universidad Estatal Peninsula de Santa Elena, 2021.

Cuesta Morante. (2019). Análisis de Amenazas y Vulnerabilidades dentro del Sistema de Gestión del Voluntariado en la Cruz Roja ubicada en la Ciudad de Babahoyo, Ecuador. Tesis de pregrado, Universidad Técnica de Ambato.

Cedeño Zambrano. (2021). Detección de vulnerabilidades mediante pruebas de penetración a la red de servidores y servicios del Instituto Superior Tecnológico Sucre Cohorte, 2021. Tesis de pregrado, Universidad Estatal Península de Santa Elena .

Borbor Toala. (2022). Estudio de la Seguridad Informática a los servidores de una cooperativa de Transporte de la Provincia de Santa Elena, Ecuador 2022. Tesis de pregrado,Universidad Estatal Península de Santa Elena .

Cossio, O. (2022). Vulnerabilidades de Ciberseguridad en Sistema de Control Industrial y accesibilidad a través de redes públicas. Tesis de pregrado,Universidad Nacional Nordeste.

Aliaga Yupanqui, T. (2021). Implementación de un Sistema de Ciberseguridad para la prevención de los ataques cibernéticos en la Empresa Radiadores Fortaleza. Tesis de pregrado, Universidad César Vallejo.

Davila Angeles, et al. (2021). Propuesta de una Implementación de un programa de Gestión de Vulnerabilidades de Seguridad Informática para mitigar los siniestros de la información en el policlínico de salud AMC alineado a la NTP-ISO/IEC 27001:2014 en la ciudad de Lima. Tesis de pregrado, Universidad Tecnológica del Perú.

Huaman Mauricio, et al. (2022). Propuesta de implementación de políticas de seguridad basado en CISCO ISE (identity services engine) en la red LAN de Caja Huancayo. Tesis de pregrado, Universidad Continental.

Avalos Mendoza, et al. (2023). Diseño de un modelo de Gestión en Seguridad Digital para la aplicación en entidades peruanas del Sector Público. Tesis de pregrado, Universidad ESAN y ESAN graduate school of Business.

Huara Mere, G. (2019). Gestión de riesgos de seguridad de la información para empresas del sector telecomunicaciones. Tesis de pregrado, Universidad Mayor de San Marcos.

McGraw, G. (2006). Software Security: Building Security In. Addison-Wesley Professional. ISBN 978-0321356703.

Viega, J., & McGraw, G. (2006). The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities. Addison-Wesley Professional.ISBN: 978-0321444424.

Howard, M., & LeBlanc, D. (2009). 24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them. McGraw-Hill.ISBN: 978-0071626750

Redman, T. C. (2008). Data Driven: Profiting from Your Most Important Business Asset. Harvard Business Review Press.ISBN: 978-1422163649

Litchfield, D. (2007). The Shellcoder's Handbook: Discovering and Exploiting Security Holes. Wiley.ISBN: 978-0470080238

Fowler, M. (2018). Refactoring: Improving the Design of Existing Code. Addison-Wesley Professional. ISBN: 978-0134757599

Das, S., & Mishra, A. P. (2019). Vulnerability Management: A Review and Future Directions. International Journal of Information Management, 45, 102-113. DOI: 10.1016/j.ijinfomgt.2018.10.014

Chess, D., & McGraw, G. (2007). Static Analysis for Security. Addison-Wesley Professional ISBN: 978-0321424778

Whitman, M., & Mattord, H. (2018). Principles of Information Security. Cengage Learning. ISBN: 978-1337102063

Rhee, M., & Kim, H. (2019). A Comprehensive Study on Vulnerability Management. IEEE Access, 7, 66576-66589. DOI: 10.1109/ACCESS.2019.2919182

Booth, W., Colomb, G., & Williams, J. (2008). The Craft of Research. University of Chicago Press.

Gartner. (2021). Framework Gartner. En Título del libro A Guidance Framework for Developing and Implementing Vulnerability Management**.**

ISO/IEC 27001:2013. Information technology - Security techniques - Information security management systems - Requirements. Ginebra: ISO, 2013.

National Institute of Standards and Technology (NIST).(2014) Framework for Improving Critical Infrastructure Cybersecurity. NIST, 2014.

International Organization for Standardization (ISO). Risk Management - Guidelines. ISO, 2018.

International Organization for Standardization (ISO). Information technology - Security techniques - Code of practice for information security controls. ISO, 2013.

X. ANEXOS

ANEXO 01: MATRIZ DE CONSISTENCIA

“IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE VULNERABILIDADES PARA MEJORAR LA PRODUCTIVIDAD EN LA EMPRESA CONTACTA HABILIDAD S.A.C - LIMA 2024”

Problema	Objetivos	Hipótesis	Matriz de Consistencia						
			Variable	Definición Conceptual	Definición Operacional	Dimensión	Indicador	Instrumento	Metodología
Problema General "¿De qué manera la implementación de un Sistema de Gestión de Vulnerabilidades mejora la productividad en la empresa Contacta Habilidad S.A.C. - LIMA 2024?"	Problema General Determinar de qué manera la implementación de un Sistema de Gestión de Vulnerabilidades mejora la productividad en la empresa Contacta Habilidad S.A.C. - LIMA 2024.	Problema General La implementación de un sistema de gestión de vulnerabilidades mejora la productividad en la empresa Contacta Habilidad S.A.C - LIMA en el primer semestre 2024	Variable Independiente: Sistema de Gestión de Vulnerabilidades	La gestión de vulnerabilidades es el proceso de remediar y encontrar las vulnerabilidades de softwares con el propósito de mantener los riesgos del Sistema de Información en un nivel aceptable. Todos los sistemas y aplicaciones de Tecnología de Información tienen vulnerabilidades. Una vulnerabilidad es una debilidad que permite a un atacante reducir las características fundamentales de los Sistemas de	Se define un Sistema de Gestión de Vulnerabilidades es un enfoque integral y sistemático para identificar, clasificar y gestionar las vulnerabilidades en los sistemas de información de una organización. Este enfoque implica la implementación de procesos estructurados para la evaluación continua de las amenazas, la priorización de las	Identificación. Priorización Remediación Validación Mejora Continua	NC== Ejecutado/ Planificado	Fichas de registro	**TIPO DE ESTUDIO** APLICADA **DISEÑO DE ESTUDIO** EXPERIMENTAL **POBLACIÓN** 16 Servidores 6 Aplicaciones **MUESTRA** 16 Servidores 6 Aplicaciones **METODO DE INVESTIGACIÓN** Hipotético deductivo

Problema	Objetivos	Hipótesis	Matriz de Consistencia						
			Variable	Definición Conceptual	Definición Operacional	Dimensión	Indicador	Instrumento	Metodología
				Información. (Dávila, et al, 2021)	vulnerabilidades y la aplicación de controles de seguridad adecuados para mitigar los riesgos asociados (White, et al,2016)				**ESCALA DE MEDICIÓN TECNICA** Fichaje **INSTRUMENTO** Ficha de Registro
P1 : ¿De qué manera la implementación de un Sistema de Gestión de Vulnerabilidades mejora la eficiencia en la empresa Contacta Habilidad S.A.C. - LIMA 2024?	O1: Determinar de qué manera la implementación de un Sistema de Gestión de Vulnerabilidades mejora la eficiencia en la empresa Contacta Habilidad S.A.C. - LIMA 2024	H1: La implementación de un sistema de gestión de vulnerabilidades mejora la eficiencia en la empresa Contacta Habilidad S.A.C. - LIMA 2024	Variable Dependiente: Productividad	define como la relación entre la producción obtenida y los recursos utilizados para obtenerla. En otras palabras, representa la eficiencia con la que se utilizan los recursos para generar resultados tangibles. Esta definición enfatiza la capacidad de una organización	Se define la productividad en el ámbito de la ciberseguridad puede entenderse como la eficiencia con la que una organización gestiona y responde a las vulnerabilidades de seguridad en sus sistemas de información. Se relaciona	Eficiencia	Eficiencia en la Gestión de Vulnerabilidades: Número de vulnerabilidades remediadas automáticamente / Total de Vulnerabilidades corregidas x 100%	Fichas de registro	

Problema	Objetivos	Hipótesis	Matriz de Consistencia						
			Variable	Definición Conceptual	Definición Operacional	Dimensión	Indicador	Instrumento	Metodología
P2: ¿De qué manera la implementación de un Sistema de Gestión de Vulnerabilidades mejora la eficacia en la empresa Contacta Habilidad S.A.C., - LIMA 2024?	O2: Determinar de qué manera la implementación de un Sistema de Gestión de Vulnerabilidades mejora la eficacia en la empresa Contacta Habilidad S.A.C. - LIMA 2024	H2: La implementación de un sistema de gestión de vulnerabilidades mejora la eficacia en la empresa Contacta Habilidad S.A.C. - LIMA 2024		para maximizar la producción utilizando la menor cantidad de recursos posibles. La capacidad de una empresa para mantener altos niveles de productividad puede influir significativamente en su posición en el mercado y su capacidad para adaptarse a los cambios en el entorno empresarial. (García et al, 2022)	directamente con la capacidad de la organización para mantener un entorno tecnológico seguro y protegido, garantizando al mismo tiempo la continuidad operativa y minimizando los riesgos de incidentes de seguridad. (Aghajani, et al, 2017)	Eficacia	Eficacia de vulnerabilidades mitigadas: Número de vulnerabilidades críticas o de alta de severidad mitigadas/ Total de vulnerabilidades críticas o de alta de severidad comprometidas x 100%	Ficha de registro	

ANEXO 02: ACTIVOS DE LA EMPRESA CONTACTA HABILIDAD S.A.C

Nº	ID	Nombre	Tipo	Descripción	Propietario	Ambiente	Clasificación
1	SV1	vm-prd-sw-mes-sige-dwh-us-east	Servidor	Es un servidor de aplicaciones que almacena los war de las app.	Product Owner Infraestructura	Producción	Alto
2	SV2	vm-prd-postgre-main-us-east	Servidor	Es un servidor que almacena la base de datos.	Product Owner Infraestructura	Producción	Alto
3	SV3	vm-prd-sw-mes2-app-us-east	Servidor	Es un servidor que almacena el servicio mes2app	Product Owner Infraestructura	Producción	Alto
4	SV4	vm-prd-ml-task-arm-java11-us-east	Servidor	Es un servidor que almacena las tareas desarrolladas en Java11	Product Owner Infraestructura	Producción	Alto
5	SV5	vm-prd-contacta-python-us-east	Servidor	Es un servidor donde se conecta el equipo de sms para descargar el archivo de Sullana, con el objetivo de crear una campaña.	Product Owner Infraestructura	Producción	Alto
6	SV6	vir-prd-contactahabilidad-portal	Servidor	Servidor que almacena y levanta wordpress de MOWA.	Product Owner Infraestructura	Producción	Alto
7	SV7	vir-prd-contacta-wordpress	Servidor	Servidor que almacena y levanta wordpress de ContactaHabilidad	Product Owner Infraestructura	Producción	Alto
8	SV8	vm-prd-task-main-us-east	Servidor	Servidor que almacena las tareas automáticas en Java 8.	Product Owner Infraestructura	Producción	Alto
9	SV9	vm-prd-sftp-externals-users-us-east-1	Servidor	Servidor que almacena el SFTP del Santander	Product Owner Infraestructura	Producción	Alto
10	SV10	vm-prd-mst-main-us-east	Servidor	Servidor que almacena la aplicación que soporta el manejo de la URL corta desde la plataforma MES.	Product Owner Infraestructura	Producción	Alto

Nº	ID	Nombre	Tipo	Descripción	Propietario	Ambiente	Clasificación
11	SV11	vm-prd-ml-analytics-python3-us-east	Servidor	Servidor que almacena el proyecto Analytics de MOWA de las aplicaciones: MES, SIGE, DWH.	Product Owner Infraestructura	Producción	Alto
12	SV12	vm-prd-external-minera-corona-us-east	Servidor	Servidor que almacena el sistema que permite generar Documento Seguro.	Product Owner Infraestructura	Producción	Alto
13	SV13	vm-dev-mes-sige-dwh-us-east	Servidor	Servidor que almacena las aplicaciones para el ambiente de desarrollo.	Product Owner Infraestructura	Desarrollo	Medio
14	SV14	vm-prd-ncorto-us-east	Servidor	Servidor que almacena el sistema que envía los mensajes del tipo de salida de corto	Product Owner Infraestructura	Producción	Alto
15	SV15	vm-dev-postgre	Servidor	Servidor que almacena la base de datos para el ambiente de desarrollo.	Product Owner Infraestructura	Desarrollo	Medio
16	SV16	vm-dev-contacta-us-east	Servidor	Servidor que almacena pruebas en Docker entre otras.	Product Owner Infraestructura	Desarrollo	Medio
17	APP1	app.contactahabilidad.com/MES	Aplicación	Aplicación web de la plataforma MES	Product Owner Infraestructura	Producción	Alto
18	APP2	app.contactahabilidad.com/sige	Aplicación	Aplicación web de la plataforma SIGE	Product Owner Infraestructura	Producción	Alto
19	APP3	app.contactahabilidad.com/DWH	Aplicación	Aplicación web de la plataforma DWH	Product Owner Infraestructura	Producción	Alto
20	APP4	web.contactahabilidad.com	Aplicación	Aplicación web Contacta Habilidad	Product Owner Infraestructura	Producción	Alto
21	APP5	www.mowa.com.pe	Aplicación	Aplicación web Mowa Contact	Product Owner Infraestructura	Producción	Alto
22	APP6	www.m.mstpe.com	Aplicación	Aplicación web de documento seguro	Product Owner Infraestructura	Producción	Alto

Fuente: Elaboración propia

ANEXO 03: INSTRUMENTOS VALIDADOS

CARTA DE PRESENTACIÓN

Señor(a): Experto Validador

Asunto: VALIDACIÓN DE INSTRUMENTOS

Me es grato comunicarme con usted para expresarle mi saludo y, asimismo, hacer de su conocimiento que, siendo estudiantes de la Facultad de Ingeniería Industrial y de Sistemas de la Universidad Nacional del Callao, requiero validar los instrumentos con los cuales recogeré la información necesaria para poder desarrollar la investigación. El título del proyecto de investigación es **"Implementación de un Sistema de Gestión de Vulnerabilidades para mejorar la Productividad en la empresa Contacta Habilidad S.A.C., Lima – 2024"**, y siendo imprescindible contar con la aprobación de docentes especializados para poder aplicar los instrumentos en mención, he considerado conveniente recurrir a usted, ante su connotada experiencia en temas de Ingeniería de Sistemas, aplicación de metodologías y herramientas de calidad, y/o investigación. El expediente de validación, que le hago llegar contiene lo siguiente:

- Definiciones conceptuales de las variables y dimensiones.
- Matriz de operacionalización de las variables.
- Certificado de validez de contenido de los instrumentos.
- Protocolo de evaluación de instrumento

Expresándole mis sentimientos de respeto y consideración, me despido de usted, no sin antes agradecerle por la atención que dispense a la presente.

Atentamente.

MARÍA INÉS FLORES HUANCA
DNI:77174623

FIORELLA ARACELI NUÑEZ ZEGARRA
DNI:77096692

ANDREA GIULIANA VILLEGAS
DNI:73684340

Definiciones Conceptuales de las variables y dimensiones

Variable Independiente:

Sistema de Gestión de Vulnerabilidades

La gestión de vulnerabilidades es el proceso de remediar y encontrar las vulnerabilidades de softwares con el propósito de mantener los riesgos del Sistema de Información en un nivel aceptable. Todos los sistemas y aplicaciones de Tecnología de Información tienen vulnerabilidades. Una vulnerabilidad es una debilidad que permite a un atacante reducir las características fundamentales de los Sistemas de Información. (Dávila, et al, 2021)

De acuerdo con nuestro análisis, sistema de gestión de vulnerabilidades es una herramienta diseñada para identificar, priorizar, remediar, validar y mejora continua de vulnerabilidades, la cual permite automatizar el proceso de encontrar, gestionar y solucionar vulnerabilidades en las aplicaciones e infraestructura con el fin de mantener la integridad, disponibilidad y confidencialidad de los datos y recursos informáticos en una organización.

Dimensiones

Identificación

Esta fase implica la identificación proactiva de vulnerabilidades en los sistemas y redes de la organización, utilizando herramientas de escaneo de vulnerabilidades, análisis de seguridad y otros métodos de evaluación de vulnerabilidades. (Gartner, 2021)

Priorización

Una vez identificadas las vulnerabilidades, se deben priorizar según su criticidad y el impacto potencial en la organización. Las vulnerabilidades más críticas y

urgentes deben abordarse primero para mitigar los riesgos más importantes. En esta etapa, se realiza un análisis más detallado de las vulnerabilidades identificadas, evaluando su impacto potencial en los activos de información y los sistemas de la organización, así como la probabilidad de explotación y los posibles efectos adversos. (Gartner, 2021)

Remediación

Basándose en los resultados del análisis de riesgos, se desarrollan y aplican medidas correctivas y soluciones para abordar las vulnerabilidades identificadas, que pueden incluir parches de seguridad, actualizaciones de software, cambios de configuración y otras acciones correctivas. (Gartner, 2021)

Validación

Una vez implementadas las soluciones de remediación, es importante verificar la efectividad de las medidas correctivas implementadas. Después de aplicar las correcciones o soluciones recomendadas, se vuelve a realizar un escaneo de vulnerabilidades para verificar si las vulnerabilidades identificadas previamente han sido correctamente remediadas. (Gartner, 2021)

Mejora Continua

La gestión de vulnerabilidades es un proceso continuo y en evolución. Se requiere monitoreo constante, evaluación de nuevas amenazas y actualización de políticas y controles de seguridad para garantizar la protección continua de los activos de información de la organización. (Gartner, 2021)

Productividad

La productividad se define como la relación entre la producción obtenida y los recursos utilizados para obtenerla. En otras palabras, representa la eficiencia con la que se utilizan los recursos para generar resultados tangibles. Esta

definición enfatiza la capacidad de una organización para maximizar la producción utilizando la menor cantidad de recursos posibles. La capacidad de una empresa para mantener altos niveles de productividad puede influir significativamente en su posición en el mercado y su capacidad para adaptarse a los cambios en el entorno empresarial. (García et al, 2022)

Eficiencia

La eficiencia se refiere a la capacidad de realizar tareas o producir resultados utilizando la menor cantidad de recursos posibles, minimizando el desperdicio y maximizando la producción, implica la mejora continua y la capacidad de adaptación a cambios en el entorno empresarial, asegurando así la sostenibilidad a largo plazo. Las organizaciones eficientes son aquellas que pueden responder rápidamente a las demandas del mercado y ajustarse a nuevas condiciones sin incurrir en costos excesivos ni desperdiciar recursos. Richter (2018),

La eficiencia en la gestión de vulnerabilidades incluye la implementación de procesos automatizados y herramientas de escaneo que permiten a las organizaciones detectar y corregir vulnerabilidades de manera rápida y precisa. El estudio destaca que las empresas eficientes en este ámbito son capaces de reducir significativamente el tiempo de respuesta a las amenazas y disminuir la cantidad de recursos necesarios para gestionar la seguridad. Esto implica optimizar el uso del tiempo, personal, y tecnologías disponibles para minimizar los riesgos de seguridad de manera rentable y efectiva. (Humphreys, 2018)

Eficacia

La eficacia se define como la capacidad de lograr sus objetivos estratégicos y operativos de manera efectiva, utilizando de manera óptima sus recursos humanos y tecnológicos. Se ve impulsada por la capacidad de adaptación al cambio, la innovación continua y la alineación de los procesos internos con los objetivos de la organización. La eficacia subraya la importancia de la

implementación de sistemas de gestión del rendimiento y de la evaluación continua para asegurar que todas las actividades de la organización estén orientadas hacia la consecución de sus metas. (Lopez,2023).

La eficacia en la gestión de vulnerabilidades se refiere a la capacidad de una organización para alcanzar sus objetivos de seguridad, asegurando que las vulnerabilidades sean adecuadamente identificadas, priorizadas y mitigadas para proteger los activos críticos de la organización. La eficacia en este contexto implica no solo la implementación de controles y medidas de seguridad adecuadas, sino también la alineación de las estrategias de seguridad con los objetivos generales de la organización. (Shameli-Sendi, 2018),

Matriz de Operacionalización de Variables

Variable	Definición Conceptual	Definición Operacional	Dimensión	Indicador	Escala de Medición
Variable Independiente: Sistema de Gestión de Vulnerabilidades	La gestión de vulnerabilidades es el proceso de remediar y encontrar las vulnerabilidades de softwares con el propósito de mantener los riesgos del Sistema de Información en un nivel aceptable. Todos los sistemas y aplicaciones de Tecnología de Información tienen vulnerabilidades. Una vulnerabilidad es una debilidad que permite a un atacante reducir las características fundamentales de los Sistemas de Información. (Dávila, et al, 2021)	Se define un Sistema de Gestión de Vulnerabilidades es un enfoque integral y sistemático para identificar, clasificar y gestionar las vulnerabilidades en los sistemas de información de una organización. Este enfoque implica la implementación de procesos estructurados para la evaluación continua de las amenazas, la priorización de las vulnerabilidades y la aplicación de controles de seguridad adecuados para mitigar los riesgos asociados (White, et al,2016)	Identificación. Priorización Remediación Validación Mejora Continua	NC== Ejecutado/Planificado	Razón

Variable Dependiente: Productividad	La productividad se define como la relación entre la producción obtenida y los recursos utilizados para obtenerla. En otras palabras, representa la eficiencia con la que se utilizan los recursos para generar resultados tangibles. Esta definición enfatiza la capacidad de una organización para maximizar la producción utilizando la menor cantidad de recursos posibles. La capacidad de una empresa para mantener altos niveles de productividad puede influir significativamente en su posición en el mercado y su capacidad para adaptarse a los cambios en el entorno empresarial. (García et al, 2022)	Se define la productividad en el ámbito de la ciberseguridad puede entenderse como la eficiencia con la que una organización gestiona y responde a las vulnerabilidades de seguridad en sus sistemas de información. Se relaciona directamente con la capacidad de la organización para mantener un entorno tecnológico seguro y protegido, garantizando al mismo tiempo la continuidad operativa y minimizando los riesgos de incidentes de seguridad. (Aghajani,et al, 2017)	Eficiencia	Eficiencia en la Gestión de Vulnerabilidades: Número de vulnerabilidades remediadas automáticamente / Total de Vulnerabilidades corregidas x 100%	Razón
			Eficacia	Eficacia de vulnerabilidades mitigadas: Número de vulnerabilidades críticas o de alta de severidad mitigadas / Total de vulnerabilidades críticas o de alta de severidad comprometidas x 100%	

Certificado de validez de contenido del instrumento que mide el Sistema de Gestión de Vulnerabilidades

N	DIMENSIONES	Pertinencia		Relevancia		Claridad		Sugerencias
	DIMENSIÓN 1: Identificación	SI	NO	SI	NO	SI	NO	
1	$\mathrm{NC} = \frac{\textbf{Ejecutado}}{\textbf{Planificado}}$	**X**		X		X		
	DIMENSIÓN 2: Priorización	SI	NO	SI	NO	SI	NO	
2	$\mathrm{NC} = \frac{\textbf{Ejecutado}}{\textbf{Planificado}}$	**X**		X		X		
3	**DIMENSIÓN 3: Remediación**	SI	NO	SI	NO	SI	NO	
	$\mathrm{NC} = \frac{\textbf{Ejecutado}}{\textbf{Planificado}}$	**X**		X		X		
4	**DIMENSIÓN 4: Validación**	SI	NO	SI	NO	SI	NO	
	$\mathrm{NC} = \frac{\textbf{Ejecutado}}{\textbf{Planificado}}$	**X**		X		X		
5	**DIMENSIÓN 5: Mejor Continua**	SI	NO	SI	NO	SI	NO	
	$\mathrm{NC} = \frac{\textbf{Ejecutado}}{\textbf{Planificado}}$	**X**		X		X		

Certificado de validez de contenido del instrumento que mide la Productividad

N°	DIMENSIONES	Pertinencia		Relevancia		Claridad		Sugerencias
	DIMENSIÓN 1: Eficiencia	SI	NO	SI	NO	SI	NO	
1	$= \frac{\text{Número de vulnerabilidades remediadas automáticamente}}{\text{Total de Vulnerabilidades corregidas}} \times 100\%$	**X**		X		X		
	DIMENSIÓN 2: Eficacia	SI	NO	SI	NO	SI	NO	
2	$\frac{\text{Número de vulnerabilidades críticas y de alta de severidad mitigadas}}{\text{Total de vulnerabilidades críticas y de alta de severidad comprometidas}} \times 100\%$	**X**		X		X		

Protocolo de evaluación de instrumento

Observaciones:

_____

_____

Opinión de aplicabilidad:

Aplicable [x] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador:

DNI del juez validador:

_____

Firma del Experto Validador

Pertinencia: El ítem corresponde al concepto teórico formulado.

Relevancia: El ítem es apropiado para representar al componente o dimensión específica del constructo

Claridad: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

CARTA DE PRESENTACIÓN

Señor(a): Experto Validador

Asunto: VALIDACIÓN DE INSTRUMENTOS

Me es grato comunicarme con usted para expresarle mi saludo y, asimismo, hacer de su conocimiento que, siendo estudiantes de la Facultad de Ingeniería Industrial y de Sistemas de la Universidad Nacional del Callao, requiero validar los instrumentos con los cuales recogeré la información necesaria para poder desarrollar la investigación. El título del proyecto de investigación es **"Implementación de un Sistema de Gestión de Vulnerabilidades para mejorar la Productividad en la empresa Contacta Habilidad S.A.C., Lima – 2024"**, y siendo imprescindible contar con la aprobación de docentes especializados para poder aplicar los instrumentos en mención, he considerado conveniente recurrir a usted, ante su connotada experiencia en temas de Ingeniería de Sistemas, aplicación de metodologías y herramientas de calidad, y/o investigación. El expediente de validación, que le hago llegar contiene lo siguiente:

- Definiciones conceptuales de las variables y dimensiones.
- Matriz de operacionalización de las variables.
- Certificado de validez de contenido de los instrumentos.
- Protocolo de evaluación de instrumento

Expresándole mis sentimientos de respeto y consideración, me despido de usted, no sin antes agradecerle por la atención que dispense a la presente.

Atentamente.

MARÍA INÉS FLORES HUANCA
DNI:77174623

FIORELLA ARACELI NUÑEZ ZEGARRA
DNI:77096692

ANDREA GIULIANA VILLEGAS
DNI:73684340

Definiciones Conceptuales de las variables y dimensiones

Variable Independiente:

Sistema de Gestión de Vulnerabilidades

La gestión de vulnerabilidades es el proceso de remediar y encontrar las vulnerabilidades de softwares con el propósito de mantener los riesgos del Sistema de Información en un nivel aceptable. Todos los sistemas y aplicaciones de Tecnología de Información tienen vulnerabilidades. Una vulnerabilidad es una debilidad que permite a un atacante reducir las características fundamentales de los Sistemas de Información. (Dávila, et al, 2021)

De acuerdo con nuestro análisis, sistema de gestión de vulnerabilidades es una herramienta diseñada para identificar, priorizar, remediar, validar y mejora continua de vulnerabilidades, la cual permite automatizar el proceso de encontrar, gestionar y solucionar vulnerabilidades en las aplicaciones e infraestructura con el fin de mantener la integridad, disponibilidad y confidencialidad de los datos y recursos informáticos en una organización.

Dimensiones

Identificación

Esta fase implica la identificación proactiva de vulnerabilidades en los sistemas y redes de la organización, utilizando herramientas de escaneo de vulnerabilidades, análisis de seguridad y otros métodos de evaluación de vulnerabilidades. (Gartner, 2021)

Priorización

Una vez identificadas las vulnerabilidades, se deben priorizar según su criticidad y el impacto potencial en la organización. Las vulnerabilidades más críticas y urgentes deben abordarse primero para mitigar los riesgos más importantes. En esta etapa, se realiza un análisis más detallado de las vulnerabilidades identificadas, evaluando su impacto potencial en los activos de información y los

sistemas de la organización, así como la probabilidad de explotación y los posibles efectos adversos. (Gartner, 2021)

Remediación

Basándose en los resultados del análisis de riesgos, se desarrollan y aplican medidas correctivas y soluciones para abordar las vulnerabilidades identificadas, que pueden incluir parches de seguridad, actualizaciones de software, cambios de configuración y otras acciones correctivas. (Gartner, 2021)

Validación

Una vez implementadas las soluciones de remediación, es importante verificar la efectividad de las medidas correctivas implementadas. Después de aplicar las correcciones o soluciones recomendadas, se vuelve a realizar un escaneo de vulnerabilidades para verificar si las vulnerabilidades identificadas previamente han sido correctamente remediadas. (Gartner, 2021)

Mejora Continua

La gestión de vulnerabilidades es un proceso continuo y en evolución. Se requiere monitoreo constante, evaluación de nuevas amenazas y actualización de políticas y controles de seguridad para garantizar la protección continua de los activos de información de la organización. (Gartner, 2021)

Productividad

La productividad se define como la relación entre la producción obtenida y los recursos utilizados para obtenerla. En otras palabras, representa la eficiencia con la que se utilizan los recursos para generar resultados tangibles. Esta definición enfatiza la capacidad de una organización para maximizar la producción utilizando la menor cantidad de recursos posibles. La capacidad de una empresa para mantener altos niveles de productividad puede influir

significativamente en su posición en el mercado y su capacidad para adaptarse a los cambios en el entorno empresarial. (García et al, 2022)

Eficiencia

La eficiencia se refiere a la capacidad de realizar tareas o producir resultados utilizando la menor cantidad de recursos posibles, minimizando el desperdicio y maximizando la producción, implica la mejora continua y la capacidad de adaptación a cambios en el entorno empresarial, asegurando así la sostenibilidad a largo plazo. Las organizaciones eficientes son aquellas que pueden responder rápidamente a las demandas del mercado y ajustarse a nuevas condiciones sin incurrir en costos excesivos ni desperdiciar recursos. Richter (2018),

La eficiencia en la gestión de vulnerabilidades incluye la implementación de procesos automatizados y herramientas de escaneo que permiten a las organizaciones detectar y corregir vulnerabilidades de manera rápida y precisa. El estudio destaca que las empresas eficientes en este ámbito son capaces de reducir significativamente el tiempo de respuesta a las amenazas y disminuir la cantidad de recursos necesarios para gestionar la seguridad. Esto implica optimizar el uso del tiempo, personal, y tecnologías disponibles para minimizar los riesgos de seguridad de manera rentable y efectiva. (Humphreys, 2018)

Eficacia

La eficacia se define como la capacidad de lograr sus objetivos estratégicos y operativos de manera efectiva, utilizando de manera óptima sus recursos humanos y tecnológicos. Se ve impulsada por la capacidad de adaptación al cambio, la innovación continua y la alineación de los procesos internos con los objetivos de la organización. (Lopez,2023).

La eficacia en la gestión de vulnerabilidades se refiere a la capacidad de una organización para alcanzar sus objetivos de seguridad, asegurando que las vulnerabilidades sean adecuadamente identificadas, priorizadas y mitigadas

para proteger los activos críticos de la organización. La eficacia en este contexto implica no solo la implementación de controles y medidas de seguridad adecuadas, sino también la alineación de las estrategias de seguridad con los objetivos generales de la organización. (Shameli-Sendi, 2018).

Matriz de Operacionalización de Variables

Variable	Definición Conceptual	Definición Operacional	Dimensión	Indicador	Escala de Medición
Variable Independiente: Sistema de Gestión de Vulnerabilidades	La gestión de vulnerabilidades es el proceso de remediar y encontrar las vulnerabilidades de softwares con el propósito de mantener los riesgos del Sistema de Información en un nivel aceptable. Todos los sistemas y aplicaciones de Tecnología de Información tienen vulnerabilidades. Una vulnerabilidad es una debilidad que permite a un atacante reducir las características fundamentales de los Sistemas de Información. (Dávila, et al, 2021)	Se define un Sistema de Gestión de Vulnerabilidades es un enfoque integral y sistemático para identificar, clasificar y gestionar las vulnerabilidades en los sistemas de información de una organización. Este enfoque implica la implementación de procesos estructurados para la evaluación continua de las amenazas, la priorización de las vulnerabilidades y la aplicación de controles de seguridad adecuados para mitigar los riesgos asociados (White, et al,2016)	Identificación. Priorización Remediación Validación Mejora Continua	NC== Ejecutado/Planificado	Razón
Variable Dependiente: Productividad	La productividad se define como la relación entre la producción obtenida y los recursos utilizados para obtenerla. En otras palabras, representa la eficiencia con la que se utilizan los recursos para generar resultados tangibles. Esta definición enfatiza la capacidad de una organización para maximizar la	Se define la productividad en el ámbito de la ciberseguridad puede entenderse como la eficiencia con la que una organización gestiona y responde a las vulnerabilidades de seguridad en sus sistemas de información. Se relaciona directamente con la capacidad de la organización para mantener un entorno tecnológico seguro y	Eficiencia	Eficiencia en la Gestión de Vulnerabilidades: Número de vulnerabilidades remediadas automáticamente / Total de Vulnerabi	Razón

	producción utilizando la menor cantidad de recursos posibles. La capacidad de una empresa para mantener altos niveles de productividad puede influir significativamente en su posición en el mercado y su capacidad para adaptarse a los cambios en el entorno empresarial. (García et al, 2022)	protegido, garantizando al mismo tiempo la continuidad operativa y minimizando los riesgos de incidentes de seguridad. (Aghajani, et al, 2017=		lidades corregidas x 100%	
			Eficacia	Eficacia de vulnerabilidades mitigadas: Número de vulnerabilidades críticas o de alta de severidad mitigadas / Total de vulnerabilidades críticas o de alta de severidad comprometidas x 100%	

Certificado de validez de contenido del instrumento que mide el Sistema de Gestión de Vulnerabilidades

N°	DIMENSIONES	Pertinencia		Relevancia		Claridad		Sugerencias
	DIMENSIÓN 1: Identificación	SI	NO	SI	NO	SI	NO	
1	$\mathrm{NC} = \frac{\textbf{Ejecutado}}{\textbf{Planificado}}$	**X**		X		X		
	DIMENSIÓN 2: Priorización	SI	NO	SI	NO	SI	NO	
2	$\mathrm{NC} = \frac{\textbf{Ejecutado}}{\textbf{Planificado}}$	**X**		X		X		
3	**DIMENSIÓN 3: Remediación**	SI	NO	SI	NO	SI	NO	
	$\mathrm{NC} = \frac{\textbf{Ejecutado}}{\textbf{Planificado}}$	**X**		X		X		
4	**DIMENSIÓN 4: Validación**	SI	NO	SI	NO	SI	NO	
	$\mathrm{NC} = \frac{\textbf{Ejecutado}}{\textbf{Planificado}}$	**X**		X		X		
5	**DIMENSIÓN 5: Mejor Continua**	SI	NO	SI	NO	SI	NO	
	$\mathrm{NC} = \frac{\textbf{Ejecutado}}{\textbf{Planificado}}$	**X**		X		X		

Certificado de validez de contenido del instrumento que mide la Productividad

N°	DIMENSIONES	Pertinencia		Relevancia		Claridad		Sugerencias
	DIMENSIÓN 1: Eficiencia	SI	NO	SI	NO	SI	NO	
1	$= \frac{\textbf{Número de vulnerabilidades remediadas automáticamente}}{\textbf{Total de Vulnerabilidades corregidas}} \times 100\%$	**X**		X		X		
	DIMENSIÓN 2: Eficacia	SI	NO	SI	NO	SI	NO	
2	$\frac{\textbf{Número de vulnerabilidades críticas y de alta de severidad mitigadas}}{\textbf{Total de vulnerabilidades críticas y de alta de severidad comprometidas}} \times 100\%$	**X**		X		X		

Protocolo de evaluación de instrumento

Observaciones:

_____

_____

Opinión de aplicabilidad:

Aplicable [x] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador:

DNI del juez validador:

- -

Firma del Experto Validador

Pertinencia: El ítem corresponde al concepto teórico formulado.

Relevancia: El ítem es apropiado para representar al componente o dimensión específica del constructo

Claridad: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

CARTA DE PRESENTACIÓN

Señor(a): Experto Validador

Asunto: VALIDACIÓN DE INSTRUMENTOS

Me es grato comunicarme con usted para expresarle mi saludo y, asimismo, hacer de su conocimiento que, siendo estudiantes de la Facultad de Ingeniería Industrial y de Sistemas de la Universidad Nacional del Callao, requiero validar los instrumentos con los cuales recogeré la información necesaria para poder desarrollar la investigación. El título del proyecto de investigación es **"Implementación de un Sistema de Gestión de Vulnerabilidades para mejorar la Productividad en la empresa Contacta Habilidad S.A.C., Lima – 2024"**, y siendo imprescindible contar con la aprobación de docentes especializados para poder aplicar los instrumentos en mención, he considerado conveniente recurrir a usted, ante su connotada experiencia en temas de Ingeniería de Sistemas, aplicación de metodologías y herramientas de calidad, y/o investigación. El expediente de validación, que le hago llegar contiene lo siguiente:

- Definiciones conceptuales de las variables y dimensiones.
- Matriz de operacionalización de las variables.
- Certificado de validez de contenido de los instrumentos.
- Protocolo de evaluación de instrumento

Expresándole mis sentimientos de respeto y consideración, me despido de usted, no sin antes agradecerle por la atención que dispense a la presente.

Atentamente.

MARÍA INÉS FLORES HUANCA
DNI:77174623

FIORELLA ARACELI NUÑEZ ZEGARRA
DNI:77096692

ANDREA GIULIANA VILLEGAS
DNI:73684340

Definiciones Conceptuales de las variables y dimensiones

Variable Independiente:

Sistema de Gestión de Vulnerabilidades

La gestión de vulnerabilidades es el proceso de remediar y encontrar las vulnerabilidades de softwares con el propósito de mantener los riesgos del Sistema de Información en un nivel aceptable. Todos los sistemas y aplicaciones de Tecnología de Información tienen vulnerabilidades. Una vulnerabilidad es una debilidad que permite a un atacante reducir las características fundamentales de los Sistemas de Información. (Dávila, et al, 2021)

De acuerdo con nuestro análisis, sistema de gestión de vulnerabilidades es una herramienta diseñada para identificar, priorizar, remediar, validar y mejora continua de vulnerabilidades, la cual permite automatizar el proceso de encontrar, gestionar y solucionar vulnerabilidades en las aplicaciones e infraestructura con el fin de mantener la integridad, disponibilidad y confidencialidad de los datos y recursos informáticos en una organización.

Dimensiones

Identificación

Esta fase implica la identificación proactiva de vulnerabilidades en los sistemas y redes de la organización, utilizando herramientas de escaneo de vulnerabilidades, análisis de seguridad y otros métodos de evaluación de vulnerabilidades. (Gartner, 2021)

Priorización

Una vez identificadas las vulnerabilidades, se deben priorizar según su criticidad y el impacto potencial en la organización. Las vulnerabilidades más críticas y urgentes deben abordarse primero para mitigar los riesgos más importantes. En

esta etapa, se realiza un análisis más detallado de las vulnerabilidades identificadas, evaluando su impacto potencial en los activos de información y los sistemas de la organización, así como la probabilidad de explotación y los posibles efectos adversos. (Gartner, 2021)

Remediación

Basándose en los resultados del análisis de riesgos, se desarrollan y aplican medidas correctivas y soluciones para abordar las vulnerabilidades identificadas, que pueden incluir parches de seguridad, actualizaciones de software, cambios de configuración y otras acciones correctivas. (Gartner, 2021)

Validación

Una vez implementadas las soluciones de remediación, es importante verificar la efectividad de las medidas correctivas implementadas. Después de aplicar las correcciones o soluciones recomendadas, se vuelve a realizar un escaneo de vulnerabilidades para verificar si las vulnerabilidades identificadas previamente han sido correctamente remediadas. (Gartner, 2021)

Mejora Continua

La gestión de vulnerabilidades es un proceso continuo y en evolución. Se requiere monitoreo constante, evaluación de nuevas amenazas y actualización de políticas y controles de seguridad para garantizar la protección continua de los activos de información de la organización. (Gartner, 2021)

Productividad

La productividad se define como la relación entre la producción obtenida y los recursos utilizados para obtenerla. En otras palabras, representa la eficiencia con la que se utilizan los recursos para generar resultados tangibles. Esta definición enfatiza la capacidad de una organización para maximizar la

producción utilizando la menor cantidad de recursos posibles. La capacidad de una empresa para mantener altos niveles de productividad puede influir significativamente en su posición en el mercado y su capacidad para adaptarse a los cambios en el entorno empresarial. (García et al, 2022)

Eficiencia

La eficiencia se refiere a la capacidad de realizar tareas o producir resultados utilizando la menor cantidad de recursos posibles, minimizando el desperdicio y maximizando la producción, implica la mejora continua y la capacidad de adaptación a cambios en el entorno empresarial, asegurando así la sostenibilidad a largo plazo. Las organizaciones eficientes son aquellas que pueden responder rápidamente a las demandas del mercado y ajustarse a nuevas condiciones sin incurrir en costos excesivos ni desperdiciar recursos. Richter (2018),

La eficiencia en la gestión de vulnerabilidades incluye la implementación de procesos automatizados y herramientas de escaneo que permiten a las organizaciones detectar y corregir vulnerabilidades de manera rápida y precisa. El estudio destaca que las empresas eficientes en este ámbito son capaces de reducir significativamente el tiempo de respuesta a las amenazas y disminuir la cantidad de recursos necesarios para gestionar la seguridad. Esto implica optimizar el uso del tiempo, personal, y tecnologías disponibles para minimizar los riesgos de seguridad de manera rentable y efectiva. (Humphreys, 2018)

Eficacia

La eficacia se define como la capacidad de lograr sus objetivos estratégicos y operativos de manera efectiva, utilizando de manera óptima sus recursos humanos y tecnológicos. Se ve impulsada por la capacidad de adaptación al cambio, la innovación continua y la alineación de los procesos internos con los objetivos de la organización. (Lopez,2023).

La eficacia en la gestión de vulnerabilidades se refiere a la capacidad de una organización para alcanzar sus objetivos de seguridad, asegurando que las vulnerabilidades sean adecuadamente identificadas, priorizadas y mitigadas para proteger los activos críticos de la organización. La eficacia en este contexto implica no solo la implementación de controles y medidas de seguridad adecuadas, sino también la alineación de las estrategias de seguridad con los objetivos generales de la organización. (Shameli-Sendi, 2018).

Matriz de Operacionalización de Variables

Variable	Definición Conceptual	Definición Operacional	Dimensión	Indicador	Escala de Medición
Variable Independiente: Sistema de Gestión de Vulnerabilidades	La gestión de vulnerabilidades es el proceso de remediar y encontrar las vulnerabilidades de softwares con el propósito de mantener los riesgos del Sistema de Información en un nivel aceptable. Todos los sistemas y aplicaciones de Tecnología de Información tienen vulnerabilidades. Una vulnerabilidad es una debilidad que permite a un atacante reducir las características fundamentales de los Sistemas de Información. (Dávila, et al, 2021)	Se define un Sistema de Gestión de Vulnerabilidades es un enfoque integral y sistemático para identificar, clasificar y gestionar las vulnerabilidades en los sistemas de información de una organización. Este enfoque implica la implementación de procesos estructurados para la evaluación continua de las amenazas, la priorización de las vulnerabilidades y la aplicación de controles de seguridad adecuados para mitigar los riesgos asociados (White, et al,2016)	Identificación. Priorización Remediación Validación Mejora Continua	NC== Ejecutado/Planificado	Razón
Variable Dependiente: Productividad	La productividad se define como la relación entre la producción obtenida y los recursos utilizados para obtenerla. En otras palabras, representa la eficiencia con la que se utilizan los recursos para	Se define la productividad en el ámbito de la ciberseguridad puede entenderse como la eficiencia con la que una organización gestiona y responde a las vulnerabilidades de seguridad en sus sistemas de	Eficiencia	Eficiencia en la Gestión de Vulnerabilidades: Número de vulnerabilidades	Razón

	generar resultados tangibles. Esta definición enfatiza la capacidad de una organización para maximizar la producción utilizando la menor cantidad de recursos posibles. La capacidad de una empresa para mantener altos niveles de productividad puede influir significativamente en su posición en el mercado y su capacidad para adaptarse a los cambios en el entorno empresarial. (García et al, 2022)	información. Se relaciona directamente con la capacidad de la organización para mantener un entorno tecnológico seguro y protegido, garantizando al mismo tiempo la continuidad operativa y minimizando los riesgos de incidentes de seguridad. (Aghajani,et al, 2017=		remediadas automáticamente / Total de Vulnerabilidades corregidas x 100%	
			Eficacia	Eficacia de vulnerabilidades mitigadas: Número de vulnerabilidades críticas o de alta de severidad mitigadas / Total de vulnerabilidades críticas o de alta de severidad comprometidas x 100%	

Certificado de validez de contenido del instrumento que mide el Sistema de Gestión de Vulnerabilidades

N°	DIMENSIONES	Pertinencia		Relevancia		Claridad		Sugerencias
	DIMENSIÓN 1: Identificación	SI	NO	SI	NO	SI	NO	
1	$\mathrm{NC} = \frac{\textbf{Ejecutado}}{\textbf{Planificado}}$	**X**		X		X		
	DIMENSIÓN 2: Priorización	SI	NO	SI	NO	SI	NO	
2	$\mathrm{NC} = \frac{\textbf{Ejecutado}}{\textbf{Planificado}}$	**X**		X		X		
3	**DIMENSIÓN 3: Remediación**	SI	NO	SI	NO	SI	NO	
	$\mathrm{NC} = \frac{\textbf{Ejecutado}}{\textbf{Planificado}}$	**X**		X		X		
4	**DIMENSIÓN 4: Validación**	SI	NO	SI	NO	SI	NO	
	$\mathrm{NC} = \frac{\textbf{Ejecutado}}{\textbf{Planificado}}$	**X**		X		X		
5	**DIMENSIÓN 5: Mejor Continua**	SI	NO	SI	NO	SI	NO	
	$\mathrm{NC} = \frac{\textbf{Ejecutado}}{\textbf{Planificado}}$	**X**		X		X		

Certificado de validez de contenido del instrumento que mide la Productividad

N	DIMENSIONES	Pertinencia		Relevancia		Claridad		Sugerencias
	DIMENSIÓN 1: Eficiencia	SI	NO	SI	NO	SI	NO	
1	$= \frac{\textbf{Número de vulnerabilidades remediadas automáticamente}}{\textbf{Total de Vulnerabilidades corregidas}} \times 100\%$	**X**		X		X		
	DIMENSIÓN 2: Eficacia	SI	NO	SI	NO	SI	NO	
2	$\frac{\textbf{Número de vulnerabilidades críticas y de alta de severidad mitigadas}}{\textbf{Total de vulnerabilidades críticas y de alta de severidad comprometidas}} \times 100\%$	**X**		X		X		

Protocolo de evaluación de instrumento

Observaciones:

_____

_____

Opinión de aplicabilidad:

Aplicable [x] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador:

DNI del juez validador:

Firma del Experto Validador

Pertinencia: El ítem corresponde al concepto teórico formulado.

Relevancia: El ítem es apropiado para representar al componente o dimensión específica del constructo

Claridad: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

ANEXO 04: CONSENTIMIENTO INFORMADO

UNIVERSIDAD NACIONAL DEL CALLAO
FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS
UNIDAD DE INVESTIGACIÓN
"Año de la unidad, la paz y el desarrollo"

SOLICITO: AUTORIZACIÓN PARA REALIZAR ESTUDIO

CONSENTIMIENTO INFORMADO

Usted ha sido invitado a participar en el estudio titulado "IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE VULNERABILIDADES PARA MEJORAR LA PRODUCTIVIDAD EN LA EMPRESA CONTACTA HABILIDAD S.A.C., LIMA-2024", por esta razón es muy importante que conozca y entienda la información necesaria sobre el estudio de forma que permita tomar una decisión sobre su participación en el mismo. Cualquier duda o aclaración que surja respecto al estudio, le será aclarada por el investigador responsable.
El estudio pretende determinar de qué manera la implementación de un Sistema de Gestión de Vulnerabilidades mejora la productividad en la empresa Contacta Habilidad S.A.C., Lima-2024.
Por medio de este documento se **autoriza la investigación** en la empresa Contacta Habilidad S.AC. y se asegura la total confidencialidad de la información suministrada por usted. Queda explícito que los datos obtenidos serán de uso y análisis exclusivo del estudio de investigación con fines netamente académicos.

DECLARACIÓN PERSONAL

He sido invitado a participar en el estudio titulado "IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE VULNERABILIDADES PARA MEJORAR LA PRODUCTIVIDAD EN LA EMPRESA CONTACTA HABILIDAD S.A.C., LIMA-2024", Me han explicado y he comprendido satisfactoriamente el propósito de la investigación y se me han aclarado dudas relacionadas con mi participación en dicho estudio. Por lo tanto, acepto participar de manera voluntaria en el estudio y brindo mi total **autorización** para que se pueda realizar el estudio, aportando la información necesaria para el estudio y sé que tengo el derecho a terminar mi participación en cualquier momento.

Lima, 4 de mayo de 2024

CONTACTA HABILIDAD S.A.C
Erick Eddy Cárdenas Acuña
GERENTE GENERAL

Erick E. Cárdenas Acuña
DNI 46966805

ANEXO 05: FICHA DE REGISTRO

Reporte Vulnerabilidades

Año	Código	Nombre de escenario	Vulnerabilidad	CVSS	Severidad
Enero	VCE01	Pruebas de Ataque y Penetración Externa	Soporte de versión no segura de TLS	5	MEDIO
Febrero	VCE01	Pruebas de Ataque y Penetración Externa	Soporte de versión no segura de TLS	5	MEDIO
Marzo	VCE01	Pruebas de Ataque y Penetración Externa	Soporte de versión no segura de TLS	5	MEDIO
Abril	VCE01	Pruebas de Ataque y Penetración Externa	Soporte de versión no segura de TLS	5	MEDIO
Enero	VCE01	Pruebas de Ataque y Penetración Externa	Soporte de versión no segura de TLS	5	MEDIO
Febrero	VCE01	Pruebas de Ataque y Penetración Externa	Soporte de versión no segura de TLS	5	MEDIO
Marzo	VCE01	Pruebas de Ataque y Penetración Externa	Soporte de versión no segura de TLS	5	MEDIO
Enero	VCE01	Pruebas de Ataque y Penetración Externa	Exposición de IP interna	6.2	MEDIO
Enero	VCE03	Pruebas de Seguridad de Aplicaciones Web	Ausencia de Strict-Trasnport-Security	4.8	MEDIO
Enero	VCE03	Pruebas de Seguridad de Aplicaciones Web	Exposición de Información en Mensaje de Erro	3.5	BAJO
Enero	VCE03	Pruebas de Seguridad de Aplicaciones Web	Soporte de suites de Cifrados Débiles	3.7	BAJO
Enero	VCE03	Pruebas de Seguridad de Aplicaciones Web	Soporte de suites de Cifrados Débiles	3.7	BAJO
Enero	VCE03	Pruebas de Seguridad de Aplicaciones Web	Soporte de suites de Cifrados Débiles	3.7	BAJO
Enero	VCE03	Pruebas de Seguridad de Aplicaciones Web	Soporte de suites de Cifrados Débiles	3.7	BAJO
Enero	VCE03	Pruebas de Seguridad de Aplicaciones Web	Soporte de suites de Cifrados Débiles	3.7	BAJO
Enero	VCE03	Pruebas de Seguridad de Aplicaciones Web	Soporte de suites de Cifrados Débiles	3.7	BAJO
Enero	VCE06	Pruebas de Seguridad de Aplicaciones Móviles	Insuficiente ofuscamiento de Codigo	3.5	BAJO
Enero	VCE06	Pruebas de Seguridad de Aplicaciones Móviles	Insuficiente ofuscamiento de Codigo	3.5	BAJO
Enero	VCE12	Pruebas de Seguridad de Aplicaciones Cloud	Compatible con conjuntos de cifrado SSL de pc	6.5	MEDIO
Enero	VCE12	Pruebas de Seguridad de Aplicaciones Cloud	Compatible con conjuntos de cifrado SSL de pc	6.5	MEDIO
Enero	VCE12	Pruebas de Seguridad de Aplicaciones Cloud	Compatible con conjuntos de cifrado SSL de pc	6.5	MEDIO
Enero	VCE12	Pruebas de Seguridad de Aplicaciones Cloud	Compatible con conjuntos de cifrado SSL de pc	6.5	MEDIO
Enero	VCE12	Pruebas de Seguridad de Aplicaciones Cloud	Compatible con conjuntos de cifrado SSL de pc	6.5	MEDIO
Enero	VCE12	Pruebas de Seguridad de Aplicaciones Cloud	Versión insegura de TLS	6.5	MEDIO
Enero	VCE12	Pruebas de Seguridad de Aplicaciones Cloud	Versión insegura de TLS	6.5	MEDIO
Enero	VCE12	Pruebas de Seguridad de Aplicaciones Cloud	Versión insegura de TLS	6.5	MEDIO
Enero	VCE12	Pruebas de Seguridad de Aplicaciones Cloud	Versión insegura de TLS	6.5	MEDIO
Enero	VCE12	Pruebas de Seguridad de Aplicaciones Cloud	Versión insegura de TLS	6.5	MEDIO

Año	Código	Nombre de escenario	Vulnerabilidad	CVSS	Severidad
Enero	VCE03	Pruebas de Seguridad de Aplicaciones Web	IBM WebSphere Application Server 8.5.5.8 vulnerable	6.5	ALTO
Enero	VCE03	Pruebas de Seguridad de Aplicaciones Web	Soporte de Versión Insegura de TLS	7.5	ALTO
Enero	VCE03	Pruebas de Seguridad de Aplicaciones Web	Soporte de Versión Insegura de TLS	7.5	ALTO
Enero	VCE03	Pruebas de Seguridad de Aplicaciones Web	Fallas en el cifrado y autenticación de	7.5	ALTO
Enero	VCE03	Pruebas de Seguridad de Aplicaciones Web	Ausencia de Strict-Transport-Security	7.5	ALTO
Enero	VCE03	Pruebas de Seguridad de Aplicaciones Web	Ausencia de Strict-Transport-Security	7.5	ALTO
Enero	VCE03	Pruebas de Seguridad de Aplicaciones Web	Ausencia de Strict-Transport-Security	7.5	ALTO
Enero	VCE03	Pruebas de Seguridad de Aplicaciones Web	Ausencia de Strict-Transport-Security	7.5	ALTO
Marzo	VCE03	Pruebas de Seguridad de Aplicaciones Web	Escáner modo 6 del protocolo de tiempo de red (NTP)	7.5	ALTO
Marzo	VCE03	Pruebas de Seguridad de Aplicaciones Web	Librería JS Vulnerable	7.5	ALTO
Marzo	VCE03	Pruebas de Seguridad de Aplicaciones Web	No se requiere firma SMB	7.5	ALTO
Marzo	VCE03	Pruebas de Seguridad de Aplicaciones Web	Suites de cifrado SSL de resistencia media compatibles (SWEET32)	7.5	ALTO
Marzo	VCE03	Pruebas de Seguridad de Aplicaciones Web	Suites de cifrado SSL de resistencia media compatibles (SWEET32)	7.5	ALTO
Marzo	VCE03	Pruebas de Seguridad de Aplicaciones Web	Identificación de Versión de Servidor	7.5	ALTO
Marzo	VCE03	Pruebas de Seguridad de Aplicaciones Web	Identificación de Versión de Servidor	7.5	ALTO
Marzo	VCE03	Pruebas de Seguridad de Aplicaciones Web	Soporte de suites de Cifrado Débiles	7.5	ALTO
Marzo	VCE03	Pruebas de Seguridad de Aplicaciones Web	Soporte de suites de Cifrado Débiles	7.5	ALTO
Marzo	VCE03	Pruebas de Seguridad de Aplicaciones Web	Soporte de suites de Cifrado Débiles	7.5	ALTO
Marzo	VCE03	Pruebas de Seguridad de Aplicaciones Web	Soporte de suites de Cifrado Débiles	7.5	ALTO
Marzo	VCE03	Pruebas de Seguridad de Aplicaciones Web	Soporte de suites de Cifrado Débiles	7.5	ALTO
Marzo	VCE03	Pruebas de Seguridad de Aplicaciones Web	Soporte de suites de Cifrado Débiles	7.5	ALTO
Marzo	VCE03	Pruebas de Seguridad de Aplicaciones Web	Cookie de Sesión sin el Atributo Secure	7.5	ALTO
Marzo	VCE03	Pruebas de Seguridad de Aplicaciones Web	Cookie de Sesión sin el Atributo Secure	7.5	ALTO
Marzo	VCE03	Pruebas de Seguridad de Aplicaciones Web	Exposición de Información en Mensaje de Error	7.5	ALTO
Marzo	VCE03	Pruebas de Seguridad de Aplicaciones Web	Inadecuada validación de variables	7.5	ALTO
Marzo	VCE03	Pruebas de Seguridad de Aplicaciones Web	Inadecuada validación de variables	7.5	ALTO

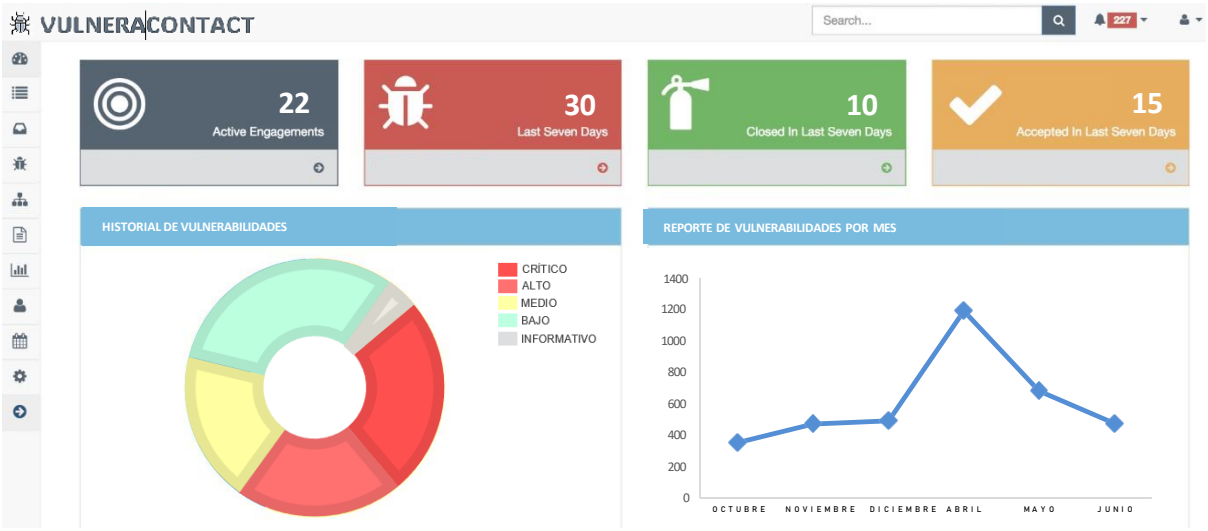
ANEXO 06: HOJA DE DATOS

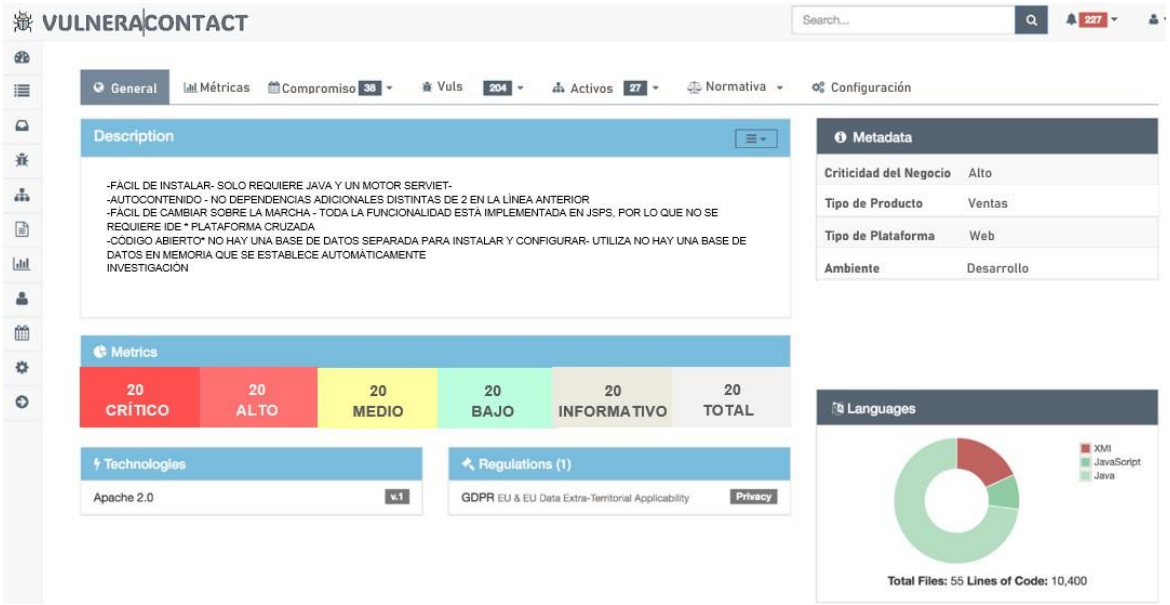
ID ACTIVO	TIPO DE ACTIVO	AMBIENTE	TOTAL VULNERA	BAJO1	MEDIO2	ALTO3	CRÍTICO4	TOTAL VULNERABILIDAD	BAJO	MEDIO	ALTO	CRÍTICO	% RESOLUCIÓN	FECHA
APP1	APLICACIÓN	PRODUCCION	5	1	1	2	1	0	0	0	0	0	0%	10/01/23
APP2	APLICACIÓN	PRODUCCION	10	2	3	5	0	0	0	0	0	0	0%	10/01/23
APP3	APLICACIÓN	PRODUCCION	5	1	2	2	0	0	0	0	0	0	0%	10/01/23
APP4	APLICACIÓN	PRODUCCION	10	2	3	4	1	0	0	0	0	0	0%	10/01/23
APP5	APLICACIÓN	PRODUCCION	8	3	2	2	1	0	0	0	0	0	0%	10/01/23
APP6	APLICACIÓN	PRODUCCION	10	4	2	2	2	0	0	0	0	0	0%	10/01/23
SV1	SERVIDOR	PRODUCCION	10	4	2	2	2	1	1	0	0	0	5%	10/01/23
SV2	SERVIDOR	PRODUCCION	10	4	2	2	2	1	0	1	0	0	5%	10/01/23
SV3	SERVIDOR	PRODUCCION	15	5	0	5	5	1	1	0	0	0	5%	10/01/23
SV4	SERVIDOR	PRODUCCION	16	3	4	3	6	1	0	0	1	0	5%	10/01/23
SV5	SERVIDOR	PRODUCCION	12	6	3	2	1	1	1	0	0	0	5%	10/01/23
SV6	SERVIDOR	PRODUCCION	14	3	5	3	3	1	0	0	0	1	5%	10/01/23
SV7	SERVIDOR	PRODUCCION	19	5	7	5	2	1	1	0	0	0	5%	10/01/23
SV8	SERVIDOR	PRODUCCION	20	3	4	5	8	1	1	0	0	0	5%	10/01/23
SV9	SERVIDOR	PRODUCCION	15	4	2	5	4	1	0	1	0	0	5%	10/01/23
SV10	SERVIDOR	PRODUCCION	20	5	7	5	3	1	1	0	0	0	5%	10/01/23
SV11	SERVIDOR	PRODUCCION	30	10	6	6	8	2	2	0	0	0	5%	10/01/23
SV12	SERVIDOR	PRODUCCION	25	10	5	5	5	1	1	0	0	0	5%	10/01/23
SV13	SERVIDOR	DESARROLLO	30	10	6	6	8	2	2	0	0	0	5%	10/01/23
SV14	SERVIDOR	DESARROLLO	40	10	10	10	10	2	2	0	0	0	5%	10/01/23
SV15	SERVIDOR	DESARROLLO	20	5	7	5	3	1	1	0	0	0	5%	10/01/23
SV16	SERVIDOR	DESARROLLO	10	4	2	2	2	1	1	0	0	0	5%	10/01/23
APP1	APLICACIÓN	PRODUCCION	12	6	3	2	1	1	1	0	0	0	10%	11/01/23
APP2	APLICACIÓN	PRODUCCION	15	5	0	5	5	2	0	0	2	0	10%	11/01/23
APP3	APLICACIÓN	PRODUCCION	5	1	1	2	1	1	1	0	0	0	10%	11/01/23
APP4	APLICACIÓN	PRODUCCION	4	3	1	0	0	1	1	0	0	0	5%	11/01/23
APP5	APLICACIÓN	PRODUCCION	8	3	2	2	1	1	1	0	0	0	5%	11/01/23
APP6	APLICACIÓN	PRODUCCION	9	2	3	2	2	1	1	0	0	0	10%	11/01/23
SV1	SERVIDOR	PRODUCCION	15	5	0	5	5	2	0	0	2	0	15%	11/01/23
SV2	SERVIDOR	PRODUCCION	15	5	0	5	5	2	0	2	0	0	10%	11/01/23
SV3	SERVIDOR	PRODUCCION	30	10	6	6	8	3	3	0	0	0	10%	11/01/23
SV4	SERVIDOR	PRODUCCION	25	10	5	5	5	4	2	2	0	0	15%	11/01/23
SV5	SERVIDOR	PRODUCCION	40	10	10	10	10	8	8	0	0	0	20%	11/01/23
SV6	SERVIDOR	PRODUCCION	14	4	4	3	3	1	0	0	1	0	10%	11/01/23
SV7	SERVIDOR	PRODUCCION	19	5	7	5	2	4	0	4	0	0	20%	11/01/23
SV8	SERVIDOR	PRODUCCION	30	10	6	6	8	3	3	0	0	0	10%	11/01/23

ID ACTIVO	TIPO DE ACTIVO	AMBIENTE	TOTAL VULNERA	BAJO1	MEDIO2	ALTO3	CRÍTICO4	TOTAL VULNERABILIDAD	BAJO	MEDIO	ALTO	CRÍTICO	% RESOLUCIÓN	FECHA
SV11	SERVIDOR	PRODUCCION	30	10	6	6	8	6	0	3	3	0	20%	12/01/23
SV12	SERVIDOR	PRODUCCION	40	10	10	10	10	4	4	0	0	0	10%	12/01/23
SV13	SERVIDOR	DESARROLLO	30	10	6	6	8	3	1	2	0	0	10%	12/01/23
SV14	SERVIDOR	DESARROLLO	40	10	10	10	10	8	8	0	0	0	20%	12/01/23
SV15	SERVIDOR	DESARROLLO	20	3	4	5	8	4	2	2	0	0	20%	12/01/23
SV16	SERVIDOR	DESARROLLO	15	4	2	5	4	3	0	0	3	0	20%	12/01/23
APP1	APLICACIÓN	PRODUCCION	40	10	10	10	10	16	0	0	6	10	40%	01/01/24
APP2	APLICACIÓN	PRODUCCION	50	20	10	10	10	22	0	2	10	10	45%	01/01/24
APP3	APLICACIÓN	PRODUCCION	45	15	10	10	10	23	0	3	10	10	50%	01/01/24
APP4	APLICACIÓN	PRODUCCION	35	10	10	10	5	18	0	3	10	5	50%	01/01/24
APP5	APLICACIÓN	PRODUCCION	40	10	10	10	10	20	0	0	10	10	50%	01/01/24
APP6	APLICACIÓN	PRODUCCION	55	20	10	15	10	28	0	3	15	10	50%	01/01/24
SV1	SERVIDOR	PRODUCCION	80	20	20	20	20	40	0	0	20	20	50%	01/01/24
SV2	SERVIDOR	PRODUCCION	60	20	20	10	10	36	0	16	10	10	60%	01/01/24
SV3	SERVIDOR	PRODUCCION	50	20	10	10	10	30	0	10	10	10	60%	01/01/24
SV4	SERVIDOR	PRODUCCION	50	20	10	10	10	30	0	10	10	10	60%	01/01/24
SV5	SERVIDOR	PRODUCCION	70	20	20	20	10	42	0	2	20	20	60%	01/01/24
SV6	SERVIDOR	PRODUCCION	50	20	10	10	10	30	0	10	10	10	60%	01/01/24
SV7	SERVIDOR	PRODUCCION	50	20	10	10	10	30	0	10	10	10	60%	01/01/24
SV8	SERVIDOR	PRODUCCION	65	20	20	15	10	39	0	0	19	20	60%	01/01/24
SV9	SERVIDOR	PRODUCCION	50	20	10	10	10	30	0	16	10	10	60%	01/01/24
SV10	SERVIDOR	PRODUCCION	60	20	20	10	10	36	0	16	10	10	60%	01/01/24
SV11	SERVIDOR	PRODUCCION	60	20	20	10	10	36	0	16	10	10	60%	01/01/24
SV12	SERVIDOR	PRODUCCION	70	20	20	20	10	42	0	2	20	20	60%	01/01/24
SV13	SERVIDOR	DESARROLLO	50	20	10	10	10	30	0	10	10	10	60%	01/01/24
SV14	SERVIDOR	DESARROLLO	40	10	10	10	10	24	0	4	10	10	60%	01/01/24
SV15	SERVIDOR	DESARROLLO	60	20	20	10	10	36	0	16	10	10	60%	01/01/24
SV16	SERVIDOR	DESARROLLO	60	20	20	10	10	42	2	20	10	10	70%	01/01/24
APP1	APLICACIÓN	PRODUCCION	16	3	4	3	6	11	0	2	3	6	70%	02/01/24
APP2	APLICACIÓN	PRODUCCION	23	5	5	8	5	16	0	3	8	5	70%	02/01/24
APP3	APLICACIÓN	PRODUCCION	23	5	5	8	5	16	0	3	8	5	70%	02/01/24
APP4	APLICACIÓN	PRODUCCION	18	3	5	5	5	13	0	3	5	5	70%	02/01/24
APP5	APLICACIÓN	PRODUCCION	20	3	4	5	8	14	0	1	5	8	70%	02/01/24
APP6	APLICACIÓN	PRODUCCION	28	10	5	5	8	20	2	5	5	8	70%	02/01/24
SV1	SERVIDOR	PRODUCCION	40	10	10	10	10	28	0	8	10	10	70%	02/01/24

ANEXO 07: SOFTWARE DESARROLADO E IMPLEMENTADO

VULNERACONTACT





ANEXO 08: PRESUPUESTO PARA LA ELABORACIÓN DE TESIS

Tabla: Costos de Elaboración de Tesis

PRESUPUESTO PARA LA ELABORACIÓN DE TESIS			
TÍTULO: "IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE VULNERABILIDADES PARA MEJORAR LA PRODUCTIVIDAD EN LA EMPRESA CONTACTA HABILIDAD S.A.C., LIMA-2024"			
TESISTA1: FLORES HUANCA MARÍA INÉS			
TESISTA2: NUÑEZ ZEGARRA FIORELLA ARACELI			
TESISTA3: VILLEGAS PACHECO ANDREA GIULIANA			
ITEM	**PARTIDAS**	**COSTO s/.**	**COSTO $ (T. C. 4.00)**
1.0.	**REMUNERACIONES**	**6200**	**1550**
1.1.	ASESORAMIENTO	6000	1500
1.2.	OTROS	200	50
2.0.	**BIENES**	**340**	**85**
2.1.	IMPRESIONES	100	25
2.2.	PAPELERIA	100	25
2.3.	FOTOCOPIAS	80	20
2.4.	OTROS	60	15
3.0.	**SERVICIOS**	**540**	**135**
3.1.	LUZ	280	70
3.2.	MOVILIDAD	80	20
3.3.	INTERNET	180	45
	TOTAL	**7080**	**1770**

Fuente: Elaboración propia