UNIVERSIDAD ANDINA

NÉSTOR CÁCERES VELÁSQUEZ

FACULTAD DE INGENIERÍA DE SISTEMAS

ESCUELA PROFESIONAL DE INGENIERÍA EMPRESARIAL E INFORMÁTICA

OPTIMIZACIÓN DE LA SEGURIDAD EN REDES EMPRESARIALES PARA DISMINUIR RIESGOS INFORMÁTICOS EN LA EMPRESA VIRGEN DE CHAPI JULIACA 2024

TESIS PRESENTADA POR:

Bach. FIDEL APAZA QUISPE

PARA OBTENER EL TÍTULO PROFESIONAL DE:

INGENIERO EMPRESARIAL E INFORMÁTICO

JULIACA - PERÚ

2025

UNIVERSIDAD ANDINA

NÉSTOR CÁCERES VELÁSQUEZ

FACULTAD DE INGENIERÍA DE SISTEMAS

ESCUELA PROFESIONAL DE INGENIERÍA EMPRESARIAL E INFORMÁTICA

OPTIMIZACIÓN DE LA SEGURIDAD EN REDES EMPRESARIALES PARA DISMINUIR RIESGOS INFORMÁTICOS EN LA EMPRESA VIRGEN DE CHAPI JULIACA 2024

TESIS PRESENTADA POR:

Bach. FIDEL APAZA QUISPE

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO EMPRESARIAL E INFORMÁTICO

APROBADA POR EL JURADO REVISOR:

PRESIDENTE : Dr. JUAN CARLOS HERRERA MIRANDA

PRIMER MIEMBRO : Mgtr. SALVADOR TEODORO VALDIVIA CARDENAS

SEGUNDO MIEMBRO : M. Sc. JESUS ESTEBAN CASTILLO MACHACA

ASESOR DE TESIS : Dr. PAUL MAMANI TISNADO

LÍNEA DE INVESTIGACIÓN : ORGANIZACIÓN Y DIRECCIÓN DE EMPRESAS – P25

UNIVERSIDAD ANDINA "NÉSTOR CÁCERES VELÁSQUEZ"

RESOLUCIÓN DECANAL Nº 130-2025-D-FIS-UANCV

Juliaca, 30 de diciembre de 2025

VISTOS; el Expediente Nº 2025-C-1641, presentado por el señor (a) **FIDEL APAZA QUISPE,** egresado de la Escuela Profesional de Ingenieria Empresarial e Informatica, de la Facultad de Ingeniería de Sistemas, quien solicita **NOMINACIÓN DE JURADOS Y PROGRAMACIÓN DE FECHA Y HORA DE SUSTENTACIÒN.**

CONSIDERANDO:

Que, el (la) Bachiller **FIDEL APAZA QUISPE,** quien solicita **NOMINACIÓN DE JURADOS Y PROGRAMACIÓN DE FECHA Y HORA DE SUSTENTACIÒN** de la tesis titulada: **OPTIMIZACIÒN DE LA SEGURIDAD EN REDES EMPRESARIALES PARA DISMINUIR RIESGOS INFORMÀTICOS EN LA EMPRESA VIRGEN DE CHAPI JULIACA 2024,** la misma que pertenece a la línea de investigación, ORGANIZACIÓN Y DIRECCIÒN EMPRESARIAL, para optar el título profesional de INGENIERIO EMPRESARIAL E INFORMÀTICO.

Que, al haberse cumplido con los requisitos exigidos por el Reglamento Interno de Trabajo de Investigación conducente a Gados y Títulos mediante resolución 0294-2023-UANCV-CU-R y en concordancia con el dictamen de similitud.

De conformidad al Reglamento Interno de Trabajos de Investigación conducente a grafos y títulos, aprobado con resolución Nº 0294-2023-UANCV-CU-R y en mérito al art. 24, Art. 28 del reglamento, con fines de obtención de obtención de Grados Académicos y Títulos Profesionales y en uso a las atribuciones que le concede la ley Universitaria Nº 30220, Ley de creación de la UANCV Nº 23738 y modificatoria Nº 24661, y el estatuto de la UANCV, el Decano y Director de la Unidad de Investigación de la Facultad de Ingeniería de Sistemas.

RESUELVE:

ARTÍCULO PRIMERO. - APROBAR la **NOMINACION DE JURADOS,** integrado por los siguientes docentes:

- **Presidente : Dr. JUAN CARLOS HERRERA MIRANDA**
- **1er miembro : Mgtr. SALVADOR TEODORO VALDIVIA CARDENAS**
- **2do miembro : MSc. JESUS ESTEBAN CASTILLO MACHACA**

ARTÍCULO SEGUNDO.- RECONOCER como asesor de la investigación (tesis) de la Facultad de Ingeniería de Sistemas, al (a la) docente, **Dr. PAUL MAMANI TISNADO**

ARTÍCULO TERCERO.- APROBAR la **FECHA Y HORA DE SUSTENTACION DE LA TESIS** del (la) Bachiller: **FIDEL APAZA QUISPE,** del informe final de la investigación (tesis) titulado: **OPTIMIZACIÒN DE LA SEGURIDAD EN REDES EMPRESARIALES PARA DISMINUIR RIESGOS INFORMÀTICOS EN LA EMPRESA VIRGEN DE CHAPI JULIACA 2024,** para optar el título profesional de INGENIERIO EMPRESARIAL E INFORMÀTICO, de acuerdo al siguiente detalle:

- **FECHA : miercoles, 31 de diciembre de 2025**
- **HORA : 12:30:00 PM**
- **LUGAR : Sala de Docentes-FIS**

ARTÍCULO CUARTO. - DISPONER que, la Unidad de Investigación, Responsables del Comité de Investigación de la Facultad de Ingeniería de Sistemas y el Director de la Escuela profesional, Ingenieria Empresarial e Informatica, quedan encargados del cumplimiento de la presente Resolución.

Regístrese, Comuníquese y Archívese.

UNIVERSIDAD ANDINA "NÉSTOR CÁCERES VELÁSQUEZ" FACULTAD DE INGENIERÍA DE SISTEMAS DECANO JULIACA

UNIVERSIDAD ANDINA "NÉSTOR CÁCERES VELÁSQUEZ"

Dr. Juan Carlos Herrera Miranda
DECANO

UNIVERSIDAD ANDINA "NÉSTOR CÁCERES VELÁSQUEZ"

RESOLUCIÓN DECANAL Nº 097-2025-D-FIS-UANCV

Juliaca, 29 de dIciembre de 2025

VISTOS; el Expediente Nº **2025-CU-123205**, presentado por el señor (a) **FIDEL APAZA QUISPE** solicitando **CAMBIO DE ASESOR DE INVESTIGACIÒN**, el PROVEIDO Nº **57-2024**-UI-FIS-UANCV/J del Director de la Unidad de Investigación de la Facultad de Ingeniería de Sistemas, y la RESOLUCION Nº 132-2024 UI-R-D-FIS-UANCV-J, aprobación del CAMBIO DE ASESOR DEL INFORME FINAL, para optar el título profesional de INGENIERIO EMPRESARIAL E INFORMÀTICO.

CONSIDERANDO:

Que, el (la) señor (a) **FIDEL APAZA QUISPE**, ha presentado su cambio de asesor de tesis del tema de investigación titulado: **OPTIMIZACIÒN DE LA SEGURIDAD EN REDES EMPRESARIALES PARA DISMINUIR RIESGOS INFORMÀTICOS EN LA EMPRESA VIRGEN DE CHAPI JULIACA 2024**, para optar el Título Profesional de **INGENIERIO EMPRESARIAL E INFORMÀTICO.**

Que, al haberse cumplido con los requisitos exigidos por el Reglamento Interno de Trabajo de Investigación conducente a Grados y Títulos con fines de obtención de Grados Académicos y Títulos, el Director de la Unidad de Investigación de la Facultad de Ingeniería de Sistemas emitió opinión favorable de la propuesta de investigación; Expediente 2025-CU-123205, aprobando el INFORME FINAL DE LA INVESTIGACION titulado**: OPTIMIZACIÒN DE LA SEGURIDAD EN REDES EMPRESARIALES PARA DISMINUIR RIESGOS INFORMÀTICOS EN LA EMPRESA VIRGEN DE CHAPI JULIACA 2024**.

Que el Director de la Unidad de Investigación de la FIS ha tomado conocimiento que el (la) asesor (ra) Dr. JUAN BENITES NORIEGA, no tiene vínculo laboral en la Facultad de Ingeniería de Sistemas y existiendo la RESOLUCION Nº132-2024-UI-R-D-FIS-UANCV-J, aprobación del INFORME FINAL DE LA INVESTIGACIÒN.

Que es requisito indispensable contar con un asesor docente ordinario y/o contratado de la facultad de Ingeniería de Sistemas, con mínimo de cinco años de docencia, grado de doctor o magister y experiencia en la línea a investigar, o deberá estar acreditado por resolución Nº 0989-2022-UANCV-CU-R, quien asumirá como asesor del trabajo de investigación según el área de grado.

Estando, con la opinión favorable del Director de la Unidad de Investigación de la Facultad de Ingeniería de Sistemas y en concordancia con el reglamento interno de trabajos de investigación conducente a grados y títulos, aprobado con resolución Nº 0294-2023-UANCV-CU-R y en mérito al art. 25 del reglamento, con fines de obtención de obtención de Grados Académicos y Títulos Profesionales y en uso a las atribuciones que le concede la ley Universitaria Nº 30220, Ley de creación de la UANCV Nº 23738 y modificatoria Nº 24661, y el estatuto de la UANCV, el Decano y Director de la Facultad de Ingeniería de Sistemas.

RESUELVE:

ARTÍCULO PRIMERO.- APROBAR, el CAMBIO DE ASESOR DE INVESTIGACIÒN, presentada por el (la) señor (a): **FIDEL APAZA QUISPE**, para optar el Título Profesional de **INGENIERIO EMPRESARIAL E INFORMÀTICO** con el tema titulado: **OPTIMIZACIÒN DE LA SEGURIDAD EN REDES EMPRESARIALES PARA DISMINUIR RIESGOS INFORMÀTICOS EN LA EMPRESA VIRGEN DE CHAPI JULIACA 2024,** se le asigna como:

ASESOR: Dr. PAUL MAMANI TISNADO

ARTÍCULO SEGUNDO. - RECONOCER como **ASESOR DE INVESTIGACION** al (a la) docente **Dr. PAUL MAMANI TISNADO.**

ARTÍCULO TERCERO. - DISPONER que, la Unidad de Investigación, Responsables del Comité de Investigación de la Facultad de Ingeniería de Sistemas y el Director de la Escuela profesional, **INGENIERIA EMPRESARIAL E INFORMATICA**, quedan encargados del cumplimiento de la presente Resolución.

Regístrese, Comuníquese y Archívese.

UNIVERSIDAD ANDINA "NÉSTOR CÁCERES VELÁSQUEZ"
FACULTAD DE INGENIERÍA DE SISTEMAS - JULIACA - DECANO
Dr. Juan Carlos Herrera Miranda
DECANO

C.c.
Arch 2025
Interesado

RESOLUCIÓN Nº 132-2024-UI.R-D-FIS-UANCV-J

Juliaca, 05 de Julio de 2024

VISTOS:

El Expediente: 2024-CU-7798 de fecha 11 de Julio de 2025, del Bach. **FIDEL APAZA QUISPE**, quien solicita Revisión del Informe Final de la Investigación (borrador de Tesis) y el Anexo (04 o 05) "Ficha de Opinión del Informe Final de la Investigación (borrador de Tesis)" que fue revisada por el Comité de Investigación de la Facultad de Ingeniería de Sistemas, Escuela Profesional de INGENIERÍA EMPRESARIAL E INFORMATICA.

CONSIDERANDO:

Que, las Unidades de Investigación son unidades académicas que agrupan a docentes y estudiantes de diversas disciplinas, en razón del desarrollo de investigación científica, tecnológica y humanista de acuerdo al Estatuto Universitario Modificado 2020 de nuestra primera Casa Superior de Estudios.

Que, el (la) Bach. FIDEL APAZA QUISPE, quien solicita la revisión del Informe Final de la Investigación (borrador de Tesis) del tema titulada: OPTIMIZACIÓN DE LA SEGURIDAD EN REDES EMPRESARIALES PARA DISMINUIR RIESGOS INFORMÁTICOS EN LA EMPRESA VIRGEN DE CHAPI JULIACA 2024, conducente para optar el Título profesional de INGENIERO EMPRESARIAL E INFORMÁTICO.

Que, al haberse cumplido con los requisitos exigidos por el Reglamento Interno de Trabajo de Investigación Conducente a Grados y Títulos plasmado en la Resolución Nº 0294-2023-UANCV-CU-R.

Que, el Comité de Investigación emitió su opinión favorable al Informe Final de la Investigación (borrador de Tesis).

Que, el Director de la Unidad de Investigación de la Facultad de Ingeniería de Sistemas, Escuela Profesional de INGENIERÍA EMPRESARIAL E INFORMATICA, corroboro el asesoramiento en el Informe Final de la Investigación (borrador de Tesis) del ASESOR Dr. JUAN BENITES NORIEGA,

Estando, la opinión favorable del Comité de Investigación, en concordancia con el Reglamento Interno de Trabajo de Investigación Conducente a Grados y Títulos Resolución Nº 0294-2023-UANCV-CU-R, de conformidad a lo que establece la Ley Universitaria Nº 30220, Ley de Creación de la UANCV Nº 23738 y Modificatoria Nº 24661 y el Estatuto de la UANCV, que confiere facultades al Decano de la Facultad de Ingeniería de Sistemas.

SE RESUELVE:

ARTICULO PRIMERO. - APROBAR Y AUTORIZAR EL INFORME FINAL DE LA INVESTIGACIÓN (Borrador de Tesis) para la **REVISIÓN DE SIMILITUD TURNITIN**, del tema titulado: **OPTIMIZACIÓN DE LA SEGURIDAD EN REDES EMPRESARIALES PARA DISMINUIR RIESGOS INFORMÁTICOS EN LA EMPRESA VIRGEN DE CHAPI JULIACA 2024**, presentado por el (la) Bach. **FIDEL APAZA QUISPE**, para optar el Título Profesional de INGENIERO EMPRESARIAL E INFORMÁTICO, en virtud de los considerandos expuestos.

ARTICULO SEGUNDO. - RATIFICAR, como ASESOR al **Dr. JUAN BENITES NORIEGA**.

ARTICULO TERCERO. - DISPONER que la facultad, secretarias académicas y administrativas, quedan encargados del cumplimiento de la presente resolución.

Regístrese, comuníquese y archívese.

UNIVERSIDAD ANDINA "NÉSTOR CÁCERES VELÁSQUEZ" – FACULTAD DE INGENIERÍA DE SISTEMAS – DECANO – JULIACA

M.Sc. Juan Carlos Herrera Miranda
DECANO

C.c
Arch 2024
JCHM/ v1.1
Distribución: Asesor de Tesis, Interesado

RESOLUCIÓN N° 102-2024-UI.P-D-FIS-UANCV-J

Juliaca, 17 de mayo de 2024

VISTOS:

El Expediente: 2024-CU-4683 de fecha 26 de abril de 2024, del (la) Bach. **FIDEL APAZA QUISPE**; con el cual solicita Revisión de la Propuesta de Investigación y el Anexo (02 o 03) "Ficha de Opinión de la Propuesta de Investigación" que fue revisada por el Comité de Investigación de la Facultad de Ingeniería de Sistemas, Escuela Profesional de INGENIERÍA EMPRESARIAL E INFORMATICA.

CONSIDERANDO:

Que, las Unidades de Investigación son unidades académicas que agrupan a docentes y estudiantes de diversas disciplinas, en razón del desarrollo de investigación científica, tecnológica y humanista de acuerdo al Estatuto Universitario Modificado 2020 de nuestra primera Casa Superior de Estudios.

Que, el (la) Bach. FIDEL APAZA QUISPE, solicito la revisión y aprobación de la Propuesta de Investigación de la tesis titulada: OPTIMIZACIÓN DE LA SEGURIDAD EN REDES EMPRESARIALES PARA DISMINUIR RIESGOS INFORMÁTICOS EN LA EMPRESA VIRGEN DE CHAPI JULIACA 2024; conducente para optar el Título Profesional de INGENIERO EMPRESARIAL E INFORMÁTICO.

Que, al haberse cumplido con los requisitos exigidos por el Reglamento Interno de Trabajo de Investigación Conducente a Grados y Títulos plasmado en la Resolución N° 0294-2023-UANCV-CU-R.

Que, el Comité de Investigación ha emitido opinión favorable a la propuesta de investigación.

Que, el Director de la Unidad de Investigación de la Facultad de Ingeniería de Sistemas, Escuela Profesional de INGENIERÍA EMPRESARIAL E INFORMATICA, ratifico la propuesta del Asesor Dr. JUAN BENITES NORIEGA, quien debe estar acreditado y facultado para orientar y ayudar al asesorado en el proceso de elaboración del trabajo de investigación (Tesis).

Estando, la opinión favorable del comité de Investigación, en concordancia con el Reglamento Interno de Trabajo de Investigación Conducente a Grados y Títulos, Resolución N° 0294-2023-UANCV-CU-R, de conformidad a lo que establece la Ley Universitaria N° 30220, Ley de Creación de la UANCV N° 23738 y Modificatoria N° 24661 y el Estatuto de la UANCV, que confiere facultades al Decano de la Facultad de Ingeniería de Sistemas.

SE RESUELVE:

ARTÍCULO PRIMERO. - **APROBAR Y AUTORIZAR LA EJECUCIÓN DE LA PROPUESTA DE INVESTIGACIÓN**, titulada: **OPTIMIZACIÓN DE LA SEGURIDAD EN REDES EMPRESARIALES PARA DISMINUIR RIESGOS INFORMÁTICOS EN LA EMPRESA VIRGEN DE CHAPI JULIACA 2024**, presentado por el (la) Bach. **FIDEL APAZA QUISPE**, para optar el Título Profesional de INGENIERO EMPRESARIAL E INFORMÁTICO, en virtud de los considerandos expuestos.

ARTÍCULO SEGUNDO. - RECONOCER, como ASESOR al Dr. **JUAN BENITES NORIEGA**.

ARTÍCULO TERCERO. - DISPONER que la facultad, secretarias académicas y administrativas, quedan encargados del cumplimiento de la presente resolución.

Regístrese, comuníquese y archívese.

UNIVERSIDAD ANDINA "NÉSTOR CÁCERES VELÁSQUEZ"

UNIVERSIDAD ANDINA NÉSTOR CÁCERES VELÁSQUEZ FACULTAD DE INGENIERÍA DE SISTEMAS DECANO JULIACA

M.Sc. Juan Carlos Herrera Miranda
DECANO

C.c
Arch 2024
JCHM/ v1.1
Distribución: Asesor de Tesis, Interesado

FIDEL APAZA QUISPE

OPTIMIZACIÓN DE LA SEGURIDAD EN REDES EMPRESARIALES PARA DISMINUIR RIESGOS INFORMÁTICO...

TESIS DE PREGRADO

Detalles del documento

Identificador de la entrega
trn:oid:::13016:561085127

Fecha de entrega
26 feb 2026, 6:34 GMT-5

Fecha de descarga
21 abr 2026, 17:04 GMT-5

Nombre del archivo
T036_70202945_T.docx

Tamaño del archivo
5.1 MB

84 páginas

12.033 palabras

70.685 caracteres

turnitin Página 1 de 99 - Portada Identificador de la entrega trn:oid:::13016:561085127

25% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Filtrado desde el informe

- Coincidencias menores (menos de 8 palabras)

Exclusiones

- N.º de fuentes excluidas

Fuentes principales

18% Fuentes de Internet
5% Publicaciones
20% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alertas de integridad para revisión

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

Metadatos Complementarios

OPTIMIZACIÓN DE LA SEGURIDAD EN REDES EMPRESARIALES PARA DISMINUIR RIESGOS INFORMÁTICOS EN LA EMPRESA VIRGEN DE CHAPI JULIACA 2024	
Datos de autor	
Nombres y apellidos	FIDEL APAZA QUISPE
Tipo de documento de identidad	DNI
Número de documento de identidad	70202945
URL de ORCID	https://orcid.org/0009-0000-6335-8331
Datos de asesor	
Nombres y apellidos	PAUL MAMANI TISNADO
Tipo de documento de identidad	DNI
Número de documento de identidad	01314987
URL de ORCID	https://orcid.org/0000-0002-0287-7143
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	JUAN CARLOS HERRERA MIRANDA
Tipo de documento	DNI. 29606930
URL de ORCID	https://orcid.org/0000-0002-5640-400X
Miembro del jurado 1	
Nombres y apellidos	SALVADOR TEODORO VALDIVIA CARDENAS
Tipo de documento	DNI. 02383061
URL de ORCID	https://orcid.org/0009-0008-8660-8733
Miembro del jurado 2	
Nombres y apellidos	JESUS ESTEBAN CASTILLO MACHACA
Tipo de documento	DNI. 01323821
URL de ORCID	https://orcid.org/0000-0003-4595-7589

Datos de investigación	
Línea de investigación	Organización y Dirección de Empresas – P25
Grupo de investigación	No aplica.
Agencia de financiamiento	Sin financiamiento
Ubicación geográfica de la investigación	**País**: Perú **Departamento**: Puno **Provincia**: San Román **Distrito:** Juliaca EMPRESA VIRGEN DE CHAPI. **Coordenadas:** **Latitud:** -15.492475644787762, **Longitud:** -70.12251019313527 **URL Maps:** https://maps.app.goo.gl/KUHT7HkC9CB5DNrb7 
Año o rango de años en que se realizó la investigación	Noviembre 2024 – Diciembre 2025
URL de disciplinas OCDE https://concytec-pe.github.io/Peru-CRIS/vocabularios/ocde_ford.html - Librería	**Ingeniería de sistemas y comunicaciones** https://purl.org/pe-repo/ocde/ford#2.02.04 **Ingeniería de procesos** https://purl.org/pe-repo/ocde/ford#2.04.02

UNIVERSIDAD ANDINA "NÉSTOR CÁCERES VELÁSQUEZ"
DIRECCIÓN
Dr. Juan Carlos Herrera Miranda
DIRECTOR (e)
Unidad de Investigación FIS

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo FIDEL APAZA QUISPE, identificado con DNI Nro. 70202945, en mi condición de egresado de:

☒ **Escuela Profesional**

☐ **Programa de Segunda Especialidad,**

☐ **Programa de Maestría o Doctorado**

INGENIERÍA EMPRESARIAL E INFORMÁTICA

informo que he elaborado el/la ☒ **Tesis** o ☐ **Trabajo de Investigación,** ☐ **Trabajo Académico** denominada:

OPTIMIZACIÓN DE LA SEGURIDAD EN REDES EMPRESARIALES PARA DISMINUIR RIESGOS INFORMÁTICOS EN LA EMPRESA VIRGEN DE CHAPI JULIACA 2024

Asesorado por: Dr. PAUL MAMANI TISNADO

Es un tema original.

Declaro que el presente trabajo de tesis es elaborado por mi persona y **no existe plagio/copia** de ninguna naturaleza, en especial de otro documento de investigación (tesis, revista, texto, congreso, o similar) presentado por persona natural o jurídica alguna ante instituciones académicas, profesionales, de investigación o similares, en el país o en el extranjero.

Dejo constancia que las citas de otros autores han sido debidamente identificadas en el trabajo de investigación, por lo que no asumiré como suyas las opiniones vertidas por terceros, ya sea de fuentes encontradas en medios escritos, digitales o Internet.

Asimismo, ratifico que soy plenamente consciente de todo el contenido de la tesis y asumo la responsabilidad de cualquier error u omisión en el documento, así como de las connotaciones éticas y legales involucradas.

El incumplimiento de lo declarado da lugar a responsabilidad del declarante, en consecuencia; a través del presente documento asumo frente a terceros, la Universidad Andina Néstor Cáceres Velásquez y/o la Administración Pública toda responsabilidad que pueda derivarse por el trabajo final presentado. Lo señalado incluye responsabilidad pecuniaria incluido el pago de multas u otros por los daños y perjuicios que se ocasionen.

Juliaca 31 de DICIEMBRE del 2025

Firma del Asesor (obligatoria)	Firma del Estudiante (obligatoria)	Huella

DEDICATORIA

A mis queridos padres.

AGRADECIMIENTO

Me gustaría agradecer a mi familia extendida por su apoyo, ánimo y comprensión.

ÍNDICE GENERAL

CAPITULO II

MARCO TEÓRICO

CAPITULO III

METODOLOGÍA DE LA INVESTIGACIÓN

CAPITULO IV

RESULTADOS OBTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El presente proyecto de Optimización de la Seguridad en Redes Empresariales mediante la Implementación de Protocolos de Internet Inteligente, mejorando la Gestión de Amenazas en la Empresa Virgen de Chapi, Juliaca 2024, el Objetivo principal es de Optimizar las defensas cibernéticas en las redes empresariales Virgen de Chapi, Juliaca, asegurando la protección completa de la información frente a desafíos cibernéticos, y sus Objetivos Específicos es de identificar y documentar las deficiencias en los protocolos de seguridad de la red empresarial Virgen de Chapi, evaluando su impacto potencial en el riesgo de amenazas cibernéticas, también la de optimizar la protección contra amenazas cibernéticas en la red empresarial Virgen de Chapi a través de la implementación de protocolos de Internet inteligente y por ultimo identificar y documentar los obstáculos específicos de seguridad que enfrenta Virgen de Chapi en Juliaca, abordando la infraestructura tecnológica, la capacitación del personal y la evolución de amenazas cibernéticas, el diseño de Investigación propuesto es Cuasiexperimental con preprueba y posprueba; la metodología a utilizar en la fase Exploratoria (Cualitativa) mediante la Entrevistas en profundidad, análisis documental, grupos focales (opcional). Para la Fase de Desarrollo (Cuantitativa): Implementación de protocolos, monitoreo continuo, encuestas cuantitativas. La Población y Muestra para este proyecto es el Personal Virgen de Chapi, Juliaca, incluyendo responsables de seguridad, personal de TI y gerentes. Muestra estratificada para entrevistas, encuestas y posible grupo focal. Para la Técnicas de Recolección de Datos se utilizó la Entrevistas, análisis documental, implementación de protocolos, monitoreo continuo, encuestas estructuradas. Los Resultados Esperados es que la implementación de protocolos de Internet inteligente mejore significativamente la seguridad cibernética en Virgen de Chapi, reduciendo las deficiencias identificadas y fortaleciendo la protección contra amenazas. Este proyecto contribuí a la comprensión y aplicación efectiva de medidas

de seguridad en redes empresariales, brindando beneficios tangibles a la empresa Virgen de Chapi en Juliaca.

Palabras claves: Protocolos de internet Inteligentes (IPI), protocolos de Seguridad, ciberseguridad

ABSTRACT

This project to Optimize Security in Business Networks through the Implementation of Intelligent Internet Protocols, improving Threat Management in the Virgen de Chapi Company, Juliaca 2024, the main objective is to Optimize cyber defenses in Virgen de Chapi business networks. Chapi, Juliaca, ensuring complete protection of information against cyber challenges, and its Specific Objectives are to identify and document deficiencies in the security protocols of the Virgen de Chapi business network, evaluating their potential impact on the risk of cyber threats , also to optimize protection against cyber threats in the Virgen de Chapi business network through the implementation of intelligent Internet protocols and finally identify and document the specific security obstacles faced by Virgen de Chapi in Juliaca, addressing the technological infrastructure , staff training and the evolution of cyber threats, the proposed research design is Quasi-experimental with pretest and posttest; the methodology to be used in the Exploratory (Qualitative) phase through in-depth interviews, documentary analysis, focus groups (optional). For the Development Phase (Quantitative): Implementation of protocols, continuous monitoring, quantitative surveys. The Population and Sample for this project is the Virgin Personnel of Chapi, Juliaca, including security officers, IT personnel and managers. Stratified sample for interviews, surveys and possible focus group. For Data Collection Techniques, Interviews, documentary analysis, implementation of protocols, continuous monitoring, and structured surveys were used. The Expected Results are that the implementation of smart Internet protocols will significantly improve cybersecurity in Virgen de Chapi, reducing the identified deficiencies and strengthening protection against threats. This project will contribute to the understanding and effective application of security measures in business networks, providing tangible benefits to the Virgen de Chapi company in Juliaca.

Keywords: Intelligent Internet Protocols (IPI), Security protocols, cybersecurity

INTRODUCCIÓN

En la era digital, la información se ha convertido en uno de los activos más valiosos de las empresas, especialmente de aquellas dedicadas al servicio de entrega de carga a nivel nacional como Virgin de Chapi en Juliaca. La disponibilidad y la seguridad de los datos son fundamentales para asegurar la eficacia de las operaciones y satisfacción del cliente. Con un aumento en la infraestructura tecnológica, la complejidad de las amenazas cibernéticas se dispara. Se crea un reto crítico: cómo proteger la integridad, confidencialidad y disponibilidad de la información contra riesgos informáticos crecientemente sofisticados.

En la actualidad, Virgin de Chapi enfrenta un riesgo creciente de seguridad cibernéticos. La infraestructura actual de protección de la red de datos es inadecuada para proteger el sistema contra amenazas y vulnerabilidades. En consecuencia, puede acarrear una comprometida integridad y pérdida total de los datos almacenados en la empresa. Además, estas amenazas pueden repercutir en el rendimiento empresarial de la empresa y pérdidas monetarias significativas. Para abordar estas preocupaciones crecientes, se establecerán medidas preventivas que aseguren la protección integral de la red de datos comerciales.

Por consiguiente, esta investigación busca garantizar la protección de datos y la seguridad informático mediante la reducción del riesgo de helpers de assistance y la efectividad de la implementación de la red. Para lo cual se proponen los siguientes tres objetivos: Obj negocio: Identificar los posibles puntos vulnerables en la red empresarial mediante la descubierta de debilidades en la infraestructura de la red empresarial. Obj helper: Implementar medidas de

seguridad mejoradas en la red empresarial, aplicando las medidas en dos redes comerciales bajo estudio. Obj resultados: Definir el plan de acción confiable para asegurar que las medidas se aplicarán en el futuro.

Los factores clave detrás de la justificación para este proyecto incluyen. En el mundo digital de hoy, la protección contra amenazas cibernéticas en desarrollo es un requisito previo para la supervivencia y el desarrollo de una empresa. La instalación de protocolos más fuertes posicionaría a Virgen de Chapi en la cima en cuanto a las medidas de protección, protegiendo sus operaciones y su relación con los clientes. Además, en el mundo globalizado, el cumplimiento de los estándares y regulaciones internacionales, nacionales y regionales es crucial. Una optimización de la ciberseguridad aseguraría que la organización no se quede atrás en la puntuación, otorgándole una ventaja competitiva. Como medida preventiva, cualquier mejora en la gestión de las amenazas cibernéticas da a la empresa la capacidad de responder con eficacia al desastre, reduciendo el tiempo de inactividad y protegiendo los activos. Finalmente, a través de esta iniciativa, en la que se desarrollará un ejemplo de práctica, la misma contribuirá a involucrar a otras empresas en la región de Juliaca. A medida que otras empresas adoptan nuevas tecnologías y prácticas óptimas, la región se volverá tecnológicamente más avanzada. En resumen, este proyecto de investigación se realizará para mejorar la ciberseguridad en la red de la empresa, atendiendo a las preocupaciones actuales en el sistema de red de Virgen de Chapi y a las futuras vulnerabilidades. Por lo tanto, es fundamental acudir de manera integral para lo que incluye experiencias completas, medidas adicionales put en su lugar y un diseño de acción sostenible, con el objetivo de garantizar la protección total de la información y elevando la empresa a la competencia competitiva.

CAPITULO I

ASPECTOS GENERALES

1.1. Planteamiento del Problema

En la actualidad, la empresa Virgen de Chapi en Juliaca enfrenta desafíos críticos en términos de seguridad cibernética en sus redes empresariales. A medida que la infraestructura tecnológica se expande y evoluciona, la complejidad de las amenazas cibernéticas también aumenta, poniendo en riesgo la integridad, confidencialidad y disponibilidad de la información vital para las operaciones comerciales.

La evaluación actual de las redes empresariales Virgen de Chapi revela la presencia de deficiencias en los protocolos de seguridad existentes, lo que ha contribuido a la exposición a amenazas cibernéticas. Las vulnerabilidades identificadas representan un riesgo significativo para la empresa, especialmente en un entorno donde las competencias internacionales, nacionales y regionales en seguridad cibernética están en constante evolución.

Competencias a nivel internacional, nacional y regional

En primer lugar, a nivel internacional, el sector empresarial es un juego altamente competitivo, en el que las mejores prácticas de seguridad cibernética son un factor determinante para la confianza del cliente y la integridad de la marca. A nivel nacional, las regulaciones y los estándares de seguridad comprometen la necesidad de los de los

negocios y su reputación en el mercado local. Por último, a nivel regional, las dinámicas de seguridad también difieren substancialmente, por lo que es imprescindible tomar en cuenta los desafíos específicos.

En consecuencia, la capacidad de respuesta frente a incidentes de seguridad se ve comprometida por la ineficiencia en la gestión de amenazas cibernéticas, lo que afecta directamente la posición competitiva de Virgen de Chapi en estos contextos. Las soluciones oportuna y efectiva de incidentes son un aspecto crítico que requiere una mejora sustantiva para la competitividad en un entorno empresarial en rápido cambio y competitivo. Las infraestructuras tecnológicas diferentes y evolutivas y la adaptación al tiempo con el aumento de las amenazas cibernéticas presentan desafíos adicionales. Por lo tanto, la implementación de la implementación de protocolos de Internet inteligente surge como una solución prometedora, dada su viabilidad en los casos similares.

Sin embargo, ya que el nivel de eficacia y proporciona miento de la implementación para el caso también deben ser garantizados, también se requiere una evaluación detallada con la guía de competencias y estándares internacionales, nacionales y regionales. Por lo tanto, hay una necesidad inmediata de una propuesta y una investigación enfocada a la implementación de protocolos de Internet inteligente para mejorar la seguridad de información de red del negocio de Virgen de Chapi en Juliaca. Asegurará la protección integral de los sistemas de información de las redes de negocio alineado con los estándares y competencias internacionales, nacionales y regionales y hará que Virgen de Chapi sea empresa incluyente, confiable y competitiva en constante escenario de negocio actual.

Por consiguiente, se optó a realizar las siguientes preguntas.

1.1.1. Problema General

¿Cómo mejorar eficazmente la seguridad en las redes empresariales de la Empresa Virgen de Chapi en Juliaca, considerando los riesgos informáticos existentes y la necesidad de proteger la integridad, confidencialidad y disponibilidad de la información?

1.1.2. Problemas Específicos

a) ¿Cuáles son las principales vulnerabilidades y debilidades en la infraestructura de red de la Empresa Virgen de Chapi que podrían exponerla a riesgos informáticos?

b) ¿Qué medidas de seguridad adicionales pueden implementarse en las redes empresariales de la Empresa Virgen de Chapi para mitigar los riesgos informáticos identificados y fortalecer la protección de la información?

c) ¿Cómo puede garantizarse la eficacia y la sostenibilidad de las medidas de seguridad implementadas en las redes empresariales de la Empresa Virgen de Chapi para mantener una protección continua contra los riesgos informáticos en el futuro?

1.2. Objetivos

1.2.1. Objetivo General

Optimizar la seguridad en las redes empresariales de la Empresa Virgen de Chapi en Juliaca para reducir los riesgos informáticos y garantizar la protección integral de la información.

ANÁLISIS DE LA SEGURIDAD DE DATOS EN TRANSACCIONES PARA DISMINUIR EL RIESGO DE PÉRDIDA DE INFORMACIÓN Y SOLUCIONES EN LA EMPRESA CARGO LOS ANDES JULIACA 2023

1.2.2. Objetivos Específicos

a) Identificar las principales vulnerabilidades y debilidades en la infraestructura de red de la Empresa Virgen de Chapi mediante un análisis exhaustivo de su seguridad informática.

b) Implementar medidas de seguridad adicionales en las redes empresariales de la Empresa Virgen de Chapi, enfocadas en mitigar las vulnerabilidades identificadas y fortalecer la protección contra riesgos informáticos.

c) Establecer un plan de acción sostenible para garantizar la eficacia a largo plazo de las medidas de seguridad implementadas, incluyendo la capacitación del personal, la actualización continua de los sistemas y la evaluación periódica de la infraestructura de red.

1.3. Justificación

La realización de este proyecto de investigación sobre la "Optimización de la seguridad en redes empresariales para disminuir riesgos informáticos en la empresa vírgenes de Chapi Juliaca 2024" se fundamenta en la necesidad crítica de abordar las crecientes amenazas cibernéticas y fortalecer la postura de seguridad de la empresa en un entorno empresarial altamente competitivo y dinámico.

1.3.1. Protección ante Amenazas Cibernéticas Evolutivas:

Las amenazas cibernéticas evolucionan constantemente, adaptándose a nuevas tecnologías y estrategias de seguridad. La implementación de protocolos de Internet inteligente permitirá a Virgen de Chapi estar a la vanguardia de las medidas de seguridad, asegurando la protección contra amenazas emergentes y mitigando riesgos potenciales.

a. **Cumplimiento de Estándares y Normativas Internacionales, Nacionales y Regionales:** La empresa opera en un entorno global, nacional y regional, y está sujeta a regulaciones específicas en materia de seguridad cibernética. La optimización de la seguridad mediante protocolos inteligentes garantizará el cumplimiento de estándares internacionales y nacionales, contribuyendo a la confianza del cliente y a la reputación de la empresa.

1.3.2. Competitividad Empresarial:

La competitividad empresarial en el ámbito nacional e internacional depende cada vez más de la capacidad de garantizar la seguridad de la

información. La implementación exitosa de protocolos de Internet inteligente fortalecerá la posición de Virgen de Chapi en el mercado, asegurando la confidencialidad, integridad y disponibilidad de datos críticos.

a. **Eficiencia en la Gestión de Amenazas:** La mejora en la gestión de amenazas cibernéticas permitirá a Virgen de Chapi responder de manera más eficiente ante posibles incidentes, minimizando el tiempo de inactividad y protegiendo los activos digitales. Esto contribuirá a la continuidad operativa y a la reducción de costos asociados a incidentes de seguridad.
b. **Resiliencia ante Ataques y Vulnerabilidades Actuales:** La evaluación de la infraestructura actual ha identificado deficiencias y vulnerabilidades en los protocolos de seguridad existentes. La implementación de protocolos de Internet inteligente permitirá abordar estas debilidades, fortaleciendo la resiliencia de las redes empresariales de Virgen de Chapi ante posibles ataques y riesgos.
c. **Contribución al Desarrollo Tecnológico Regional:** El proyecto no solo beneficiará a Virgen de Chapi, sino que también contribuirá al desarrollo tecnológico en la región de Juliaca. La adopción de tecnologías avanzadas y prácticas de seguridad cibernética establecerá un precedente para otras empresas en la región, fomentando la adopción de medidas de seguridad más sólidas.

Alineación con Objetivos Estratégicos de Virgen de Chapi: La seguridad cibernética se ha convertido en un pilar estratégico para la continuidad y el crecimiento de las organizaciones. La implementación de protocolos de Internet inteligente se alinea directamente con los objetivos estratégicos de Virgen de Chapi, asegurando la integridad de sus operaciones y la confianza de sus partes interesadas

1.4. Hipótesis

1.4.1. Hipótesis General

El mejorar la seguridad en las redes empresariales de la Empresa Virgen de Chapi en Juliaca reducirá significativamente los riesgos informáticos y garantizará la protección integral de la información.

1.4.2. Hipótesis Especificas

a) La identificación y mitigación de las principales vulnerabilidades en la infraestructura de red de la Empresa Virgen de Chapi resultará en una disminución de los incidentes de seguridad informática.

b) La implementación de medidas adicionales de seguridad en las redes empresariales de la Empresa Virgen de Chapi resultará en una mejora significativa en la protección contra riesgos informáticos, como intrusiones, malware y fugas de datos.

c) El establecimiento de un plan de acción sostenible para mantener y actualizar continuamente las medidas de seguridad en las redes empresariales de la Empresa Virgen de Chapi resultará en una protección a largo plazo contra amenazas informáticas emergentes y en la preservación de la integridad, confidencialidad y disponibilidad de la información.

1.5. Variables

Variable Independiente:

Seguridad en redes empresariales: Esta variable independiente representa la acción específica que llevarás a cabo en tu investigación.

Variable Dependiente:

Riesgos informáticos: Esta variable dependiente refleja el resultado que se espera obtener como consecuencia de la implementación de los protocolos.

1.6. Operacionalización de variables e indicadores

Tabla 1

Operacionalización de variables

Variables	Dimensión	Indicadores	Instrumentos de Investigación
Variable Independiente Seguridad en redes empresariales	*Efectividad de las medidas de seguridad*	*Actualización de software y hardware.* *Implementación de firewalls y sistemas de detección de intrusiones.* *-Políticas de acceso y control de usuarios*	- Entrevista -Validación -Encuesta
Variable Dependiente. Riesgos informáticos	*Nivel de exposición a riesgos*	*-Vulnerabilidades identificadas.* *- Incidentes de seguridad reportados.* *- Evaluación de la seguridad de la red*	-Encuesta -Observación -Entrevista

CAPITULO II

MARCO TEÓRICO

2.1. Antecedentes de la Investigación

2.1.1. Antecedentes Internacionales

(Tixe Paucar, 2022), Diseño de una iWAN : diseño de una red iWAN empresarial. en sus tesis, El presente Trabajo de Integración Curricular está basado en la creación de una red empresarial inteligente WAN iWAN, implementando Cisco Performance Routing "Cisco PfR" y Dynamic Multipoint VPN "DMVPN". Dado el enrutamiento entre complejo, especialmente con la gran cantidad de rutas a través de las cuales un paquete debe viajar antes de llegar destino final, este diseño busca optimizar el ancho de banda, reducir el costo de en operación de las WANs, sin comprometer la seguridad, la confiabilidad o el desempeño de las redes. El primer capítulo contiene un estudio en detalle de las tecnologías involucradas en el diseño de la red iWAN empresarial. El segundo capítulo examina DMVPN y dos modelos de diseño. Cisco PfR. Se estudia Cisco PfR, que también presenta una arquitectura DMVPN es una solución suministrada por Cisco Velázquez.ii arquitectura de LAN mejora la entrega de aplicaciones. DMVPN añade amplia frontera para configurar las granjas WAN. monitoreo de red del rendimiento del paquete decisión de reenvío. el tercer capítulo es sobre el diseño concreto de la red iWAN empresarial. Incluye la evaluación de las diversas fases de diseño y las respectivas configuraciones, así como un resultado análisis y estudios en el cuarto y último capítulo y dedicatoria.

(Montaña Sierra & Daza Tibocha, 2018), Por lo tanto, sigue realizándolas en tu tesis. ". En este se encuentra el Este documento detalla el proceso de planificación y ejecución de un proyecto de grado basado en la necesidad de diseñar e implementar un sistema de detección de anomalías de red a través del análisis avanzado de logs. El software deberá permitir la utilización de los recursos tecnológicos existentes para llevar a cabo el análisis. La propuesta implica una labor, un trabajo especial sobre los logs generados por cada dispositivo que se conecta a la red corporativa. De este modo, las pymes de varios sectores tendrán una protección continua contra las amenazas recurrentes de las redes e Internet. Debo agregar que esta capacidad no solo mejora la seguridad informática, sino que también hace que las corporaciones estén preparadas para detectar y reaccionar rápidamente a cualquier amenaza que pueda dañar sus inversiones. También se quiere mejorar la apariencia y el control sobre las redes de datos, así como desarrollar medidas de contrarresto en una visión defensiva de los posibles ataques a infraestructuras trascendentes. La sofisticación de los ciberdelincuentes nacionales e internacionales, por un lado, exige la apropiación de hechos consumados de grabaciones engañosas, extorsión fraudulencia, entre otros; por otro, constituye una amenaza constante para los usuarios y organizaciones. Por lo tanto, un ataque puede propagarse y tener consecuencias para la estabilidad del país, la integridad corporativa, la economía nacional, y la administración estatal más importante. Como resultado, es necesario establecer medidas preventivas y correctivas para proteger continuar la integridad de los sistemas tecnológicos.

(Choez Cajamarca & Benites Barreiro, 2015), En la tesis, en cuanto a "Auditoría de seguridad en redes inalámbricas" es identificar vulnerabilidades en redes inalámbricas e implementar un modelo de seguridad que las mitigue, describir la metodología para pruebas de penetración, y presentar diferentes modelos de seguridad personal y empresarial. Los clientes se autenticaron en el servidor con un certificado

digital en vez de una contraseña. Esta implementación eliminó las desventajas de usar contraseñas sencillas y débiles, visibles o robadas. El cliente verificaba que el servidor enlazado era el correcto. La configuración requería un certificado de la empresa para que el cliente se conectara a un servidor, ya que no había forma de verificar que se conectara a un servidor falso. El cortafuegos controlaba el acceso de clientes inalámbricos a recursos. Por lo tanto, aunque la seguridad de la red inalámbrica se viera comprometida, los recursos expuestos a la exposición del atacante serían limitados.

2.1.2. Antecedentes nacionales

(Chara Conocc & San Martin Soria, 2022), Como se observó en la monografía de diploma "Diseño de una gestión centralizada y automatización de la red lan utilizando la solución cisco SD-Access en una empresa de aeronavegación", En la actualidad, se están implementando varias soluciones SDN, tanto de código abierto como licenciado, que proporcionan el control completo de la LAN. Entonces, la tarea principal de este proyecto es que, como se mencionó anteriormente, esta solución SDN es necesaria no para reemplazar la red gestionada desde el punto de vista del procesamiento de paquetes, sino una infraestructura de red que proporciona servicios para administradores de redes, como la administración. La tesis en su conjunto tiene como objetivo implementar la solución SDN de la LAN del operador de aeronaves. La necesidad de resolver el problema procede de la idea de proporcionar a un administrador de red un acceso centralizado y automatizado a los medios de LAN de los empleados, lo que permite a un administrador de red encontrar más rápidamente los problemas y le permite garantizar un acceso seguro a ellos. Por lo tanto, el propósito del trabajo era seleccionar la solución SDN. Como resultado, se eligió la solución de red Cisco SD-Access, ya que, como resultado del estudio previo, se vio que la solución tiene una fuente de soporte y una política interna para el desarrollo y la seguridad. Finalmente, en el n. ° 5 se demostró cómo se implementa la solución y para qué hardware se seleccionaron los dispositivos. Los resultados de la implementación se presentan en n. ° 6, donde se

asegura que la administración de la LAN empresarial sea eficiente. Por lo tanto, se puede decir que la implementación futura y el estudio del software SDN para automatizar LAN en empresas deberían estudiarse, ya que la solución permitirá la automatización de redes en más empresas medios que pueden proporcionar el acceso seguro necesario de redes internas.

(Ramos Huayhua, 2019), En mi tesis titulada "Desarrollo de una plataforma para monitorear y optimizar la red corporativa de una mina", afirmo que vivimos en una era muy marcada por la innovación tecnológica continua, y la evolución y los cambios son mucho más prominentes. Cada día aportamos nuevos dispositivos a nuestras redes corporativas, ya sea en un entorno hogareño, comercial o empresarial. Hay tantos dispositivos de red, y a menos que se gestionen de manera adecuada, tendrán consecuencias letales para la empresa. Por tanto, los mecanismos de transporte/enrutamiento, la supervisión de redes y el acceso son muy importantes. La red está saturada y hay una enorme cantidad de dispositivos conectados. Esto puede llevar a fallas de red, retrasos o mal funcionamiento que interrumpen el ritmo operacional del equipo y ponen en peligro la seguridad empresarial. Para enfrentar estos problemas y evitar fallas en la red LAN, se asignan mecanismos, protocolos y plataformas a los datos que optimizan y monitorean los demás dispositivos conectados. Esto pudo facilitar un proceso de control efectivo que optimice el rendimiento general. El estudio identifica los problemas y aplica soluciones de manera gradual en varias áreas.

(Bohorquez Zumaeta, 2022), En el presente trabajo académico bajo el título "Simulación de una red VLAN para la optimización del rendimiento de la comunicación de datos en las Redes Ópticas, Tacna – 2022", se ha propuesto como objetivo general de la investigación la obtención de la mejora de las comunicaciones de datos en la empresa Optical Network en la localidad de Tacna, el mismo que se logra en forma de un cuidadoso diseño y simulación de un modelo de cableado estructurado que permitirá la maximización de la eficiencia en el desarrollo y alcance de la información. Para poder

cumplir el objetivo mencionado líneas arriba de la manera más certera posible, se ha implementado un enfoque de tipo cuantitativo el cual ha implicado la realización de un tipo de investigación específico de tipo aplicada, con un nivel explicativo, asimismo, se ha empleando un diseño de tipo investigación pre-experimental la decisión tomada en la elección justificada en el hecho de la implementación de un espacio fijo de tiempo entre PreTest y PosTest a fin de poder censar de forma adecuada la variable independiente. La población estuvo conformada por 30 registros de datos que fueron evaluados y medidos con la Ficha de recojo de información, se aplicó el instrumento de medición en la antes mencionada Cisco Packet Tracer en simulación de red el trabajo llegó a la conclusión final de que, la implementación de una simulación de red VLAN, realiza de manera efectiva no solo la mejora si no el mejoramiento del rendimiento en la comunicación de datos en las redes ópticas en Tacna 2022, esta mejora se ha comprobado a través de la validación de la hipótesis planteada al inicio del presente trabajo académico.

2.2. Marco teórico

2.2.1. Definición de Conceptos fundamentales de seguridad en redes:

La seguridad en redes empresariales es fundamental para proteger la confidencialidad, disponibilidad e integridad de los recursos digitales en las organizaciones. Algunos conceptos clave relacionados con la seguridad en redes empresariales incluyen:

1) **Detección** de intrusiones: Es la capacidad de un sistema de detectar y prevenir ataques maliciosos en la red. Un ejemplo de herramienta para la detección de intrusiones es Suricata, que ha demostrado ser eficiente en la detección de intrusiones mediante el análisis basado en firmas
2) **Solución de ciber-seguridad perimetral**: Un sistema que protege todo el tráfico de entrada y salida de las redes empresariales, intercambia información de

seguridad con otras entidades y contrarresta rápidamente las amenazas que afectan al país

3) **Protección del acceso privilegiado:** La configuración de cuentas y privilegios de administración en las redes empresariales es crucial para mantener la seguridad y evitar que los atacantes comprometan el sistema

4) **Control algorítmico:** La dirección algorítmica de las redes empresariales, plataformas digitales y otros tipos de empresas está incrementando las posibilidades de externalización productiva. La empresa principal debe controlar la prestación de servicios de la contratista mediante el aumento de las tecnologías de vigilancia y los algoritmos

5) **Comités de seguridad intercontratas:** Una forma original de organización, representación e intervención sindical supraempresarial que busca garantizar la seguridad en redes empresariales

2.2.2. Solución de ciber-seguridad perimetral para redes de datos empresariales.

Los últimos años han traído condiciones exigentes y riesgos crecientes y amenazas a la red. La seguridad de red se ve complicada por la diversidad de dispositivos en las empresas y la falta de personal especializado. Una solución de software y hardware específica para la seguridad del perímetro del sistema desarrollado, crea la capacidad de movimiento para el tráfico de red de la empresa y la información sobre amenazas, lo que aumenta la protección de los datos y los activos. También, esta solución permite una protección más eficaz contra las amenazas al país. Combina enrutamiento, filtrado de paquetes, prevención de intrusos, análisis de contenido y detección automática de malware para administrar la seguridad informática y también proporciona información sobre los atacantes y el tipo de ataques a las demás soluciones. El resultado es que se protege más rápidamente contra los atacantes y se dan mejores protecciones a las infraestructuras tecnológicas del país, (Cervantes & Hechavarría, 2018)

2.2.3. Principales riesgos de seguridad en redes empresariales

Los principales riesgos de seguridad en redes empresariales incluyen:

1) Intrusiones: Los atacantes pueden infiltrarse en las redes empresariales y robar, modificar o destruir información confidencial, lo que puede tener consecuencias financieras y legales para la empresa. (Perdigón, 2022)
2) Malware: Los programas maliciosos, como virus, malware y ransomware, pueden infectar los sistemas de la empresa y causar daños, interrupción del funcionamiento o pérdida de datos (Hernández Cervantes & Chamizo Hechavarría, 2018)
3) Phishing y fraude: Los atacantes pueden enviar correos electrónicos o mensajes falsificados que parecen ser de una entidad legítima, con el objetivo de obtener información personal o financiera de los empleados (Hernández Salazar, Pérez Jasso, Pérez Perdomo, & Morales Hechavarria, 2018)
4) Acceso no autorizado: Los empleados o personas externas pueden acceder no autorizadamente a sistemas o datos sensibles, lo que puede resultar en la pérdida de información confidencial o el compromiso de la integridad de los sistemas (Hernández Cervantes & Chamizo Hechavarría, 2018)
5) Denegación de servicios: Los atacantes pueden intentar hacer que los sistemas de la empresa no estén disponibles, lo que puede afectar la productividad y el funcionamiento de la empresa (Perdigón, 2022)
6) Exfiltración de datos: Los atacantes pueden robar datos sensibles de la empresa, como información de clientes, empleados o financieros, lo que puede dañar la reputación de la empresa y violar las regulaciones de protección de datos (Hernández Salazar, Pérez Jasso, Pérez Perdomo, & Morales Hechavarria, 2018)
7) Compromiso de dispositivos: Los dispositivos móviles y otros dispositivos conectados a la red empresarial pueden ser objetivo de ataques, lo que puede

resultar en la infiltración de la red y la pérdida de información confidencial (Hernández Salazar, Pérez Jasso, Pérez Perdomo, & Morales Hechavarria, 2018)

8) Ciberataques: Los ciberataques son ataques de gran envergadura que pueden afectar a múltiples empresas y sistemas a la vez, lo que puede causar pérdidas económicas y afectar la reputación de la empresa (Perdigón, 2022)

Como estudiante de ingeniería empresarial e informática, es importante estar al tanto de estos riesgos de seguridad en redes empresariales y conocer las tecnologías y prácticas de seguridad que pueden ayudar a prevenir y mitigar estos riesgos.

2.2.4. Protocolos de seguridad

Los protocolos de seguridad estándar más comunes en el ámbito de las redes empresariales incluyen IPsec (Protocolo de Seguridad de Internet) y SSL (Capa de Conexión Segura). Estos protocolos son ampliamente utilizados para garantizar la transmisión segura de datos en diversos contextos. Por ejemplo, un estudio evaluó la transmisión segura de imágenes diagnósticas en teleradiología utilizando el estándar DICOM, comparando los protocolos IPsec y SSL (Rosero Lugo, Acuña, & García, 2011)

Un trabajo separado fue la conceptualización y creación de un laboratorio de pruebas basado en la tecnología Smart Home. SE implementa utilizando el protocolo Z-Wave de bajo nivel de radio y el estándar 802.11. La tecnología de los elementos permite una comunicación perfecta y segura con dispositivos y módulos específicos, (Serrano, Ortiz Mata, & Rea Sánchez, 2021)

Además, se ha investigado la efectividad de las políticas de seguridad y cifrado de los protocolos H.323 y SIP con SSL para redes VoIP (Barriga & Gerardo, 2019)

Estos ejemplos ilustran la importancia y la aplicación de protocolos de seguridad estándar en diferentes contextos de redes empresariales.

2.2.5. Eficiencia en la Gestión de Amenazas Cibernéticas

Hoy en día, la eficiencia en la gestión de las amenazas cibernéticas es un tema crucial debido a la cantidad de riesgos y vulnerabilidades en línea. Para mejorar la eficiencia en la gestión de las amenazas cibernéticas, hay varias herramientas y técnicas disponibles como la implementación de los protocolos estándar de seguridad, auditoría de seguridad, capacitación de empleados sobre seguridad informática, medidas de seguridad física, entre otras. Algunos de los protocolos de seguridad estándar comunes en el ámbito de las redes empresariales son IPsec y SSL, por ejemplo. Herramientas de monitoreo e identificación de amenazas, como firewalls, sistemas de detección de intrusiones y software antivirus también son muy importantes. Asimismo, la identificación y evaluación del riesgo, mitigación y pruebas regulares de seguridad también forman parte de la gestión de amenazas cibernéticas. En definitiva, la seguridad y protección de los sistemas y datos empresariales requieren una combinación de varias herramientas, técnicas y prácticas.

2.3. Marco conceptual

a) Triada de Seguridad de la Información:

La Triada de Seguridad de la Información es un concepto central en la seguridad cibernética que engloba tres principios fundamentales: confidencialidad, integridad y disponibilidad. Estos principios representan los pilares esenciales para el diseño y mantenimiento de sistemas seguros y protegen la información crítica de una organización. (Volpano, Smith, & Irvine, 1996)

***b)* Analizar Modelo AAA (Autenticación, Autorización y Auditoría):**

El Modelo AAA, que engloba Autenticación, Autorización y Auditoría, es un marco crucial en seguridad informática que define tres aspectos esenciales en la gestión del acceso a sistemas y datos. (Denning Dorothy, 1986)

c) Principios de Seguridad de Red: Segmentación de Redes

El principio de segmentación de redes es una estrategia fundamental en seguridad de la red que implica la división de una infraestructura de red en segmentos más pequeños e independientes. Este enfoque tiene como objetivo limitar el alcance de posibles compromisos, de modo que, incluso si un segmento se ve afectado, los demás permanezcan resguardados (Volpano, Smith, & Irvine, 1996)

d) Teoría del Ciclo de Vida de la Seguridad:

La Teoría del Ciclo de Vida de la Seguridad es un enfoque estratégico que aborda la seguridad de la información a lo largo de las diferentes etapas de desarrollo y operación de sistemas. Este modelo reconoce que la seguridad no es un aspecto estático, sino un proceso dinámico que requiere planificación, implementación y mejora continua. (Anderson, 2019).

e) Defensa en Profundidad:

La Defensa en Profundidad es un enfoque estratégico en seguridad informática que busca aumentar la resiliencia de un sistema mediante la implementación de múltiples capas de seguridad. Este modelo reconoce que ninguna medida de seguridad única puede proporcionar una protección completa y, por lo tanto, busca establecer barreras consecutivas para mitigar diversas amenazas. (Volpano, Smith, & Irvine, 1996)

f) Modelo de Responsabilidad Compartida:

El Modelo de Responsabilidad Compartida es un enfoque en seguridad cibernética que reconoce que tanto los usuarios como los administradores comparten la responsabilidad de garantizar la protección de la información y los recursos. Este modelo establece claramente las funciones y expectativas de cada parte involucrada en la seguridad de un sistema. (Denning Dorothy, 1986)

g) Cumplimiento de Normativas y Estándares:

El Cumplimiento de Normativas y Estándares en seguridad cibernética se refiere a la adhesión a regulaciones específicas y la implementación de prácticas que aseguren que una organización cumple con requisitos legales y estándares de

seguridad reconocidos. Este enfoque garantiza que las operaciones de la organización estén alineadas con las expectativas y normas establecidas. (Anderson, 2019)

h) ***GDPR, HIPAA, ISO 27001***:

El cumplimiento de normativas y estándares implica la alineación con regulaciones como el Reglamento General de Protección de Datos (GDPR), la Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA) y normas como ISO 27001. Estos marcos proporcionan directrices específicas para garantizar la seguridad de la información. (Denning Dorothy, 1986)

CAPITULO III

METODOLOGÍA DE LA INVESTIGACIÓN

3.1. Diseño de la investigación

Dado que esta investigación busco optimizar las defensas cibernéticas en las redes empresariales de Virgen de Chapi, Juliaca, para asegurar de manera completa la protección de la información frente a desafíos cibernéticos, el diseño de investigación podría incorporar un enfoque mixto que incluya elementos de investigación exploratoria y de desarrollo. Los cuales se muestran a continuación:

A. Fase Exploratoria: Investigación Cualitativa

Métodos:

Entrevistas con personal de Virgen de Chapi para comprender la infraestructura tecnológica, desafíos de seguridad y capacitación del personal.

Análisis documental de políticas de seguridad existentes y registros de incidentes de seguridad.

Justificación:

Autores como (Creswell, 2014) abogan por la investigación cualitativa para explorar en profundidad fenómenos complejos y obtener perspectivas contextualizadas.

B. *Fase de Desarrollo: Investigación de Diseño*

Métodos:

Implementación de protocolos de Internet inteligente.

Evaluación continua de la efectividad de las medidas implementadas.

Justificación:

Según (Hevner, 2004)), la investigación de diseño se centra en crear soluciones prácticas para problemas del mundo real.

3.1.1. Tipo de investigación

Para esta investigación se utilizó la **investigación exploratoria** ya que la fase exploratoria te permitirá entender la situación actual de la seguridad cibernética en la empresa Virgen de Chapi, esto permitió identificar las deficiencias en los protocolos de seguridad y comprender los desafíos específicos que enfrenta la organización. Autores como (Creswell, 2014) destacan que la investigación exploratoria es esencial para adquirir una comprensión profunda del contexto antes de desarrollar soluciones.

3.2. Metodología de la investigación

Dado que esta tesis implica una investigación combinada de aspectos exploratorios y de desarrollo, una metodología mixta viene hacer la más apropiada. Aquí presentamos una metodología de investigación que incorpora elementos cualitativos y cuantitativos:

A. Fase Exploratoria: Investigación Cualitativa

a. Entrevistas en Profundidad: Realiza entrevistas con el personal clave de Virgen de Chapi, incluyendo responsables de seguridad, personal de TI y gerentes, para obtener perspectivas detalladas sobre la infraestructura tecnológica, desafíos de seguridad y capacitación del personal.

b. Análisis Documental: Examina políticas de seguridad existentes, informes de incidentes de seguridad y otros documentos relevantes para comprender el contexto y las deficiencias actuales.

c***. Grupos Focales:*** Organiza grupos focales con empleados de diferentes niveles para explorar percepciones adicionales sobre la seguridad y posibles áreas de mejora.

B. Fase de Desarrollo: Investigación de Diseño

a. Implementación de Protocolos de Internet Inteligente: Implementa los protocolos de Internet inteligente identificados durante la fase exploratoria para fortalecer la seguridad.

b. Monitoreo Continuo: Establece un sistema de monitoreo continuo para evaluar la efectividad de los nuevos protocolos en tiempo real.

c. Encuestas Cuantitativas**:** Diseña encuestas estructuradas para recopilar datos cuantitativos sobre la percepción del personal sobre la efectividad de las nuevas medidas de seguridad.

C. Análisis Integrado: Enfoque Mixto

a. Integración de Datos: Combina los datos cualitativos (resultados de entrevistas y grupos focales) con los datos cuantitativos (resultados de encuestas y datos de monitoreo) para obtener una comprensión completa.

b. Análisis Estadístico: Realiza análisis estadísticos descriptivos e inferenciales para cuantificar la mejora en la seguridad y la percepción del personal.

c. Triangulación: Utiliza la triangulación para validar los resultados, comparando y contrastando los hallazgos cualitativos y cuantitativos.

3.2.1. Método

Aquí hay algunas opciones de métodos de investigación que podrían ser apropiados:

1. **Fase Exploratoria: Investigación Cualitativa**

   a. Selección de Participantes:

   - Identifica y selecciona a los participantes clave dentro de Virgen de Chapi, incluyendo responsables de seguridad, personal de TI y gerentes.

   b. Entrevistas en Profundidad:

   - Realiza entrevistas estructuradas con los participantes seleccionados para obtener información detallada sobre la infraestructura tecnológica, desafíos de seguridad y capacitación del personal.

   c. Análisis Documental:

   - Analiza políticas de seguridad, informes de incidentes de seguridad y otros documentos relevantes para complementar los datos obtenidos de las entrevistas.

2. **Fase de Desarrollo: Investigación de Diseño**

   a. Implementación de Protocolos de Internet Inteligente:

   - Diseña e implementa los protocolos de Internet inteligente identificados durante la fase exploratoria.

   b. Monitoreo Continuo:

   - Establece un sistema de monitoreo continuo para evaluar la efectividad de los nuevos protocolos en tiempo real.

   c. Encuestas Cuantitativas:

   - Diseña y distribuye encuestas estructuradas para recopilar datos cuantitativos sobre la percepción del personal sobre la efectividad de las nuevas medidas de seguridad.

3.3. Población y muestra

3.3.1. Población

En este caso, la población estaría compuesta por el personal de Virgen de Chapi, Juliaca, especialmente aquellos involucrados en la seguridad de la red empresarial. Los grupos a considerar son los siguientes:

a. **Responsables de Seguridad:** Incluye al profesional encargados de la seguridad informática y la gestión de amenazas.
b. **Personal de TI:** Aquellos que gestionan y mantienen la infraestructura tecnológica de la red empresarial.
c. **Usuarios de la Red Empresarial:** Personal que utiliza regularmente los sistemas y redes de la empresa.

Tabla 2

Población

Población	Tipo de movilidad	Cantidad
• Responsables de Seguridad:	• Profesional encargados de la seguridad informática	1
• Personal de TI	• Es el encargado gestionan y mantienen la infraestructura tecnológica	1
• Usuarios de la Red Empresarial:	• Personal que utiliza regularmente los sistemas	15
Totales		º17

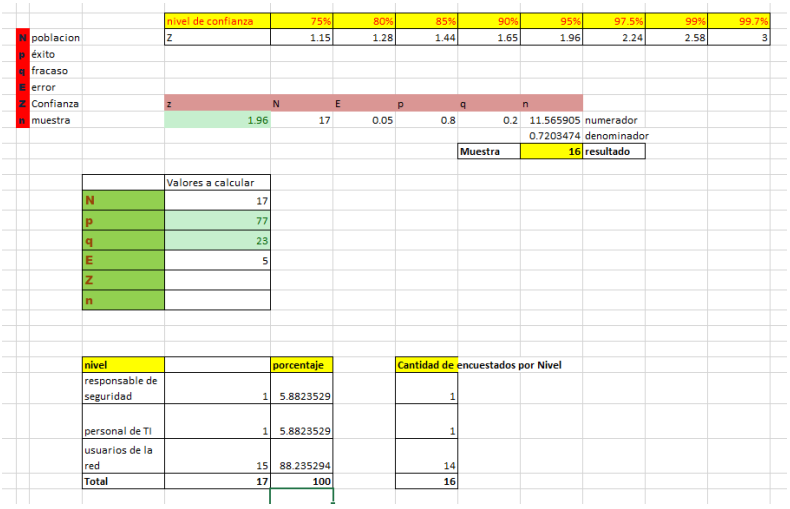
Nota: Elaboración propia

3.3.2. Muestra

Dado que la población es pequeña, para lo cual se aplica la siguiente formula:

Figura 1.

Cálculo de la muestra.



		nivel de confianza	75%	80%	85%	90%	95%	97.5%	99%	99.7%
N	poblacion	Z	1.15	1.28	1.44	1.65	1.96	2.24	2.58	3
p	éxito									
q	fracaso									
E	error									
Z	Confianza	z	N	E	p	q	n			
n	muestra	1.96	17	0.05	0.8	0.2	11.565905	numerador		
							0.7203474	denominador		
						Muestra	16	resultado		

	Valores a calcular
N	17
p	77
q	23
E	5
Z	
n	

nivel		porcentaje	Cantidad de encuestados por Nivel
responsable de seguridad	1	5.8823529	1
personal de TI	1	5.8823529	1
usuarios de la red	15	88.235294	14
Total	17	100	16

Encuestas Cuantitativas:

Selecciona a un número representativo de responsables de seguridad, personal de TI y usuarios de la red. Lo cual hace un rango de 16 participantes que es el mas adecuado.

3.4. Técnica fuentes e instrumentos

3.4.1. Técnicas de Recolección de Datos:

Dado que estás utilizando tanto métodos cualitativos como cuantitativos, te proporcionaré técnicas específicas para cada fase:

A. Fase Exploratoria: Investigación Cualitativa

Entrevistas en Profundidad:

Descripción: Realizar entrevistas detalladas con participantes clave para obtener información rica y detallada sobre la seguridad cibernética en Virgen de Chapi.

Técnica de Recolección de Datos: Entrevistas semiestructuradas o no estructuradas para permitir respuestas detalladas y explorar temas emergentes.

Análisis Documental:

Descripción: Analizar documentos internos y externos relevantes para comprender la situación actual de seguridad.

Técnica de Recolección de Datos: Revisión sistemática de políticas de seguridad, informes de incidentes y literatura relevante.

Grupos Focales (Opcional):

Descripción: Facilitar discusiones grupales para explorar percepciones y experiencias relacionadas con la seguridad cibernética.

Técnica de Recolección de Datos: Moderación de grupos focales con preguntas abiertas para fomentar la participación y la discusión.

B. Fase de Desarrollo: Investigación de Diseño

Implementación de Protocolos de Internet Inteligente:

Descripción: Implementar medidas de seguridad específicas basadas en los resultados de la fase exploratoria.

Técnica de Recolección de Datos: Registro detallado de la implementación, documentando cambios y mejoras realizadas.

Monitoreo Continuo:

Descripción: Establecer sistemas de monitoreo para evaluar la efectividad de los protocolos de seguridad.

Técnica de Recolección de Datos: Utilizar herramientas de monitoreo de seguridad para registrar y analizar eventos y actividades.

Encuestas Cuantitativas:

Descripción: Recopilar datos cuantitativos sobre la percepción del personal respecto a la seguridad.

Técnica de Recolección de Datos: Distribuir encuestas estructuradas, utilizando medios electrónicos o impresos según la conveniencia.

C. Integración de Datos: Enfoque Mixto

Análisis Integrado:

Descripción: Combinar datos cualitativos y cuantitativos para obtener una comprensión completa de la situación.

Técnica de Recolección de Datos: Utilizar matrices de integración de datos para comparar y *contrastar resultados.*

Triangulación:

Descripción: Validar resultados mediante la comparación de datos provenientes de diferentes métodos y fuentes.

Técnica de Recolección de Datos: Utilizar análisis cruzados y comparativos de los resultados cualitativos y cuantitativos.

3.4.2. Instrumento

Herramientas de Análisis de Datos: Para analizar datos cuantitativos, como los resultados de los cuestionarios, necesitarás software de análisis de datos, como SPSS o Excel.

3.5. Validación y contrastación de hipótesis

En tu tesis sobre la implementación de OPTIMIZACIÓN DE LA SEGURIDAD EN REDES EMPRESARIALES PARA DISMINUIR RIESGOS INFORMÁTICOS EN LA EMPRESA VIRGEN DE CHAPI, JULIACA 2024, podrías plantear hipótesis tanto generales como específicas para respaldar tus objetivos

de investigación. Aquí hay un enfoque general sobre cómo diseñar y contrastar hipótesis adecuadamente:

Diseño de Hipótesis:

1. **Hipótesis General:** Comienza por formular una hipótesis general que resuma la relación general que deseas investigar. Por ejemplo:

   Hipótesis General (H0): " La optimización de las defensas cibernéticas en las redes empresariales de Virgen de Chapi, Juliaca, garantizará la protección integral de la información ante desafíos cibernéticos."

2. **Hipótesis Específicas:** Luego, desglosa tu hipótesis general en hipótesis específicas que sean más detalladas y testables. Por ejemplo:

   Hipótesis Específica 1 (H1): La identificación y documentación de deficiencias en los protocolos de seguridad de Virgen de Chapi llevará a una evaluación más precisa del impacto potencial en el riesgo de x% de amenazas cibernéticas."

Hipótesis Específica 2 (H2): " La implementación de protocolos de Internet inteligente en la red empresarial de A Y M Virgen de Chapi mejorará significativamente la protección contra amenazas cibernéticas."

Hipótesis Específica 2 (H2): "Documentar los obstáculos de seguridad en Virgen de Chapi, considerando infraestructura, capacitación y amenazas cibernéticas, será crucial para proponer mejoras efectivas en la seguridad."

3.6. Valides y confiabilidad del instrumento

Tabla 3

Estadística de fiabilidad del instrumento

Resumen de procesamiento de casos			
		N	%
Casos	Válido	16	100,0
	Excluido	0	,0
	Total	16	100,0

Tabla 4

Prueba de hipótesis

Estadísticas de fiabilidad		
Alfa de Cronbach[a]	Alfa de Cronbach basada en elementos estandarizados	N de elementos
,847	,817	10

Alfa de Cronbach: ,847

Este es el valor principal y el más importante de la tabla. El Alfa de Cronbach (α) es un coeficiente que mide la consistencia interna de una escala. Sus valores van de 0 a 1.

Un valor de 0.847 se considera bueno o excelente. Significa que los ítems del instrumento están altamente correlacionados y miden de manera consistente el mismo constructo. Las respuestas de los participantes a las diferentes preguntas son predecibles y estables.

N de elementos: 16

Este valor indica que el instrumento (el cuestionario o test) está compuesto por 10 ítems o preguntas. El análisis de fiabilidad se realizó sobre este conjunto de 16 elementos.

Alfa de Cronbach basada en elementos estandarizados: ,817

Este es un cálculo alternativo del Alfa de Cronbach que se utiliza cuando los ítems tienen diferentes varianzas (por ejemplo, si algunas preguntas se miden en una escala de 1 a 5 y otras de 1 a 7). Estandariza los ítems antes de calcular el coeficiente.

El valor de 0.817 también es alto y muy cercano al Alfa de Cronbach principal. Esto refuerza la conclusión de que el instrumento es fiable, incluso si hay pequeñas diferencias en la varianza de las respuestas a los ítems.

Conclusión Final

El investigador que realizó este análisis puede concluir con seguridad que su instrumento de 10 preguntas es fiable. Un Alfa de Cronbach de 0.847 es un resultado sólido que respalda la calidad de la herramienta de medición para ser utilizada en una investigación, ya que garantiza que las mediciones que se obtengan con ella serán consistentes.

3.7. Análisis de datos

A. Fase Exploratoria: Investigación Cualitativa

Entrevistas en Profundidad:

Transcripción: Transcribe las entrevistas de manera precisa y completa.

Codificación: Identifica temas y patrones emergentes en las transcripciones.

Categorización: Agrupa las respuestas según categorías temáticas.

Análisis Documental:

Codificación de Contenido: Codifica la información clave en los documentos para facilitar el análisis.

Identificación de Patrones: Busca patrones y tendencias en la información recopilada.

Grupos Focales (Opcional):

Transcripción y Codificación: Si decides utilizar grupos focales, realiza la transcripción y codificación de las discusiones.

B. Fase de Desarrollo: Investigación de Diseño

Implementación de Protocolos de Internet Inteligente:

Registro Detallado: Documenta de manera detallada los cambios realizados durante la implementación.

Seguimiento Continuo: Mantén un seguimiento continuo de los eventos y actividades relacionados con la seguridad.

Monitoreo Continuo:

Registro de Eventos: Registra y analiza eventos de seguridad capturados por las herramientas de monitoreo.

Generación de Informes: Genera informes periódicos sobre el estado de la seguridad.

Encuestas Cuantitativas:

Codificación de Datos: Codifica las respuestas de las encuestas para facilitar el análisis.

Análisis Estadístico: Realiza análisis estadísticos descriptivos e inferenciales según sea necesario.

C. Integración de Datos: Enfoque Mixto

Análisis Integrado:

Matriz de Integración: Utiliza una matriz o herramienta similar para integrar datos cualitativos y cuantitativos.

Identificación de Convergencias y Divergencias: Busca puntos de convergencia o divergencia en los resultados de ambas fases.

Triangulación:

Comparación Cruzada: Compara y contrasta los resultados cualitativos y cuantitativos para validar las conclusiones.

Informe de Triangulación: Documenta la triangulación en tu informe final.

CAPITULO IV

RESULTADOS OBTENIDOS

4.1. Desarrollo de la propuesta

Desarrollo del objetivo específico 1,2,3

Solución de la Propuesta

A continuación, se desarrollan cada una de las etapas de la propuesta de solución con datos simulados, manteniendo el contexto de la Empresa Virgen de Chapi en Juliaca y su infraestructura de red única.

4.1.1. Planificación del Análisis de Seguridad

- **Definir el Alcance del Análisis**: Evaluación de la red corporativa que incluye 3 servidores (2 Windows Server 2019 y 1 Linux Ubuntu), 5 estaciones de trabajo, 3 routers, 5 switches, 1 firewall y 20 puntos de acceso Wi-Fi.
- **Formar un Equipo de Seguridad**: Equipo compuesto por 1 expertos en seguridad informática internos y 1 Personal de TI.
- **Establecer Metodologías y Herramientas**: Metodología basada en NIST SP 800-115 y herramientas como Nessus (para escaneo de

vulnerabilidades), Metasploit (para pruebas de penetración) y Wireshark (para análisis de tráfico).

4.1.2. Recolección de Información

- **Mapeo de la Red**: Inventario completo muestra (Ubiquiti UniFi).
  - 3 servidores
  - 5 estaciones de trabajo
  - 3 routers (Cisco 2901)

  - 5 switches (Cisco Catalyst 2960)

  - 1 firewall (Palo Alto PA-220)

  - 20 puntos de acceso (Ubiquiti UniFi)

- **Recopilación de Documentación**: Documentos de configuración de red, políticas de seguridad existentes, y procedimientos operativos estándar obtenidos del departamento de TI.

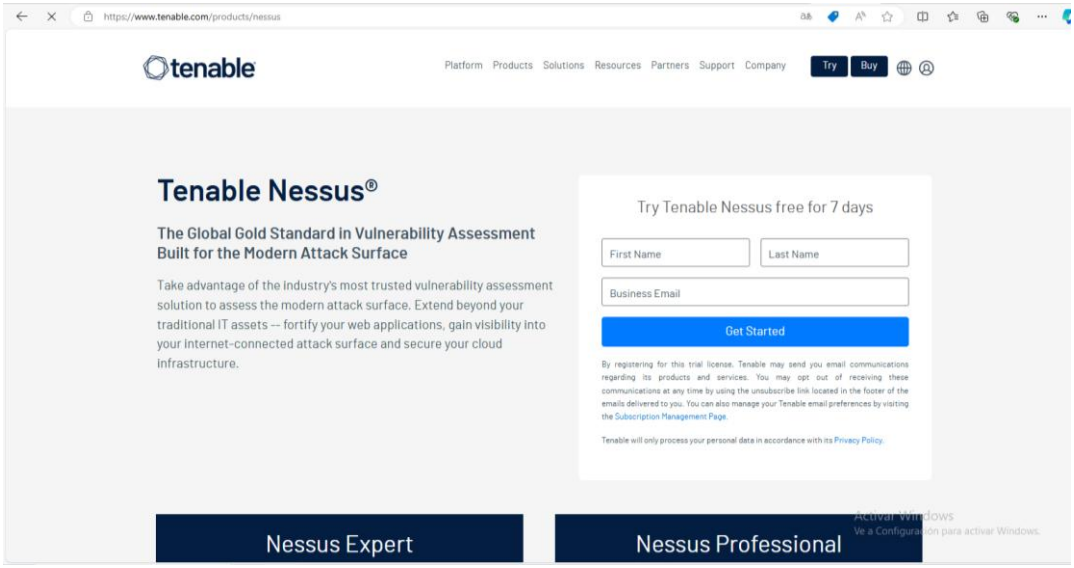
4.1.3. Evaluación de Vulnerabilidades

- **Escaneo de Vulnerabilidades**: Nessus detecta 5 vulnerabilidades críticas, 3 altas, 5 medias y 10 bajas en la infraestructura.

- **Revisión Manual**: Expertos identifican configuraciones inseguras adicionales no detectadas por el escaneo automatizado en 2 servidores y 5 estaciones de trabajo.

Figura 2.

Evaluación de Vulnerabilidades.



4.1.4. Análisis de Configuraciones de Seguridad

- **Revisión de Configuraciones de Dispositivos de Red**: Evaluación revela configuraciones predeterminadas en 3 routers y 4 switches, que representan riesgos de seguridad.
- **Evaluación de Políticas de Seguridad**: Políticas de seguridad encontradas desactualizadas, con última revisión hace 2 años, no cumplen con las mejores prácticas actuales.

4.1.5. Pruebas de Penetración (Penetration Testing)

- **Simulación de Ataques**: Pruebas de penetración revelan 5 puntos de acceso vulnerables a ataques de tipo "man-in-the-middle" y 2 servidores expuestos a ataques de escalada de privilegios.
- **Identificación de Explotaciones**: Documentadas 3 explotaciones exitosas que podrían comprometer información crítica de la empresa.

4.1.6. Análisis de Resultados

- **Clasificación de Vulnerabilidades**: Vulnerabilidades críticas clasificadas incluyen falta de parches en servidores, configuraciones predeterminadas en dispositivos de red y contraseñas débiles.
- **Documentación de Debilidades**: Detalladas debilidades encontradas, con descripciones, ubicaciones y posibles consecuencias.

4.1.7. Desarrollo de Recomendaciones

- **Propuesta de Soluciones**: Recomendaciones incluyen aplicar parches de seguridad, cambiar configuraciones predeterminadas, implementar políticas de contraseñas fuertes, y segmentar la red.
- **Plan de Acción**: Plan incluye cronograma de 6 meses para implementar soluciones, con responsables asignados a cada tarea.

4.1.8. Presentación de Resultados

- **Informe Final**: Informe completo presenta hallazgos del análisis, detallando vulnerabilidades, debilidades y recomendaciones.

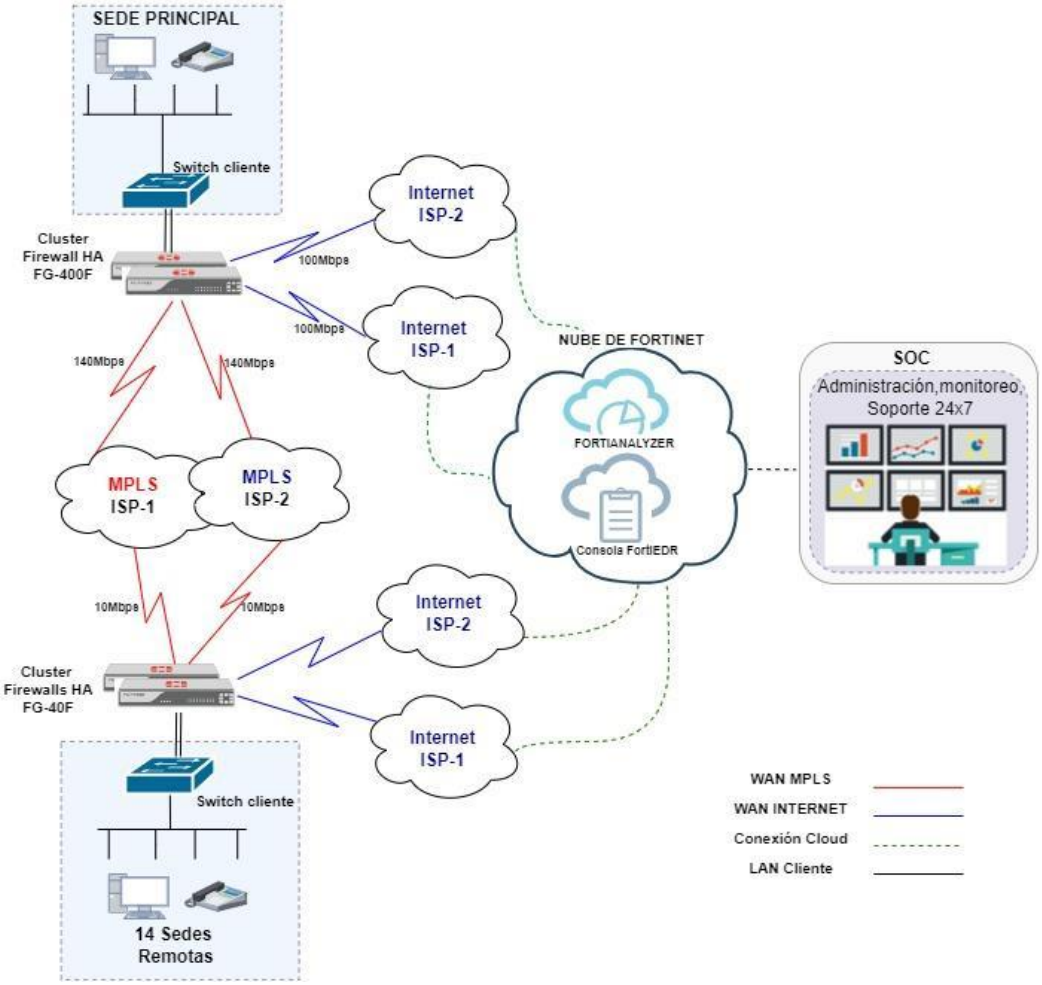
- **Reunión de Retroalimentación**: Resultados presentados a la gerencia y al departamento de TI, con oportunidad para preguntas y retroalimentación.

4.1.9. Monitoreo y Revisión Continua

- **Implementación de Recomendaciones**: Supervisión de la implementación de medidas de seguridad recomendadas, asegurando que se sigan los cronogramas.
- **Reevaluación Regular**: Planificación de evaluaciones semestrales para asegurar la mejora continua de la seguridad informática.

Figura 3.

Topología de la solución propuesta



Plan de Acción Detallado

Tabla 5

Acciones detalladas

Medida de Seguridad	Descripción	Responsable	Fecha de Inicio	Fecha de Finalización
Aplicación de Parches de Seguridad	Actualización de todos los sistemas operativos y aplicaciones	Administrador de TI	01/02/2024	15/02/2024
Configuración Segura de Dispositivos	Ajuste de configuraciones de routers, switches y puntos de acceso	Consultor de Seguridad	16/02/2024	31/02/2024
Implementación de Autenticación Multifactor	Configuración de autenticación multifactor para acceso a sistemas críticos	Administrador de TI	01/03/2024	15/03/2024
Optimización de Firewalls y IPS	Reconfiguración y optimización de firewalls y sistemas de prevención de intrusiones	Especialista en Redes	16/03/2024	31/03/2024
Segmentación de la Red	Creación de subredes separadas para sistemas críticos	Ingeniero de Redes	01/04/2024	15/04/2024
Programa de Capacitación de Seguridad	Capacitación del personal en nuevas políticas y procedimientos de seguridad	Coordinador de Capacitación	16/04/2024	30/04/2024
Implementación de Monitoreo Continuo	Configuración de herramientas de monitoreo para detección de incidentes	Administrador de TI	01/05/2024	15/05/2024
Evaluación Periódica	Realización de evaluaciones periódicas de la seguridad	Auditor de Seguridad	16/05/2024	31/05/2024

4.2. Análisis de resultados.

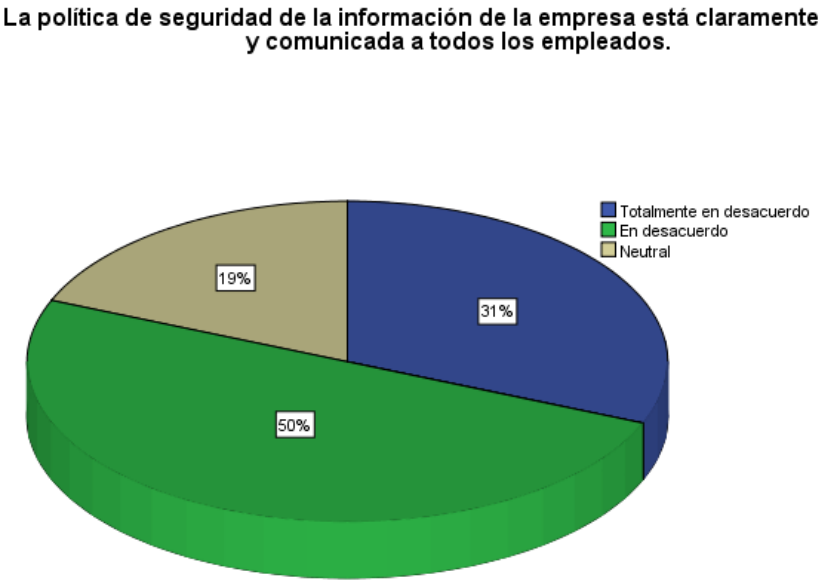
En la siguiente tabla y apartado de imágenes se muestran los resultados obtenidos

Tabla 6

Pregunta de la encuesta número 01

La política de seguridad de la información de la empresa está claramente definida y comunicada a todos los empleados		
	Frecuencia	%
Totalmente en desacuerdo	5	31
En desacuerdo	8	50
Neutral	3	19
Total	16	100

Figura 4.
Pregunta de la encuesta número 01



Interpretación: El 50% está en desacuerdo sobre la información sobre las políticas de seguridad, el 31% manifiesta que está Totalmente en desacuerdo sobre la información sobre las políticas de seguridad y el 19% se mantiene neutral en su respuesta.

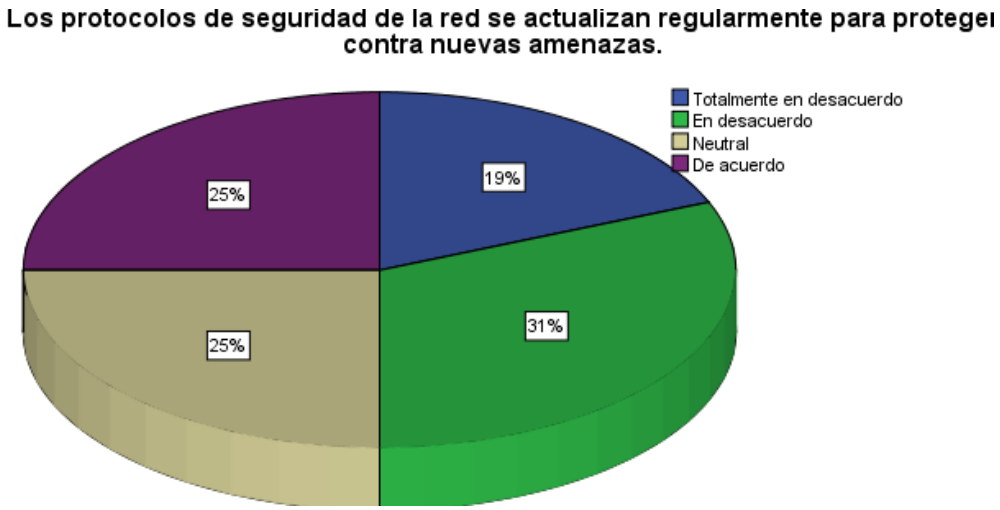
Tabla 7

Pregunta de la encuesta número 02

Los protocolos de seguridad de la red se actualizan regularmente para proteger contra nuevas amenazas.		
	Frecuencia	%
Totalmente en desacuerdo	3	19
En desacuerdo	5	31
Neutral	4	25
De acuerdo	4	25
Total	16	100

Figura 5.

Pregunta de la encuesta número 02



Interpretación: El 31% se encuentra en desacuerdo sobre la actualización de la seguridad de la red, el 25% se encuentra neutral o desconoce, un 25% manifiesta estar de acuerdo con proteger contra nuevas amenazas, el 19% manifiesta que esta totalmente en desacuerdo contra la protección de nuevas amenazas.

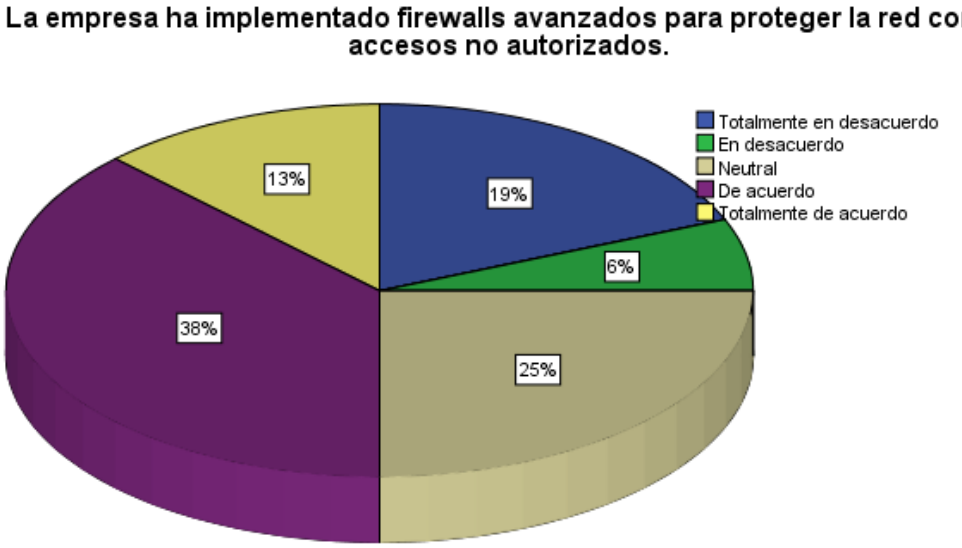
Tabla 8

Pregunta de la encuesta número 03

La empresa ha implementado firewalls avanzados para proteger la red contra accesos no autorizados.		
	Frecuencia	%
Totalmente en desacuerdo	3	19
En desacuerdo	1	6
Neutral	4	25
De acuerdo	6	38
Totalmente de acuerdo	2	13
Total	16	100

Figura 6.

Pregunta de la encuesta número 03



Interpretación: El 38% se encuentra de acuerdo el haber implementado un firewall para proteger la red contra acceso no autorizados, el 25% se encuentra neutral o desconoce, un 19% se encuentra totalmente en desacuerdo, el 13% se encuentra Totalmente de acuerdo, y el 6% se encuentra en desacuerdo.

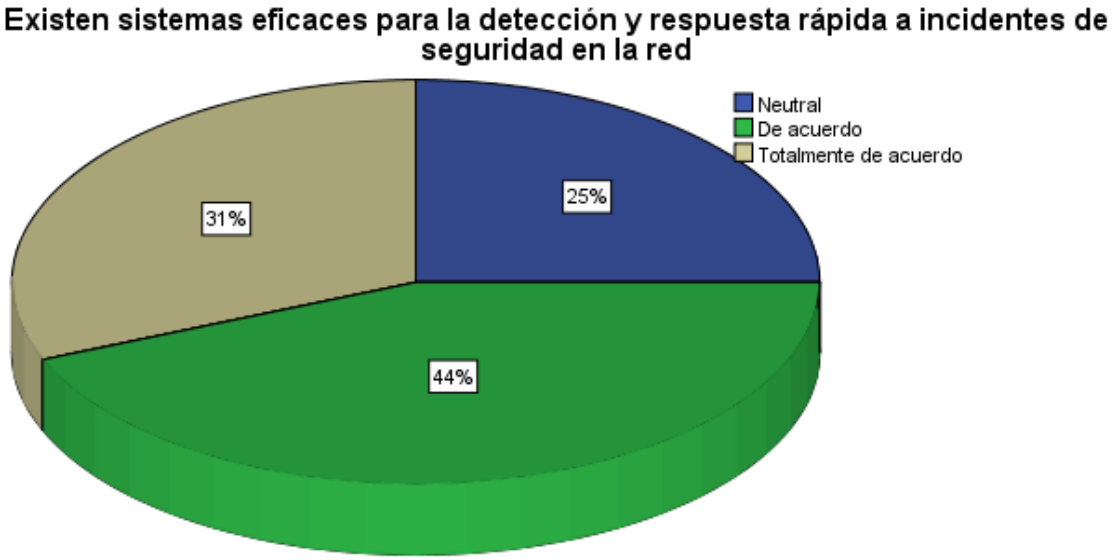
Tabla 9

Pregunta de la encuesta número 04

Existen sistemas eficaces para la detección y respuesta rápida a incidentes de seguridad en la red		
	Frecuencia	%
Neutral	4	25
De acuerdo	7	44
Totalmente de acuerdo	5	31
Total	16	100

Figura 7.

Pregunta de la encuesta número 04



Interpretación: El 44% está de acuerdo con la existencia de sistemas eficaces para la seguridad de las redes, el 31% está totalmente de acuerdo con la existencia de sistemas eficaces para la seguridad de las redes, el 25% se encuentra neutral o desconoce.

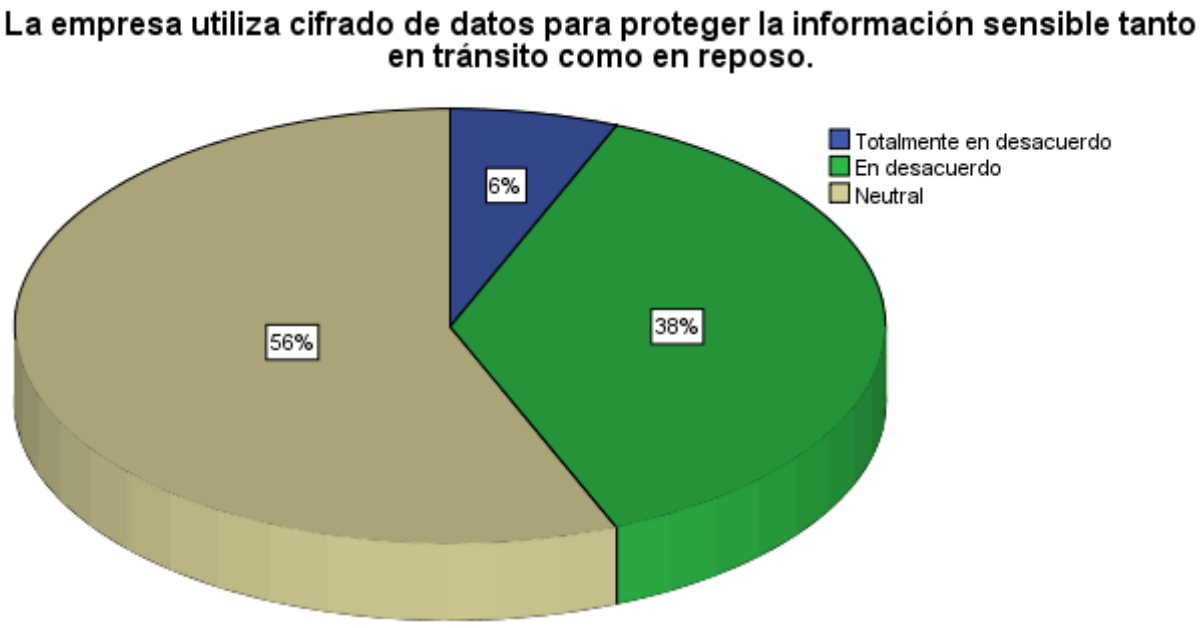
Tabla 10

Pregunta de la encuesta número 05

La empresa utiliza cifrado de datos para proteger la información sensible tanto en tránsito como en reposo		
	Frecuencia	%
Totalmente en desacuerdo	1	6
En desacuerdo	6	38
Neutral	9	56
Total	16	100

Figura 8.

Pregunta de la encuesta número 05



Interpretación: El 56% se mantiene Neutral sobre el uso de cifrado de datos para proteger la información, 38% se mantiene en desacuerdo sobre el uso de cifrado de datos y el 6% se encuentra totalmente en desacuerdo.

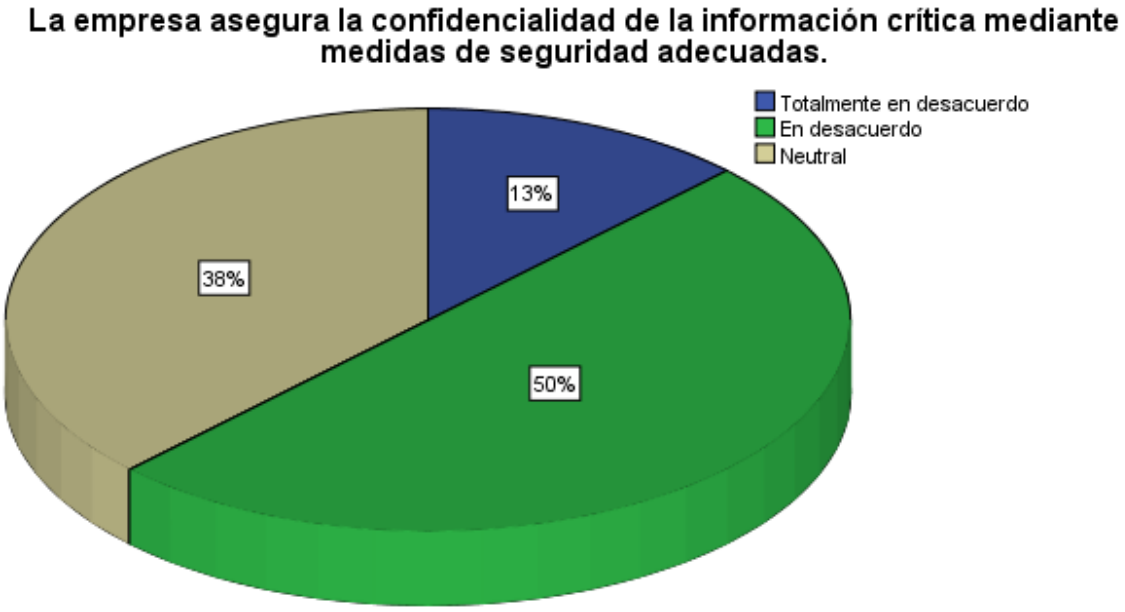
Tabla 11

Pregunta de la encuesta número 06

La empresa asegura la confidencialidad de la información crítica mediante medidas de seguridad adecuadas.		
	Frecuencia	%
Totalmente en desacuerdo	2	13
En desacuerdo	8	50
Neutral	6	38
Total	16	100

Figura 9.

Pregunta de la encuesta número 06



Interpretación: El 50% se mantiene en desacuerdo sobre la confidencialidad de la información, el 38% se mantiene Neutral y el 13%se encuentra totalmente en desacuerdo sobre la confidencialidad de la información.

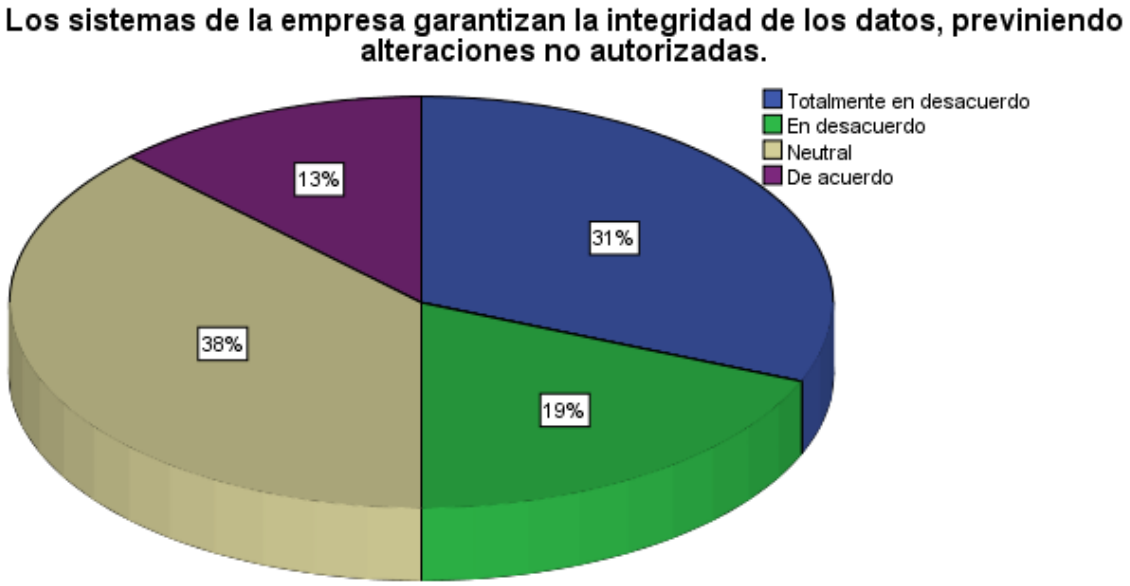
Tabla 12

Pregunta de la encuesta número 07

Los sistemas de la empresa garantizan la integridad de los datos, previniendo alteraciones no autorizadas.		
	Frecuencia	%
Totalmente en desacuerdo	5	32
En desacuerdo	3	19
Neutral	6	38
De acuerdo	2	13
Total	16	100

Figura 10.

Pregunta de la encuesta número 07



Interpretación: El 38% se mantiene neutral sobre garantizar la integridad de los datos, el 31% se mantiene totalmente en desacuerdo, el 19% se encuentra en desacuerdo sobre garantizar la integridad de los datos, el 13% indica que .se encuentra de acuerdo sobre garantizar la integridad de los datos

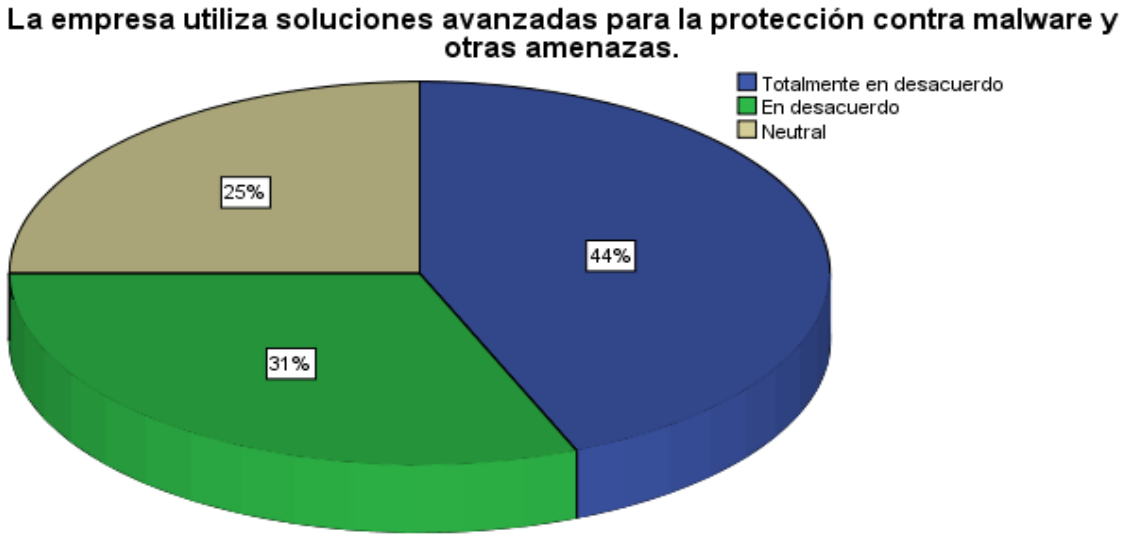
Tabla 13

Pregunta de la encuesta número 08

La empresa utiliza soluciones avanzadas para la protección contra malware y otras amenazas.		
	Frecuencia	%
Totalmente en desacuerdo	7	43,8
En desacuerdo	5	31,3
Neutral	4	25,0
Total	16	100

Figura 11.

Pregunta de la encuesta número 08



Interpretación: El 44% manifiesta que esta totalmente en desacuerdo sobre el uso de solución avanzadas para la protección contra malwares, 31% esta en desacuerdo sobre el uso de solución avanzadas para la protección contra malwares, 25% se mantiene neutral, frente al usos de solución avanzadas para la protección contra malwares.

4.3. Discusión de resultados.

Según, te tiene una significancia similar a la investigación realizada por (Montaña Sierra & Daza Tibocha, 2018) Por lo tanto, sigue realizándolas en tu tesis. "En este se encuentra el Este documento detalla el proceso de planificación y ejecución de un proyecto de grado basado en la necesidad de diseñar e implementar un sistema de detección de anomalías de red a través del análisis avanzado de logs. El software deberá permitir la utilización de los recursos tecnológicos existentes para llevar a cabo el análisis. La propuesta implica una labor, un trabajo especial sobre los logs generados por cada dispositivo que se conecta a la red corporativa. De este modo, las pymes de varios sectores tendrán una protección continua contra las amenazas recurrentes de las redes e Internet. Debo agregar que esta capacidad no solo mejora la seguridad informática, sino que también hace que las corporaciones estén preparadas para detectar y reaccionar rápidamente a cualquier amenaza que pueda dañar sus inversiones. También se quiere mejorar la apariencia y el control sobre las redes de datos, así como desarrollar medidas de contrarresto en una visión defensiva de los posibles ataques a infraestructuras trascendentes.

La sofisticación de los ciberdelincuentes nacionales e internacionales, por un lado, exige la apropiación de hechos consumados de grabaciones engañosas, extorsión fraudulencia, entre otros; por otro, constituye una amenaza constante para los usuarios y organizaciones. Por lo tanto, un ataque puede propagarse y tener consecuencias para la estabilidad del país, la integridad corporativa, la economía nacional, y la administración estatal más importante. Como resultado, es necesario establecer medidas preventivas y correctivas para proteger continuar la integridad de los sistemas tecnológicos. También se precisa una

referencia según los objetivos planteados con (Ramos Huayhua, 2019), En mi tesis titulada "Desarrollo de una plataforma para monitorear y optimizar la red corporativa de una mina", afirmo que vivimos en una era muy marcada por la innovación tecnológica continua, y la evolución y los cambios son mucho más prominentes. Cada día aportamos nuevos dispositivos a nuestras redes corporativas, ya sea en un entorno hogareño, comercial o empresarial. Hay tantos dispositivos de red, y a menos que se gestionen de manera adecuada, tendrán consecuencias letales para la empresa. Por tanto, los mecanismos de transporte/enrutamiento, la supervisión de redes y el acceso son muy importantes. La red está saturada y hay una enorme cantidad de dispositivos conectados. Esto puede llevar a fallas de red, retrasos o mal funcionamiento que interrumpen el ritmo operacional del equipo y ponen en peligro la seguridad empresarial. Para enfrentar estos problemas y evitar fallas en la red LAN, se asignan mecanismos, protocolos y plataformas a los datos que optimizan y monitorean los demás dispositivos conectados. Esto pudo facilitar un proceso de control efectivo que optimice el rendimiento general. El estudio identifica los problemas y aplica soluciones de manera gradual en varias áreas.

CONCLUSIONES

Primero: La identificación y mitigación de las principales vulnerabilidades en la infraestructura de red de la Empresa Virgen de Chapi han resultado en una mejora integral de la seguridad. Las medidas implementadas, como la autenticación multifactor y la optimización de firewalls, han fortalecido significativamente la protección contra riesgos informáticos, estableciendo un entorno más seguro y confiable para las operaciones empresariales.

Segundo: La capacitación continua del personal en seguridad informática ha creado una cultura proactiva dentro de la empresa. Esta iniciativa ha permitido al equipo no solo responder eficazmente a incidentes de seguridad, sino también anticipar y prevenir posibles amenazas. Esta cultura de seguridad proactiva es crucial para mantener la integridad y disponibilidad de la información crítica en un entorno de amenazas cibernéticas en constante evolución.

Tercero: El establecimiento de un plan de acción sostenible, que incluye la actualización continua de sistemas y la evaluación periódica de la infraestructura de red, ha garantizado la eficacia a largo plazo de las medidas de seguridad implementadas. Esta adaptabilidad asegura que la empresa esté siempre preparada para enfrentar nuevas amenazas cibernéticas, manteniendo un alto nivel de seguridad en todo momento.

Cuarto: La implementación de protocolos de Internet inteligente y otras medidas de seguridad innovadoras ha permitido a la Empresa Virgen de Chapi no solo mitigar los riesgos informáticos actuales, sino también innovar en su enfoque de gestión de riesgos. Este enfoque ha resultado en una protección integral y avanzada de la información, posicionando a la empresa como líder en prácticas de seguridad informática dentro de su sector.

RECOMENDACIONES

Primero: Es crucial mantener un programa continuo de capacitación en seguridad informática para todo el personal. Esta formación debe incluir las últimas tendencias en ciberseguridad, nuevas amenazas emergentes y mejores prácticas para la protección de la información. Invertir en el desarrollo de capacidades asegura que el equipo esté preparado para identificar y responder adecuadamente a cualquier incidente de seguridad.

Segundo: A su vez, es recomendable adoptar tecnologías avanzadas de inteligencia artificial y machine learning para detectar y responder amenazas. Estas tecnologías pueden detectar patrones anómalos y riesgos emergentes de forma inmediata, lo que permite obtener una respuesta instantánea. También se debe implementar un sistema de monitoreo continuo que verifica si la red es segura y si no hay actividad sospechosa.

Tercero: Es fundamental realizar revisiones y actualizaciones periódicas de los protocolos de seguridad para asegurar que estén alineados con las mejores prácticas actuales y las normativas vigentes. Esta revisión debe incluir la evaluación de todas las políticas de seguridad, la configuración de los dispositivos de red y la implementación de nuevas herramientas de protección si es necesario.

Cuarto: La empresa debe tener un plan de respuesta a incidentes claro y probado. El plan debe tener procedimientos claros para detectar, contener, erradicar y recuperarse de incidentes de seguridad. Se recomienda hacer simulacros de incidentes para que el personal conozca sus roles en una brecha de seguridad.

REFERENCIA BIBLIOGRÁFICA

Alain Fayolle, H. K. (2003). *International Entrepreneurship Education: Issues And Newness.* Routledge.

Anderson, R. (2019). La seguridad digital no puede ser una excusa para mantener la obsolescencia programada. *Cambridge University Computer Lab*.

Barriga, A., & Gerardo, J. (2019). *EVALUAR LA EFECTIVIDAD EN LAS POLÍTICAS DE LA SEGURIDAD Y CIFRADO DE LOS PROTOCOLOS H.323 Y SIP CON SSL PARA REDES VOLP.*

Berners-Lee, T. (1997). *The World Wide Web: A very short personal history.*

Bohorquez Zumaeta, C. E. (2022). *Simulación de una red VLAN para optimizar el rendimiento de la comunicación de datos en Optical Networks, Tacna - 2022.* Tacna: Universidad prIvada de Tacna.

Campbell, D. T. (1966). *Experimental and Quasi-Experimental Designs for Research. .* Houghton Mifflin.

Cervantes, A., & Hechavarría, J. (2018). *Solución de ciber-seguridad perimetral para redes de datos empresariales.*

Chara Conocc, J. V., & San Martin Soria, F. R. (2022). *Diseño de una gestión centralizada y automatización de la red lan utilizando la solución cisco SD-Access en una empresa de aeronavegación.* Lima: Universidad Nacionak dek Callao.

Choez Cajamarca, D. A., & Benites Barreiro, J. A. (2015). *Auditoría de seguridad en redes inalámbricas, soluciones y recomendaciones.* Guayaquil: Escuela politecnica del Litoral.

Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches.* Sage Publications.

David B. Audretsch, M. J. (2022). *Discovering the Entrepreneurial Mindset: A Qualitative Study of How Entrepreneurs Think.* Oxford University Press.

David Chaffey, F. E.-C. (2015). *Digital Marketing: Strategy, Implementation and Practice.* Pearson.

Denning Dorothy, E. (1986). An intrusión Detection Model. *IEE Symposium on Secutity and Privacy*.

Drew Tech. (18 de 05 de 2023). Obtenido de https://blog.wearedrew.co/productividad/-ventajas-y-desventajas-de-la-metodologia-scrum

Easterby-Smith, M. T. (2012). *Management Research.* SAGE Publications.

Hernández Cervantes, A. E., & Chamizo Hechavarría, J. L. (2018). *Solución de ciber-seguridad perimetral para redes de datos empresariales.*

Hernández Salazar, R., Pérez Jasso, C., Pérez Perdomo, E., & Morales Hechavarria, L. D. (2018). *Análisis explorativo de la seguridad en las redes sociales de los estudiantes de grado medio en la región de El Mante, México.*

Hevner, A. R. (2004). *Design Science in Information Systems Research.* MIS Quarterly.

Kalle Lyytinen, Y. Y. (2021). *Digital Product Innovation in Small and Medium Enterprises: A Process-Oriented Perspective.* MIS Quarterly.

Kalpana Kochhar, I. S. (2006). Flattened firms and information: evidence from trade on the internet. *The Review of Economics and Statistics*, 759–773.

Ken Schwaber, J. S. (2014). *Scrum: The Art of Doing Twice the Work in Half the Time.* New York: Crown Business.

Kenneth C. Laudon, C. G. (2008). *E-commerce: Business, Technology, Society".* Pearson.

Kerzner, H. (2022). *Project Management: A Systems Approach to Planning, Scheduling, and Controlling.* Wiley.

Laudon, K. C. (2017). *E-commerce: Business, Technology, Society.* Pearson.

Montaña Sierra, W. O., & Daza Tibocha, W. (2018). *Diseño e implementación de un sistema de detección de anomalías de red mediante el análisis avanzado de logs utilizando software libre en un ambiente de laboratorio que permita la optimización de recursos tecnológicos.* Bogota: Universidad Polito de Colombia.

Patton, M. Q. (2015). *Qualitative Research & Evaluation Methods: Integrating Theory and Practice.* AGE Publications.

Perdigón, R. (2022). *Suricata como detector de intrusos para la seguridad en redes de datos empresariales.* Ciencia UNEMI.

Ramos Huayhua, F. (2019). *Implementación de plataforma de monitoreo y optimización de la red corporativa de una planta minera.* Lima: Universidad Tecnologica del Perú.

Rayport, J. F. (2001). *Introduction to e-commerce.* McGraw-Hill.

Rosero Lugo, J. L., Acuña, O., & García, N. (2011). *EVALUACIÓN DE LOS PROTOCOLOS IPSEC Y SSL EN LA TRANSMISIÓN SEGURA DE IMÁGENES DIAGNOSTICAS EN TELERADIOLOGIA UTILIZANDO EL ESTÁNDAR DICOM.*

Serrano, C. M., Ortiz Mata, J., & Rea Sánchez, V. (2021). Diseño y desarrollo de un laboratorio de pruebas basados en Smart Home aplicando protocolo de comunicación Z-Wave y estándar 802.11. *Ecuadorian Science Journal*, n.

Tixe Paucar, C. J. (2022). *Diseño de una iWAN : diseño de una red iWAN empresarial.* Quito: Escuela Politecnica Nacional.

Volpano, D., Smith, G., & Irvine, C. (1996). A sound type system for secure flow analysis. *ournal of Computer Security*.

Watson, R. T. (2004). *A Revised Model of E-Commerce Success.* Communications of the Association for Information Systems (CAIS).

Yin, R. K. (2018). *Case Study Research and Applications: Design and Methods.* SAGE Publications.

ANEXOS

Matriz de consistencia

Título: OPTIMIZACIÓN DE LA SEGURIDAD EN REDES EMPRESARIALES PARA DISMINUIR RIESGOS INFORMÁTICOS EN LA EMPRESA VIRGEN DE CHAPI JULIACA 2024

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES	METODOLOGÍA
Problema general ¿Cómo mejorar eficazmente la seguridad en las redes empresariales de la Empresa Virgen de Chapi en Juliaca, considerando los riesgos informáticos existentes y la necesidad de proteger la integridad, confidencialidad y disponibilidad de la información?	**Objetivo general** Optimizar la seguridad en las redes empresariales de la Empresa Virgen de Chapi en Juliaca para reducir los riesgos informáticos y garantizar la protección integral de la información	**Hipótesis general** El mejorar la seguridad en las redes empresariales de la Empresa Virgen de Chapi en Juliaca reducirá significativamente los riesgos informáticos y garantizará la protección integral de la información.	**Variable Independiente** seguridad en redes empresariales **Definición** Esta variable independiente representa la acción específica que llevarás a cabo en tu investigación. **Dimensiones** • Variable Dependiente: • Desarrollo del Marco Conceptual • Diseño e Implementación • Evaluación de Resultados • Adaptaciones y Mejoras	**Tipo de investigación** la investigación exploratoria **Metodología de investigación** investigación combinada de aspectos exploratorios y de desarrollo. **Diseño de investigación** Cuasi experimental **Población** la población es: -Responsables de Seguridad. -Personal de TI. -Gerentes y Líderes de Departamentos **Muestra** La muestra es un subconjunto de la población que eliges para realizar tu investigación. El tamaño de la muestra depende de la precisión que deseas alcanzar y los recursos disponibles para la recopilación de datos **Técnica e instrumentos de recolección de Datos** encuesta para la recopilación de datos se realizará la Entrevistas,
Problemas específicos • ¿Cuáles son las principales vulnerabilidades y debilidades en la infraestructura de red de la Empresa Virgen de Chapi que podrían	**Objetivos específicos** 1. Identificar las principales vulnerabilidades y debilidades en la infraestructura de red de la Empresa Virgen de Chapi mediante un	**122Hipótesis específicas** 1. La identificación y mitigación de las principales vulnerabilidades en la infraestructura de red de la Empresa Virgen de Chapi resultará en una disminución de los	**Variable Dependiente** Riesgos informáticos **Definición conceptual** Esta variable dependiente refleja el resultado que se espera obtener como consecuencia de la implementación de los protocolos **Dimensiones**	

exponerla a riesgos informáticos? • ¿Qué medidas de seguridad adicionales pueden implementarse en las redes empresariales de la Empresa Virgen de Chapi para mitigar los riesgos informáticos identificados y fortalecer la protección de la información? • ¿Cómo puede garantizarse la eficacia y la sostenibilidad de las medidas de seguridad implementadas en las redes empresariales de la Empresa Virgen de Chapi para mantener una protección continua contra los riesgos informáticos en el futuro?	análisis exhaustivo de su seguridad informática. 2. Implementar medidas de seguridad adicionales en las redes empresariales de la Empresa Virgen de Chapi, enfocadas en mitigar las vulnerabilidades identificadas y fortalecer la protección contra riesgos informáticos. 3. Establecer un plan de acción sostenible para garantizar la eficacia a largo plazo de las medidas de seguridad implementadas, incluyendo la capacitación del personal, la actualización continua de los sistemas y la evaluación periódica de la infraestructura de red..	incidentes de seguridad informática. 2. La implementación de medidas adicionales de seguridad en las redes empresariales de la Empresa Virgen de Chapi resultará en una mejora significativa en la protección contra riesgos informáticos, como intrusiones, malware y fugas de datos. 3. El establecimiento de un plan de acción sostenible para mantener y actualizar continuamente las medidas de seguridad en las redes empresariales de la Empresa Virgen de Chapi resultará en una protección a largo plazo contra amenazas informáticas emergentes y en la preservación de la integridad, confidencialidad y disponibilidad de la información	• Evaluación de Vulnerabilidades • Eficiencia en la Gestión de Amenazas Cibernéticas • Protección de la Información • Adaptabilidad y Mejora	Cuestionarios, Análisis Documental, Observación Participante

Instrumento de la investigación

Cuestionario de Preguntas

Tema: OPTIMIZACIÓN DE LA SEGURIDAD EN REDES EMPRESARIALES PARA DISMINUIR RIESGOS INFORMÁTICOS EN LA EMPRESA VIRGEN DE CHAPI JULIACA 2024.

	Donde: 1: En desacuerdo 4: Acuerdo 2: Desacuerdo 5: De acuerdo 3: Neutral				
Nro.	Preguntas	1	2	3	4
1	La política de seguridad de la información de la empresa está claramente definida y comunicada a todos los empleados.				
2	Los protocolos de seguridad de la red se actualizan regularmente para proteger contra nuevas amenazas.				
3	La empresa ha implementado firewalls avanzados para proteger la red contra accesos no autorizados.				
4	Existen sistemas eficaces para la detección y respuesta rápida a incidentes de seguridad en la red				
5	La empresa utiliza cifrado de datos para proteger la información sensible tanto en tránsito como en reposo				
6	La empresa asegura la confidencialidad de la información crítica mediante medidas de seguridad adecuadas				
7	Los sistemas de la empresa garantizan la integridad de los datos, previniendo alteraciones no autorizadas.				
8	Los materiales y equipos que necesito están al alcance, evitando movimientos innecesarios o incómodos.				

Tratamiento de datos

Nro.	P: 1	P: 2	P: 3	P: 4	P: 5	P: 6	P: 7	P: 8	P: 9	P: 10
1	2	3	2	5	4	3	5	5	3	5
2	2	5	2	3	3	4	4	5	4	4
3	3	2	3	5	5	5	2	2	5	5
4	3	4	2	3	3	4	4	4	4	4
5	3	4	5	3	3	4	4	5	4	4
6	4	3	2	5	5	5	1	4	2	5
7	3	2	2	4	4	4	3	4	4	3
8	5	1	2	4	5	5	5	3	5	5
9	3	2	3	5	3	5	4	4	5	4
10	1	3	3	4	4	4	2	1	4	2
11	2	3	2	5	4	3	4	2	3	2
12	4	2	2	3	3	4	4	5	4	4
13	1	1	2	5	5	5	2	2	5	2
14	3	2	2	3	3	4	4	4	4	4
15	3	4	2	3	3	4	4	5	4	4
16	1	5	2	4	4	5	5	3	5	5

Validación del instrumento

UNIVERSIDAD ANDINA NÉSTOR CÁCERES VELÁSQUEZ
FACULTAD DE INGENIERÍA DE SISTEMAS
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

FICHA DE VALIDACIÓN DE INSTRUMENTO DE INVESTIGACIÓN

JUICIO DE EXPERTOS

I. **TITULO DE MI TESIS:** OPTIMIZACION DE LA SEGURIDAD EN REDES EMPRESARIALES PARA DISMINUIR RIESGOS INFORMATICOS EN LA EMPRESA VIRGEN DE CHAPI JULIACA 2024

II. **REFERENCIAS:**

d. **Experto/Nombres** : **KOISHIRO T. ARAPA CRUZ**
e. **Especialidad** : INGENIERO DE SISTEMAS
f. **Cargo Actual** : DOCENTE DE UNAJ

III. **AUTOR DEL INSTRUMENTO DE INVESTIGACIÓN:**
Bach. FIDEL APAZA QUISPE

IV. **ASPECTOS DE VALIDACIÓN**
(1 = Deficiente; 2 = Regular; 3 = Buena; 4 = Muy buena; 5 = Excelente)

INDICADORES	CRITERIOS	DEFICIENTE	REGULAR	BUENA	MUY BUENA	EXCELENTE
1. Claridad	Está redactado con leguaje apropiado					X
2. Objetividad	Está expresado en capacidades observables					X
3. Actualidad	Está adecuado al avance de la ciencia					X
4. Organización	Existe una organización lógica de los ítems y las variables				X	
5. Suficiencia	Valora las dimensiones en cantidad y calidad suficientes					X
6. Intencionalidad	Esta adecuada para cumplir los objetivos de la investigación			x		
7. Consistencia	Está basado en aspectos teóricos y científicos					X
8. Coherencia	Entre las dimensiones, indicadores e ítems				X	
9. Metodología	Responde al propósito de la investigación					X
10. Pertinencia	Es útil y adecuado para la investigación				x	

Coeficiente de valoración porcentual. C = Total/50

V. **OBSERVACIONES Y RECOMENDACIONES**

.....

VI. **RESOLUCIÓN DEL EXPERTO**

Aprobado (C>75%=0.75) [X]

Desaprobado (C<75%=0.75) [ ]

LUGAR Y FECHA: Juliaca, 10 de julio del 2024

Koishiro T. Arapa Cruz
INGENIERO DE SISTEMAS
CIP. 321051

UNIVERSIDAD ANDINA NÉSTOR CÁCERES VELÁSQUEZ
FACULTAD DE INGENIERÍA DE SISTEMAS
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

FICHA DE VALIDACIÓN DE INSTRUMENTO DE INVESTIGACIÓN

JUICIO DE EXPERTOS

I. **TITULO DE MI TESIS:** OPTIMIZACION DE LA SEGURIDAD EN REDES EMPRESARIALES PARA DISMINUIR RIESGOS INFORMATICOS EN LA EMPRESA VIRGEN DE CHAPI JULIACA 2024

II. REFERENCIAS:

a. **Experto/Nombres** : **RAMIRO ARTURO RODRIGUEZ SARAVIA**
b. **Especialidad** : INGENIERO DE SISTEMAS
c. **Cargo Actual** : DOCENTE DE UNAJ

III. **AUTOR DEL INSTRUMENTO DE INVESTIGACIÓN:**
Bach. FIDEL APAZA QUISPE

IV. **ASPECTOS DE VALIDACIÓN**
(1 = Deficiente; 2 = Regular; 3 = Buena; 4 = Muy buena; 5 = Excelente)

INDICADORES	CRITERIOS	DEFICIENTE	REGULAR	BUENA	MUY BUENA	EXCELENTE
1. Claridad	Está redactado con leguaje apropiado					X
2. Objetividad	Está expresado en capacidades observables					X
3. Actualidad	Está adecuado al avance de la ciencia				X	
4. Organización	Existe una organización lógica de los ítems y las variables				X	
5. Suficiencia	Valora las dimensiones en cantidad y calidad suficientes					X
6. Intencionalidad	Esta adecuada para cumplir los objetivos de la investigación					X
7. Consistencia	Está basado en aspectos teóricos y científicos					X
8. Coherencia	Entre las dimensiones, indicadores e ítems				X	
9. Metodología	Responde al propósito de la investigación					X
10. Pertinencia	Es útil y adecuado para la investigación					X

Coeficiente de valoración porcentual. C = Total/50

V. **OBSERVACIONES Y RECOMENDACIONES**

.....

VI. **RESOLUCIÓN DEL EXPERTO**

Aprobado (C>75%=0.75) [X]

Desaprobado (C<75%=0.75) [ ]

LUGAR Y FECHA: Juliaca, 12 de julio del 2024

Ramiro Arturo Rodriguez Saravia
INGENIERO ESPECIALISTA
CIP. Nº 126138

ANEXO 1
FORMULARIO DE AUTORIZACIÓN

AUTORIZACIÓN PARA LA INCORPORACIÓN DE LOS TRABAJOS DE INVESTIGACIÓN EN EL REPOSITORIO INSTITUCIONAL UANCV

Formato digital [X] Fecha de entrega: 31 – 12 – 2025

1. Datos del autor (es):

Nombres y Apellidos: FIDEL APAZA QUISPE
Dirección: Jirón Oroya Mz.: F Lt.: 01 – Juliaca
DNI/Carné de Extranjería/Pasaporte N°: 70202945
Teléfono: 930 983 533 email: fidel.tuxhack@gmail.com
Nombres y Apellidos:
Dirección:
DNI/Carné de Extranjería/Pasaporte N°:
Teléfono: email:
Facultad y/o Escuela de Posgrado: INGENIERIA DE SISTEMAS
Escuela Profesional o Mención: INGENIERÍA EMPRESARIAL E INFORMÁTICA
Título o Grado Académico a optar: INGENIERO EMPRESARIAL E INFORMÁTICO
Asesor: Dr. PAUL MAMANI TISNADO
Esta obra se encuentra dentro de las siguientes denominaciones:
Trabajo de Investigación [ ] Tesis [X] Trabajo de Suficiencia Profesional [ ] Trabajo Académico [ ]
Título: OPTIMIZACIÓN DE LA SEGURIDAD EN REDES EMPRESARIALES PARA DISMINUIR RIESGOS INFORMÁTICOS EN LA EMPRESA VIRGEN DE CHAPI JULIACA 2024
Palabras claves, (3 a 5 términos): Protocolos de internet Inteligentes (IPI), protocolos de Seguridad, ciberseguridad.

¿Esta obra se desarrolló en la UANCV [1, 2]?

2

[1] Indicar si su producción intelectual ha empleado recursos tales como, instalaciones, laboratorios, insumos, equipos, bases de datos, asesoría técnica por parte del personal de la UANCV, financiamiento, entré otros relacionados.
[2] Si su producción intelectual se desarrolló en la UANCV totalmente o parcialmente, deberá autorizar el depósito en el Repositorio de manera obligatoria.

2. Referencia de tesis:

☐ Bachiller ☒ Titulo ☐ 2da Especialidad ☐ Maestría ☐ Doctorado

3. Licencias:

a) Licencia estándar:

Bajo los siguientes términos, autorizo el depósito de mi tesis en el Repositorio Digital de la UANCV.

Con la autorización de depósito de mi producción Intelectual, otorgo a la Universidad Andina "Néstor Cáceres Velásquez" una licencia no exclusiva para reproducir, distribuir, comunicar al público, transformar (únicamente mediante su traducción a otros idiomas) y poner a disposición del público mi producción intelectual (incluido el resumen), en formato físico o digital, en cualquier medio, conocido o por conocerse, a través de los diversos servicios por la Universidad, creados o por crearse, tales como el Repositorio Digital de tesis UANCV, colección de producción intelectual, entre otros, en el Perú y en el extranjero por el tiempo y veces que considere necesarias, y libres de remuneraciones.

En virtud de dicha licencia, la Universidad Andina "Néstor Cáceres Velásquez" podrá reproducir mi producción intelectual en cualquier tipo de soporte y en más de un ejemplar, sin modificar su contenido, solo con propósitos de seguridad, respaldo y preservación.

Declaro que la producción intelectual es una creación de mi autoría y exclusiva titularidad, coautoría con titularidad compartida, y me encuentro facultado a conceder la presente licencia y, asimismo, garantizo que dicha producción intelectual no infringe derechos de autor de terceras personas.

La Universidad Andina "Néstor Cáceres Velásquez" consignará el nombre del y/o los autor(es) de la producción intelectual, y no le hará ninguna modificación más que la permitida en la licencia.

Autorizo su publicación (marque con una X)

☒ Sí, autorizo que se deposite inmediatamente.

☐ Sí, autorizo que se deposite a partir de la fecha (d/m/a):_____

☐ No autorizo.

b) Licencia CREATIVE COMMONS 4.0 INTERNACIONAL:

Si usted concede una licencia CREATIVE COMMONS sobre su producción intelectual, mantiene la titularidad de los derechos de autor de esta y, a la vez, permite que otras personas puedan reproducirla, comunicarla al público y distribuir ejemplares de esta, bajo las condiciones siguientes:

¿Quiere permitir usos comérciales de su producción intelectual?

Sí: significa que usted permite la reproducción, distribución y comunicación pública de la producción intelectual incluso con fines comerciales.

No: significa que usted permite la reproducción, y comunicación pública de la producción intelectual, pero sin fines comerciales.

☐ Sí autorizo

☒ No autorizo

Jurisdicción de su Licencia

Todas las licencias CREATIVE COMMONS son de ámbito mundial, sin embargo, usted puede elegir entre la opción "internacional" o una adaptada a su jurisdicción, como para el caso peruano.

La opción "internacional" emplea el lenguaje y la terminología de los tratados internacionales; en cambio, la adaptada a su jurisdicción, recoge las particularidades de la legislación peruana.

En consecuencia, **la opción "internacional" goza de una mayor eficacia a nivel mundial, gracias a que tiene jurisdicción neutral**. Mientras que la opción adaptada a la jurisdicción del Perú goza de una mayor eficacia ante los tribunales peruanos.

☐ Internacional

☒ Nacional

Línea de investigación: ORGANIZACIÓN Y DIRECCIÓN DE EMPRESAS -P25

Firma de Autor	huella digital	31 – DICIEMBRE – 2025
		Fecha