Universidad Científica del Perú - UCP
Registrado en el Asiento Nº A00010 de la Partida Nº 11000318, Personas Jurídicas de Iquitos, Superintendencia de los Registros Públicos - SUNARP

FACULTAD DE CIENCIAS E INGENIERÍA

PROGRAMA ACADEMICO DE INGENIERIA INFORMATICA Y DE SISTEMAS - INGENIERIA DE SISTEMAS DE INFORMACIÓN

TESIS

AUDITORIA DE LA RED DE DATOS DE LA MUNICIPALIDAD DISTRITAL DE PUNCHANA – 2024

PARA OBTAR EL TITÚLO PROFESIONAL

INGENIERO INFORMÁTICO Y DE SISTEMAS

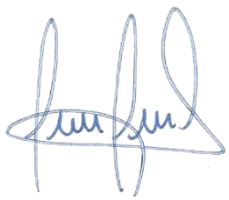
INGENIERO DE SISTEMAS DE INFORMACIÓN

AUTORES:

- **BACH. HILDA JETTSSENIA SOLANGE GÓNGORA PEREYRA**
- **BACH. JOAO CARLOS DEL ÁGUILA QUIROZ**

ASESOR:

- **ING. LEE FRANK MENDOZA LÓPEZ, Dr.**



SAN JUAN BAUTISTA – MAYNAS – LORETO - PERÚ – 2024

UNIVERSIDAD CIENTÍFICA DEL PERÚ

Facultad de Ciencias
e Ingeniería

ACTA DE SUSTENTACIÓN DE TESIS

- Con Resolución Decanal N° 474-2024-UCP-FCEI, del 18 de junio del 2024, se designa jurado Evaluador.
- Con Resolución Decanal N° 58-2025-UCP-FCEI, del 22 de enero del 2025, se aprueba fecha de sustentación.

Siendo las 8:00 am. del día 30de enero del 2025, se constituyó de modo presencial el Jurado para escuchar la sustentación y defensa de la Tesis: **AUDITORÍA DE LA RED DE DATOS DE LA MUNICIPALIDAD DISTRITAL DE PUNCHANA-2024**

Presentado por los Bachilleres:

GONGORA PEREYRA HILDA JETTSSENIA SOLANGE
DEL AGUILA QUIROZ JOAO CARLOS

Para optar el título profesional de:

INGENIERÍA INFORMÁTICA Y DE SISTEMAS

INGENIERO DE SISTEMAS DE INFORMACIÓN

Ingeniería Informática y de Sistemas

Asesor: *Ing. Lee Frank Mendoza López, Mtr*

Luego de escuchar la sustentación, defensa y contestadas las preguntas, el jurado pasó a la deliberación en forma reservada, llegando a la siguiente conclusion:

La sustentación es : APROBADA POR UNANIMIDAD

a las 9:00 horas culminó el acto público.

En fe de lo cual los miembros del Jurado firman el acta y comunican en acto público

Ing. Jimmy Max Ramírez Villacorta, Dr.
Presidente

Ing. Tonny Eduardo Bardales Lozano,Mtro. .
Miembro

Ing. Christian Alfredo Arévalo Jesús, Mtro
Miembro

UNIVERSIDAD CIENTÍFICA DEL PERÚ

HOJA DE APROBACIÓN

PROGRAMA ACADÉMICO DE: INGENIERÍA INFORMÁTICA Y DE SISTEMAS E INGENIERÍA DE SISTEMAS DE INFORMACIÓN
TESISTA: GONGORA PEREYRA HILDA JETTSSENIA SOLANGE y DEL AGUILA QUIROZ JOAO CARLOS
TESIS sustentada en acto público el **30 de enero del 2025, a las 8:00 am** en las instalaciones de la UNIVERSIDAD CIENTÍFICA DEL PERÚ.

ING. JIMMY MAX RAMÍREZ VILLACORTA, DR.
PRESIDENTE DE JURADO

ING. TONNY EDUARDO BARDALES LOZANO,MTRO.
MIEMBRO DE JURADO

ING. CHRISTIAN ALFREDO ARÉVALO JESÚS, MTRO
MIEMBRO DE JURADO

ING. LEE FRANK MENDOZA LÓPEZ, MTRO.
ASESOR

"Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho"

CONSTANCIA DE ORIGINALIDAD DEL TRABAJO DE INVESTIGACIÓN

DE LA UNIVERSIDAD CIENTÍFICA DEL PERÚ - UCP

El presidente del Comité de Ética de la Universidad Científica del Perú - UCP

Hace constar que:

La Tesis titulada:

"AUDITORIA DE LA RED DE DATOS DE LA MUNICIPALIDAD DISTRITAL DE PUNCHANA – 2024"

De los alumnos: **HILDA JETTSSENIA SOLANGE GÓNGORA PEREYRA Y JOAO CARLOS DEL ÁGUILA QUIROZ,** de la Facultad de Ciencias e Ingeniería, pasó satisfactoriamente la revisión por el Software Antiplagio, con un porcentaje de **25% de similitud**.

Se expide la presente, a solicitud de la parte interesada para los fines que estime conveniente.

San Juan, 18 de Diciembre del 2024.

Mgr. Arq. Jorge L. Tapullima Flores
Presidente del Comité de Ética – UCP

JLTF/ri-a
417-2024

CERTIFICADO DE ANÁLISIS
magister

UCP_SISTEMAS_DE_INFORMACION_2024_TESIS_SOLAGE_GONGORA_JOAO_DEL AGUILA_V2

25% Textos sospechosos

1% **Similitudes (ignorado)**
0% similitudes entre comillas
0% entre las fuentes mencionadas
< 1% **Idiomas no reconocidos**
24% **Textos potencialmente generados por la IA**

Nombre del documento: UCP_SISTEMAS_DE_INFORMACION_2024_TESIS_SOLAGE_GONGORA_JOAO_DEL AGUILA_V2.pdf
ID del documento: 9e49a3d675770477c8d17a0c53072492c0f71b51
Tamaño del documento original: 313,9 kB
Autores: []

Depositante: Chris Angela Ramirez Flores
Fecha de depósito: 16/12/2024
Tipo de carga: interface
fecha de fin de análisis: 16/12/2024

Número de palabras: 4778
Número de caracteres: 33.654

Ubicación de las similitudes en el documento:

Fuente principal detectada

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	repositorio.ucp.edu.pe http://repositorio.ucp.edu.pe/bitstreams/69c7700a-2afd-4527-9559-2dd0aec2e9ee/download	< 1%		Palabras idénticas: < 1% (21 palabras)

Fuentes con similitudes fortuitas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	repositorio.usanpedro.edu.pe https://repositorio.usanpedro.edu.pe/bitstreams/d8dd4efc-22d7-43fd-a92c-7e68ce19fba6/downl...	< 1%		Palabras idénticas: < 1% (24 palabras)
2	repositorio.uladech.edu.pe https://repositorio.uladech.edu.pe/bitstream/handle/20.500.13032/21842/CABLEADO_ESTRUCTU...	< 1%		Palabras idénticas: < 1% (16 palabras)
3	Documento de otro usuario #6d229a El documento proviene de otro grupo	< 1%		Palabras idénticas: < 1% (10 palabras)

DEDICATORIA

Dedico este trabajo, a mis amados padres Marla Ninon Pereira Piña y Oscar Manuel Góngora Chávez, quienes con su valentía y determinación han sido mi inspiración y guía en cada paso de este proyecto. Su espíritu emprendedor ha sido la chispa que encendió mi pasión por crear y crecer. Gracias por enseñarme que, con esfuerzo y perseverancia, los sueños se convierten en realidad.
A mis hermanos y sobrinos, que han confiado en mí y apoyado en todo momento.

BACH. HILDA JETTSSENIA SOLANGE GÓNGORA PEREYRA

DEDICATORIA

Con mucho amor y esperanza, dedico este proyecto de tesis, a cada uno de mis seres queridos, quienes han sido mis pilares para seguir adelante y no dejar este sueño.
Es para mí una gran satisfacción poder dedicarles a mis hermanos, sobrinos y tíos, que con mucho esfuerzo y trabajo me lo he ganado.
A mi madre Marista Jacoba Quiroz Tuesta, porque ella es mi motivación de mi vida mi orgullo de ser lo que seré.

BACH. JOAO CARLOS DEL ÁGUILA QUIROZ

AGRADECIMIENTO

En este camino, de tropiezos y aciertos, quiero agradecer a Dios entendiendo que es el principio de toda sabiduría, expresar también mi gratitud a mis padres, Marla y Oscar, por ser siempre mi apoyo, mi fortaleza y orientación a lo largo de toda mi vida; su sabiduría, experiencia y amor incondicional fueron fundamentales para superar los desafíos y obstáculos del camino. Gracias a su paciencia y comprensión, logré mantenerme enfocada y motivada para alcanzar mis metas.

Por otro lado, mi hermano Oscar desempeñó un papel crucial en la realización de mi carrera profesional; su colaboración activa, entusiasmo y dedicación me inspiraron a esforzarme al máximo y a no rendirme ante las dificultades que surgieron en el camino.

BACH. HILDA JETTSSENIA SOLANGE GÓNGORA PEREYRA

Agradecido enormemente con Dios por haberme brindado salud, trabajo y permitirme seguir adelante, con sabiduría, paciencia y hacer realidad una de mis aspiraciones y obtener el grado de título profesional de INGENIERO DE SISTEMAS DE INFORMACION.

A mi asesor por ser parte fundamental de la culminación de este proyecto, por haberme brindado sus conocimientos y sus experiencias, a cada una de las personas que colaboraron con un granito de arena para que este proyecto se haga realidad, mi agradecimiento por su incondicional apoyo y ayuda.

BACH. JOAO CARLOS DEL ÁGUILA QUIROZ

INDICE DE CONTENIDO

Página

RESUMEN 11
CAPÍTULO I.- MARCO TEÓRICO: 13
1.1 Antecedentes de Estudio: 13
1.2 Bases Teóricas: 15
1.3 Definición de Términos Básicos: 17
CAPÍTULO II.- PLANTEAMIENTO DEL PROBLEMA: 19
2.1 Descripción del Problema: 19
2.2 Formulación del Problema: 20
2.2.1 Problema General: 20
2.2.2 Problemas Específicos: 20
2.3 Objetivos: 20
2.3.1 Objetivo General: 20
2.3.2 Objetivos Específicos: 21
2.4 Hipótesis: 22
2.5 Variables: 22
2.5.1 Identificación de Variables: 22
2.5.2 Definición Conceptual de las Variables: 22
Tabla N° 01.- Definición conceptual de la variable 22
2.5.3 Operacionalización de las Variables: 23
Tabla N° 02.- Operacionalización de la variable 23
CAPÍTULO III.- METODOLOGÍA: 24
3.1 Tipo y Diseño de Investigación: 24
3.2 Población y Muestra: 24
3.3 Técnicas, instrumentos y procedimientos de recolección de datos: 26
3.4 Procesamiento y análisis de datos: 28
CAPÍTULO IV.- RESULTADOS: 29
CAPÍTULO V.- DISCUSIÓN: 34
CAPÍTULO VI. - CONCLUSIONES: 36
CAPÍTULO VII.- RECOMENDACIONES: 38
CAPÍTULO VIII.- REFERENCIAS BIBLIOGRÁFICAS: 39

Anexos. 41

INDICE DE TABLAS

Página

Tabla N°01: Definición conceptual de la variable ……22

Tabla N°02: Operacionalización de la variable ……..……...23

Tabla N°03: Vulnerabilidades de la red de datos**..…….....29**

Tabla N°04: Riesgo de la red de datos **……..……...30**

Tabla N°05: Políticas, procedimientos y controles de seguridad existentes en la municipalidad **……..…...31**

Tabla N°06: Recomendaciones de mejoras tecnológicas **…….……..…...32**

RESUMEN

Este informe final de tesis se centra en la auditoría de la red de datos de la Municipalidad Distrital de Punchana, con el objetivo de identificar vulnerabilidades y amenazas, evaluar las políticas de seguridad existentes, y proponer mejoras tecnológicas y procedimentales. Se emplearon herramientas como Nmap, Nessus y Metasploit para identificar vulnerabilidades críticas, incluyendo puertos abiertos innecesarios y falta de actualizaciones de software, mediante la ejecución de este trabajo de investigación se logró identificar muchas deficiencias respecto a políticas de seguridad, falta de procesos para la gestión incidentes y control de accesos físicos al ambiente donde se encuentra los equipos servidores, luego de la evaluación se está proponiendo mejoras respecto a los problemas identificados, como son la implementación de un equipo firewalls, sistema de detección de intrusos, así como la actualización periódicas de hardware y software, dentro de las propuestas más resaltantes también existe la necesidad de capacitar al personal de manera continua respeto a temad de seguridad informática, actualizar las políticas de seguridad existente, dentro de las conclusiones se destaca la urgencia de robustecer la infraestructura de red, mejorar las medidas necesarias para asegurar de manera eficaz y efectiva los datos y sistemas con que cuenta la municipalidad, cumpliendo con estándares y normas sobre la seguridad informática.

Palabras claves: auditoria, redes, municipalidad.

ABSTRACT

This final thesis report focuses on the data network audit of the Municipalidad Distrital de Punchana, aiming to identify vulnerabilities and threats, evaluate existing security policies, and propose technological and procedural improvements. Tools such as Nmap, Nessus, and Metasploit were used to identify critical vulnerabilities, including unnecessary open ports and lack of software updates. Through the execution of this research, numerous deficiencies were identified, such as weaknesses in security policies, lack of processes for incident management, and insufficient physical access controls to the environment housing the server equipment. Following the evaluation, improvements have been proposed to address the identified issues, including the implementation of a firewall, an intrusion detection system, as well as periodic updates of hardware and software. Among the most significant proposals, there is also a strong need for continuous training of personnel on information security topics, and the update of existing security policies. The conclusions emphasize the urgency of strengthening the network infrastructure and implementing necessary measures to effectively and efficiently secure the municipality's data and systems, in compliance with information security standards and regulations.

Keywords: audit, networks, municipality.

CAPÍTULO I.- MARCO TEÓRICO:

1.1 Antecedentes de Estudio:

Zúñiga (2020), se enfoca en realizar un análisis de red en la Facultad de Artes y Comunicación para determinar si una red sin estándares y sin topología es viable o deficiente en comparación con una red basada en estándares. El análisis se realizó utilizando la metodología Top-Down, centrándose en la identificación de las necesidades, así como en la prueba y documentación de la red actual, el análisis de la red se llevó a cabo utilizando el software Speedtest de la compañía Ookla, y la documentación se realizó en la plataforma Visual RF Plan de Aruba Networks. Para conocer el contexto de la red actual en la Facultad de Artes y Comunicación, se realizó una encuesta y se aplicaron técnicas de procesamiento del lenguaje natural (NLP) para identificar patrones clave, se compararon las redes de la Facultad de Artes y Comunicación y la Facultad de Ingeniería y Tecnología utilizando herramientas estadísticas como las gráficas Boxplot y la prueba de varianzas iguales de la prueba ANOVA. Los resultados mostraron que la variabilidad en las velocidades de subida y bajada de la red de Artes y Comunicación era más amplia que la de la Facultad de Ingeniería y Tecnología. facultades funcionan de manera distinta y no presentan semejanza entre ellas,

Susanibar (2021), El proceso de formulación de su propuesta tuvo un componente investigativo tecnológico, recolectando información sobre la seguridad de la red de datos del Hospital Regional de Huacho. La investigación fue de innovación incremental, evaluando la seguridad de un proceso existente para identificar vulnerabilidades y amenazas en la institución. De alcance sincrónico y circunspectivo-prospectivo, se incluyeron opiniones de expertos y profesionales. La población evaluada fueron los trabajadores del área de informática, una muestra de dos personas. Se planificó la evaluación y se evidenciaron deficiencias organizacionales, como la ausencia de un área específica de redes y la falta de auditorías de sistemas, con la responsabilidad de la seguridad en el personal de informática. Aplicando la metodología MAIGTI bajo entorno Cobit, se detectó la falta de políticas y procedimientos adecuados

para manejar incidentes de seguridad, dificultando la recuperación ante percances. Se desarrollaron propuestas de mejora para garantizar la continuidad de los servicios, implantando nuevos métodos de control y un adecuado registro de datos de usuarios. La metodología MAIGTI fue fundamental para la investigación, destacando la necesidad de entender las interrelaciones entre diversos objetivos de control para su correcta aplicación.

Álvarez (2021), su objetivo fue realizar una propuesta de reestructuración del cableado estructurado para la Unidad de Seguros del Hospital Eleazar Guzmán Barrón en Nuevo Chimbote en 2021, con el fin de mejorar la transmisión de datos debido a las deficiencias en la red actual. El alcance abarcó unidades y departamentos institucionales, siendo una investigación descriptiva de nivel cuantitativo, no experimental y de corte transversal. La población consistió en 30 empleados y la muestra también fue de 30, seleccionados por conveniencia. Para la recolección de datos se utilizó un cuestionario mediante la técnica de la encuesta. Los resultados mostraron que, en la dimensión de Nivel de Satisfacción de la red de datos, basada en 10 preguntas, el 26.67% de los trabajadores de la Unidad de Seguros no están satisfechos con la red actual. En la dimensión de Necesidad de reestructurar el cableado estructurado, también con 10 preguntas, el 100% de los encuestados coincidió en la necesidad de reestructurar el cableado de la red.

Fonseca (2021), El presente proyecto de investigación tuvo como objetivo principal diseñar un proyecto de seguridad para la red de datos de la empresa “EURODIESEL” de la ciudad de Ambato, con el fin de prevenir ataques de intrusos a la red de datos de Internet de la empresa y así garantizar a los clientes la confidencialidad, disponibilidad e integridad de su información personal, así como la información propia de la empresa. Para ello, se realizó un análisis de vulnerabilidades, logrando diseñar e implementar un esquema de seguridad adecuado para la red de datos. En el primer capítulo se presentó la fundamentación teórica que sirvió para definir la propuesta y diseñar el esquema. El segundo capítulo se centró en un diseño metodológico y diagnóstico mediante

observación directa y entrevistas al gerente y personal administrativo de EURODIESEL, con el fin de conocer las expectativas del sistema informático y la red de datos a implementar con las debidas seguridades. En el tercer capítulo se desarrolló la propuesta de solución al problema, detallando el desarrollo del esquema, explicando paso a paso el diseño del sistema informático de seguridad de datos, y realizando pruebas de hacking ético (Pentesting y Sniffing) con herramientas como Nmap, Nessus y Metasploit de Kali Linux 2019, para determinar las vulnerabilidades en los equipos informáticos de EURODIESEL.

Lino (2021), esta investigación destaco la importancia de implementar medidas de seguridad en las redes inalámbricas, de tal forma que permitió identificar los protocolos, normas y métodos de seguridad que se necesitó para asegurar el perímetro de la red inalámbrica, con esta medida permitió asegurar la integridad de los datos y la seguridad de la información de la entidad, además se concluyó que la implementación de nuevos protocolos y métodos de seguridad puede producir resultados factibles y valiosos en la protección de la información de la red inalámbrica.

1.2 Bases Teóricas:

Auditoría de Redes de Datos

La auditoría de redes de datos es un proceso estructurado que evalúa la infraestructura de red de una organización con el propósito de evaluar el cumplimiento de protocolos, políticas y vulnerabilidades con la finalidad de garantizar la integridad, disponibilidad y confidencialidad de la información en el tráfico de una red de datos. (Stallings, 2013).

Escaneo de Puertos y Servicios

El escaneo de puertos es una técnica que permite identificar los servicios activos en un sistema, así como los puertos abiertos que podrían ser explotados por atacantes. Esta técnica es fundamental para evaluar el nivel de exposición de una red y determinar si hay servicios innecesarios que deben deshabilitarse. Herramientas como Nmap son comúnmente utilizadas para realizar este tipo de

análisis, ya que permiten realizar escaneos detallados y detectar configuraciones inapropiadas (Lyon, 2009).

Pruebas de Penetración

Las pruebas de penetración, también conocidas como "pentesting," consisten en la simulación controlada de ciberataques para evaluar la resistencia de una red frente a posibles intrusiones. Estas pruebas no solo identifican vulnerabilidades, sino que también evalúan la capacidad de respuesta de los sistemas ante incidentes reales. Metodologías como OWASP y OSSTMM (Open Source Security Testing Methodology Manual) proporcionan marcos de trabajo estandarizados para este tipo de auditorías (Anderson, 2020).

Evaluación de Políticas de Seguridad

Además del análisis técnico, una auditoría debe incluir la evaluación de las políticas y normativas de seguridad aplicadas en la organización. Esto incluye verificar el cumplimiento de estándares internacionales, como ISO/IEC 27001, y la implementación de procedimientos relacionados con la gestión de incidentes y el control de accesos (ISO, 2022).

Herramientas de Auditoría de Redes

Nmap

Es una herramienta de código abierto ampliamente utilizada para escanear redes y sistemas en busca de puertos abiertos y servicios activos. Su versatilidad permite realizar escaneos rápidos y detallados, identificar sistemas operativos, y detectar posibles configuraciones inseguras. Lyon (2009) señala que Nmap es ideal tanto para pequeñas auditorías como para grandes entornos empresariales debido a su capacidad de personalización.

Nessus

Es una herramienta comercial que permite realizar análisis de vulnerabilidades en sistemas y redes. Su funcionalidad abarca desde la detección de software desactualizado hasta la identificación de configuraciones inseguras en

dispositivos críticos. Según Stallings (2021), Nessus es una de las herramientas más completas debido a su amplia base de datos de vulnerabilidades, actualizada constantemente.

Metasploit

Es un marco de pruebas de penetración que facilita la explotación de vulnerabilidades en sistemas. Su capacidad de automatización lo convierte en una herramienta potente para identificar y demostrar brechas de seguridad. Este marco también permite simular ataques complejos para medir la efectividad de las medidas de seguridad implementadas (Anderson, 2020).

Wireshark

Es una herramienta de análisis de tráfico que permite capturar y examinar paquetes de datos en tiempo real. Esta herramienta es esencial para auditar redes, ya que ofrece una visión detallada del tráfico que circula por la red, ayudando a identificar posibles anomalías y comportamientos sospechosos (Comer, 2018).

1.3 Definición de Términos Básicos:

Red de Datos: Sistema de dispositivos interconectados que permite el intercambio de información mediante medios físicos o inalámbricos.

Auditoría de Redes: Proceso que evalúa una red para identificar vulnerabilidades, verificar políticas de seguridad y optimizar su rendimiento.

Vulnerabilidad: Debilidad en un sistema que puede ser explotada para obtener acceso no autorizado.

Pentesting: Simulación controlada de ataques para identificar fallos de seguridad en sistemas o redes.

Confidencialidad: Principio que asegura que solo personas autorizadas accedan a la información.

Integridad: Garantiza que los datos se mantengan precisos, completos y sin alteraciones no autorizadas.

Disponibilidad: Asegura que los datos y recursos estén accesibles cuando se necesiten.

Firewall: Dispositivo o software que controla el tráfico de red según reglas de seguridad.

Sistema de Detección de Intrusos: Herramienta que identifica actividades sospechosas en redes o sistemas y alerta a los administradores.

Política de Seguridad: Conjunto de reglas para proteger la información y gestionar riesgos de seguridad.

Hacking Ético: Uso autorizado de técnicas de hacking para identificar y corregir vulnerabilidades.

CAPÍTULO II.- PLANTEAMIENTO DEL PROBLEMA:

2.1 Descripción del Problema:

La auditoría de la red de datos de la Municipalidad Distrital de Punchana, realizada en 2024, surge en un contexto donde la seguridad de las redes es esencial para garantizar la integridad, confidencialidad y disponibilidad de la información que maneja la entidad, las amenazas cibernéticas son cada vez más complejas y frecuentes, lo que obliga a las organizaciones a cumplir normativas como la ISO 27001 y a adoptar prácticas de ciberseguridad reconocidas. En el ámbito nacional, las regulaciones sobre protección de datos y la digitalización creciente de los servicios públicos exigen que las municipalidades implementen medidas de seguridad robustas para proteger la información de los ciudadanos. Localmente, la Municipalidad distrital de Punchana enfrenta serios desafíos, como vulnerabilidades en su red, falta de políticas de seguridad efectivas, insuficiente capacitación del personal y limitaciones en su infraestructura tecnológica, esta investigación trata de la ejecución de una auditoria de la red de datos de la municipalidad, cuyos resultados permitirá diseñar un plan o actividades para mejorar la seguridad de la red, disminuyendo las vulnerabilidades y otros factores que afecten el funcionamiento de la red, a parte de la metodología general de una auditoria de red también usaremos herramientas como Nmap, Nessus y Metasploit, al concluir la evaluación se mostrará de manera descriptiva los resultados, luego plantearemos las conclusiones y recomendaciones necesarias para contribuir a la mejora de la seguridad de la red de datos de la municipalidad distrital de punchana.

2.2 Formulación del Problema:

2.2.1 Problema General:

- ✓ ¿Cómo puede mejorar la Municipalidad Distrital de Punchana la seguridad de su red de datos mediante una auditoría exhaustiva que identifique y mitigue vulnerabilidades, evalúe la efectividad de las medidas actuales y proponga mejoras tecnológicas y procedimentales en el contexto de crecientes amenazas cibernéticas?

2.2.2 Problemas Específicos:

- ✓ ¿Cuáles son las vulnerabilidades de la red de datos de la Municipalidad distrital de Punchana?

- ✓ ¿Cuáles son los riesgos con que cuenta la red de datos de la Municipalidad distrital de Punchana?

- ✓ ¿Cuál es el nivel de implementación de políticas y procedimientos de seguridad implementadas en la red de datos de la Municipalidad distrital de Punchana?

- ✓ ¿Qué mejoras tecnológicas y procedimentales, pueden recomendarse e implementarse para fortalecer la infraestructura de red y asegurar el cumplimiento de los estándares de seguridad?

2.3 Objetivos:

2.3.1 Objetivo General:

- ✓ Evaluar el nivel de seguridad de la red de datos de la municipalidad distrital de Punchana mediante una auditoria.

2.3.2 Objetivos Específicos:

1. Evaluar las vulnerabilidades de la red de datos de la Municipalidad distrital de Punchana.
2. Evaluar los riesgos con que cuenta la red de datos de la Municipalidad distrital de Punchana.
3. Evaluar el nivel de implementación de políticas y procedimientos de seguridad implementadas en la red de datos de la Municipalidad distrital de Punchana.
4. Plantear mejoras tecnológicas y procedimentales para fortalecer la infraestructura de red y asegurar el cumplimiento de los estándares de seguridad.

2.4 Hipótesis:

No aplica para esta investigación

2.5 Variables:

2.5.1 Identificación de Variables:

- **Variable 1:** Auditoria de la red de datos

2.5.2 Definición Conceptual de las Variables:

- **Definición Conceptual de las Variables:**

Tabla N° 01.- Definición conceptual de la variable

Variable	Definición Conceptual	Definición Operacional
Auditoria de la red de datos	La auditoría de la red de datos es un proceso sistemático y exhaustivo de evaluación de la infraestructura de red de una organización con el objetivo de identificar, analizar y mitigar vulnerabilidades y riesgos de seguridad.	Procedimientos específicos y medibles para cada componente clave, garantizando una evaluación integral y precisa de la seguridad en la red de datos.

Fuente: Elaboración Propia

2.5.3 Operacionalización de las Variables:

Tabla N° 02.- Operacionalización de la variable

Variables	Dimensiones	Indicadores	Instrumento de Recolección de Datos
Auditoria de la red de datos	Identificación de Vulnerabilidades	Número de vulnerabilidades identificadas	Cuestionarios y fichas de observación
	Evaluación de Riesgos	Riesgo total asignado a cada vulnerabilidad	
	Revisión de Políticas y Procedimientos	Número de políticas y procedimientos evaluados	
		Porcentaje de cumplimiento con estándares de seguridad	

Fuente: Elaboración Propia

CAPÍTULO III.- METODOLOGÍA:

3.1 Tipo y Diseño de Investigación:

- **Tipo o enfoque de la Investigación:**

La investigación aplicada se enfoca en la resolución de problemas prácticos y específicos utilizando conocimientos científicos. En este caso, el objetivo es mejorar la seguridad de la red de datos de la Municipalidad Distrital de Punchana mediante una auditoría exhaustiva que proporcione recomendaciones prácticas y accionables.

- **Diseño de la Investigación:**

La investigación descriptiva se centra en describir de manera detallada y sistemática las características y componentes de un fenómeno específico. En este estudio, se describirá el estado actual de la red de datos, las políticas de seguridad, las prácticas operativas y las vulnerabilidades existentes.

3.2 Población y Muestra:

- **Población:**

La población en el contexto de esta investigación se refiere a todos los elementos y sujetos relacionados con la red de datos de la Municipalidad Distrital de Punchana, estos son:

a. Infraestructura de Red:
- Todos los dispositivos de red (routers, switches, firewalls).
- Servidores y sistemas de almacenamiento de datos.
- Estaciones de trabajo y dispositivos de usuario final conectados a la red.

b. Personal Relacionado:

- Todos los empleados del área de TI que gestionan y operan la red de datos.
- Personal administrativo que utiliza los sistemas y la red de datos de la municipalidad.

c. Políticas y Procedimientos:

- Todos los documentos y registros de políticas de seguridad, procedimientos operativos y protocolos de red.

- **Muestra:**

Dado que una auditoría de red puede implicar un análisis intensivo y detallado, la muestra será una selección representativa y manejable de la población total que permita obtener conclusiones precisas y relevantes sin necesidad de evaluar cada elemento individualmente.

Infraestructura de Red:

- Dispositivos de Red: 2 routers, 2 switches y 01 firewall.
- Servidores y Almacenamiento: 01 servidor
- Estaciones de Trabajo: 10 computadoras seleccionadas aleatoriamente

Personal Relacionado:

- Personal de TI: 5 personas que trabajan en el área de Informática
- Personal Administrativo: 10 empleados administrativos de diferentes niveles y áreas que utilizan la red y los sistemas de datos.

Políticas y Procedimientos:

- Documentación: Políticas de seguridad y procedimientos implementados

3.3 Técnicas, instrumentos y procedimientos de recolección de datos:

- **Técnica de Recolección de Datos:**

Entrevistas:

Realizar entrevistas estructuradas y semiestructuradas con el personal de TI y administrativo para comprender las prácticas actuales de seguridad y el uso de la red de datos.

Observación Directa:

Inspección física de los dispositivos de red y configuraciones actuales.

Revisión Documental:

Análisis de todas las políticas de seguridad, procedimientos operativos y registros de incidentes de seguridad.

Evaluación de documentos relacionados con la configuración de la red y los sistemas de TI.

Herramientas Automatizadas:

- Nmap.
- Nessus.
- Metasploit.
- Wireshark.

Instrumento de Recolección de Datos:

Guías de Entrevista:

Conjuntos de preguntas predefinidas para las entrevistas estructuradas y semiestructuradas con el personal de TI y administrativo.

Checklists: Para la verificación de la configuración de dispositivos de red y la verificación de las políticas y procedimientos de seguridad implementados

Software de Escaneo y Monitoreo: Nmap, Nessus, Metasploit Wireshark.

Documentos y Registros: Verificacion de documentos de políticas de seguridad, procedimientos operativos, registros de configuración de red y logs de incidentes de seguridad.

- **Procedimiento de Recolección de Datos:**

Planificación:
Definir el cronograma de actividades y asignar responsabilidades específicas para cada tarea de recolección de datos.
Obtener permisos y accesos necesarios para realizar observaciones y ejecutar herramientas de escaneo en la red.

Ejecución:
Realizar entrevistas y observaciones según lo planificado.

Documentación:
Registrar todas las respuestas obtenidas en las entrevistas, las observaciones realizadas y los resultados de los escaneos de vulnerabilidades de forma clara y estructurada, asegurando que cada dato esté debidamente documentado.

3.4 Procesamiento y análisis de datos:

La combinación de técnicas cualitativas y cuantitativas, junto con el uso de herramientas automatizadas y la revisión documental, permitirá una recolección de datos exhaustiva y un análisis detallado de la seguridad de la red de datos de la Municipalidad Distrital de Punchana. Esto asegurará que las recomendaciones proporcionadas sean basadas en evidencia sólida y directamente aplicables para mejorar la seguridad de la red.

CAPÍTULO IV.- RESULTADOS:

Respecto al objetivo específico 01: Evaluar las vulnerabilidades de la red de datos de la Municipalidad distrital de Punchana.

Durante la evaluación se identificaron las vulnerabilidades mostradas en la siguiente tabla:

Tabla N° 03.- Vulnerabilidades de la red de datos

Vulnerabilidad/Amenaza	Descripción	Impacto	Recomendaciones
Puertos abiertos innecesarios	Puertos no utilizados estaban abiertos, exponiendo la red.	Alto	Cerrar puertos no necesarios.
Configuraciones predeterminadas	Uso de configuraciones de fábrica, incluyendo credenciales.	Alto	Cambiar todas las configuraciones predeterminadas.
Falta de actualizaciones de software	Dispositivos y sistemas sin los últimos parches de seguridad.	Alto	Implementar un plan de actualización regular.
Acceso no autorizado	Intentos de acceso no autorizado detectados.	Crítico	Implementar autenticación multifactorial y monitoreo constante.
Falta de firewall robusto	Configuración de firewall insuficiente.	Alto	Optimizar la configuración del firewall.
Ausencia de IDS	No se contaba con un sistema de detección de intrusos.	Crítico	Implementar un IDS para monitorear la red.

Interpretación: La tabla 03 evidencia que se existen equipos de red con puertos de red abiertos los cuales vienen utilizando las configuraciones predeterminadas de fábrica, estas condiciones permiten accesos no autorizados a la red de datos, también existe la falta de actualizaciones de software en varios dispositivos dejando expuesta la red de datos a vulnerabilidades, lo que incrementa el riesgo de ser objeto de ataques, también se evidencio que dentro de la red de datos no cuenta con un equipo firewall, menos con sistema de detección de intrusos (IDS), lo cual agrava la exposición a ciberataques y compromete la seguridad global de la infraestructura.

Respecto al objetivo específico 02: Evaluar los riesgos con que cuenta la red de datos de la Municipalidad distrital de Punchana.

Durante la evaluación se identificaron los riesgos mostradas en la siguiente tabla:

Tabla N° 04.- Riesgo de la red de datos

Riesgo	Descripción	Impacto	Probabilidad
Puertos abiertos innecesarios	Se detectaron puertos habilitados que no son utilizados, lo que puede facilitar accesos no autorizados.	Alta	Alta
Software sin actualizar	Algunos sistemas y aplicaciones no cuentan con los últimos parches de seguridad, lo que los vuelve vulnerables.	Alta	Media
Control de acceso insuficiente	Se identificó la ausencia de políticas claras para limitar los accesos a usuarios según sus funciones.	Alta	Alta
Falta de detección de intrusos	No existen herramientas instaladas para monitorear posibles actividades maliciosas en la red.	Alta	Alta
Uso de contraseñas débiles	Muchas cuentas utilizan contraseñas poco seguras o fáciles de adivinar.	Media	Alta
Acceso físico no controlado	El área de servidores carece de medidas suficientes para restringir el acceso a personas no autorizadas.	Alta	Media
Respaldo de datos insuficiente	Los sistemas no cuentan con copias de seguridad periódicas ni procesos de verificación de estas.	Alta	Media
Falta de segmentación de red	La red no está dividida en segmentos, lo que expone a todos los dispositivos a posibles ataques.	Alta	Media
Conexión de dispositivos externos inseguros	No hay controles para evitar que dispositivos USB introduzcan malware a los equipos.	Media	Alta
Capacitación insuficiente en ciberseguridad	El personal no está debidamente formado para identificar amenazas ni responder ante incidentes.	Alta	Alta

Fuente: Elaboración propia

Interpretación: De la tabla 04 se puede evidenciar que los riesgos en la red de datos de la Municipalidad Distrital de Punchana son muy críticos, entre los principales hallazgos están los puertos abiertos innecesarios, software desactualizado y la falta de control de accesos, tanto lógico como físico, aunado a ello está la ausencia de segmentación de red, sistemas de respaldo adecuados y capacitación en ciberseguridad agravan la vulnerabilidad general de la infraestructura.

Respecto al objetivo específico 03: Evaluar el nivel de implementación de políticas y procedimientos de seguridad implementadas en la red de datos de la Municipalidad distrital de Punchana.

Durante la evaluación se identificaron los riesgos mostradas en la siguiente tabla:

Tabla N° 05.- Políticas, procedimientos y controles de seguridad existentes en la municipalidad

Política/Procedimiento	Descripción	Adecuación	Recomendaciones
Política de seguridad	Falta de políticas actualizadas y claras sobre la seguridad.	Bajo	Desarrollar y actualizar políticas de seguridad
Procedimientos de gestión de incidentes	Inexistencia de procedimientos claros para manejo de incidentes.	Crítico	Establecer procedimientos claros y entrenar al personal.
Control de acceso físico	Deficiencias en el control de acceso a áreas sensibles.	Medio	Mejorar medidas de control de acceso físico.
Registro y monitoreo de actividades	Falta de registros detallados de actividades en la red.	Medio	Implementar sistemas de registro y monitoreo.

Interpretación de la tabla 05: La evaluación de las políticas y procedimientos de seguridad reveló importantes deficiencias. Las políticas de seguridad no estaban actualizadas ni bien definidas, lo que crea incertidumbre sobre cómo gestionar adecuadamente la seguridad de la red. Además, se constató la ausencia de procedimientos claros para la gestión de incidentes de seguridad, lo que aumenta el riesgo de una respuesta desorganizada en caso de una amenaza.

Respecto al objetivo 04: Plantear mejoras tecnológicas y procedimentales para fortalecer la infraestructura de red y asegurar el cumplimiento de los estándares de seguridad.

Las recomendaciones son las siguientes:

Tabla N° 06.- Recomendaciones de mejoras tecnológicas

Area de Mejora	Mejora Propuesta	Descripción	Prioridad	Beneficios Esperados
Actualización de Herramientas de Seguridad	Implementación de Firewalls de Próxima Generación	Actualizar los firewalls para incluir inspección profunda de paquetes, filtrado de contenido, y protección contra amenazas avanzadas.	Alta	Mejora de la seguridad perimetral y protección contra amenazas avanzadas
	Actualización de Sistemas Operativos y Aplicaciones	Mantener todos los sistemas operativos y aplicaciones actualizados con los últimos parches de seguridad.	Alta	Reducción de vulnerabilidades conocidas y mejora de la estabilidad del sistema.
	Sustitución de Equipos Obsoletos	Reemplazar hardware antiguo con soporte limitado para mejorar la eficiencia y la seguridad.	Media	Incremento de la capacidad de procesamiento y reducción de fallos.
Implementación de Nuevas Tecnologías	Sistema de Detección y Prevención de Intrusos (IDS/IPS)	Implementar soluciones IDS/IPS para monitorear y bloquear tráfico sospechoso en la red.	Crítica	Detección y mitigación de ataques en tiempo real.
	Sistemas de Gestión de Información y Eventos de Seguridad (SIEM)	Implementar herramientas SIEM para la centralización y análisis de eventos de seguridad.	Alta	Visibilidad centralizada de eventos de seguridad y respuesta proactiva.
	Soluciones de Autenticación Multifactor (MFA)	Implementar MFA para fortalecer la autenticación de usuarios.	Alta	Reducción de riesgos de acceso no autorizado.
Capacitación del Personal	Programas de Capacitación Continua	Realizar capacitaciones periódicas para el personal de TI y administrativo sobre mejores prácticas de seguridad.	Alta	Aumento de la conciencia y habilidades en ciberseguridad.
	Simulacros de Respuesta a Incidentes	Realizar simulacros regulares para preparar al personal en la gestión de incidentes de seguridad.	Alta	Mejora de la respuesta ante incidentes y minimización del impacto.
Mejora de Políticas y Procedimientos	Revisión y Actualización de Políticas de Seguridad	Actualizar las políticas de seguridad para reflejar las mejores prácticas y normativas actuales.	Media	Alineación con estándares internacionales y normativas locales.
	Implementación de Procedimientos de Gestión de Incidentes	Desarrollar procedimientos claros para la identificación, reporte y manejo de incidentes de seguridad.	Alta	Respuesta más rápida y efectiva a los incidentes de seguridad.
	Control de Acceso Físico	Mejorar los controles de acceso físico a áreas críticas con sistemas de acceso electrónico y vigilancia.	Media	Prevención de accesos no autorizados y protección de activos físicos.

Fuente: Elaboración propia

Interpretación de la tabla 06: Las mejoras tecnológicas y procedimentales propuestas están enfocadas en reforzar la infraestructura de red de la Municipalidad Distrital de Punchana. Estas medidas buscan garantizar la protección adecuada de los datos, alineándose con los estándares internacionales de seguridad. Al implementar estas recomendaciones, se mitigarán riesgos potenciales, se incrementará la eficiencia operativa, y se asegurará la integridad y confidencialidad de la información manejada por la municipalidad. Esto contribuye a crear un entorno más seguro y confiable para la gestión de los sistemas de información.

CAPÍTULO V.- DISCUSIÓN:

Zúñiga (2020) analizó la red de la Facultad de Artes y Comunicación y encontró que la falta de estándares y topologías definidas generaba problemas en el rendimiento. De manera similar, en la Municipalidad de Punchana se identificó la ausencia de políticas de seguridad estandarizadas y configuraciones predeterminadas, lo que evidencia la necesidad de establecer directrices claras y una infraestructura de red uniforme para mejorar tanto la seguridad como el rendimiento.

Por su parte, Susanibar (2021), al evaluar la seguridad de la red de datos del Hospital Regional de Huacho, detectó la falta de un área específica dedicada a redes y la ausencia de auditorías sistemáticas. En Punchana se observó un panorama parecido, con debilidades en la gestión de incidentes y la inexistencia de políticas de seguridad formalmente documentadas. Esto subraya la importancia de contar con áreas especializadas y protocolos claros para proteger la información.

Álvarez (2021) señaló la urgencia de reestructurar el cableado estructurado en la Unidad de Seguros del Hospital Eleazar Guzmán Barrón debido a deficiencias en la red. En Punchana, también se evidenció la necesidad de actualizar tanto el hardware como los sistemas de red, lo que resalta que una infraestructura moderna es clave para garantizar la seguridad y el desempeño.

Fonseca (2021) propuso un esquema de seguridad para la empresa EURODIESEL, que incluyó pruebas de penetración y herramientas como Nmap y Metasploit. En el caso de Punchana, estas mismas herramientas permitieron detectar vulnerabilidades críticas, demostrando que las tecnologías avanzadas son esenciales para identificar y mitigar riesgos.

Lino (2021) realizó un análisis de redes inalámbricas, destacando la importancia de protocolos de seguridad robustos. En la Municipalidad de Punchana se detectó la ausencia de medidas como la autenticación multifactor y sistemas de

detección de intrusos, lo que coincide con los hallazgos de Lino respecto a la necesidad de implementar tecnologías avanzadas para proteger la red.

CAPÍTULO VI. - CONCLUSIONES:

Se detectaron fallas importantes en la red de datos de la Municipalidad Distrital de Punchana, entre ellas, configuraciones predeterminadas en los equipos de red y la falta de actualizaciones de software, lo cual facilita accesos no autorizados y eleva el riesgo de ataques cibernéticos. Además, la inexistencia de un firewall y de un sistema de detección de intrusos (IDS) agrava la exposición de la red, poniendo en peligro la integridad de toda la infraestructura. Esto deja en evidencia la necesidad urgente de implementar soluciones que refuercen la seguridad.

Los hallazgos muestran que la red enfrenta riesgos graves, como puertos abiertos innecesarios, software desactualizado y controles de acceso insuficientes, tanto físicos como lógicos. Adicionalmente, la falta de segmentación de la red y de sistemas de respaldo, sumado a la ausencia de capacitación en ciberseguridad para el personal, incrementa la vulnerabilidad global. Estos factores comprometen tanto la operación continua como la seguridad de la información que maneja la municipalidad.

Se constató que las políticas y procedimientos de seguridad de la municipalidad presentan deficiencias significativas. No existen políticas actualizadas ni bien definidas, lo que genera incertidumbre en la gestión de la seguridad de la red. Además, no se cuenta con procedimientos claros para responder a incidentes, lo que podría derivar en una respuesta desordenada frente a amenazas. Asimismo, los controles de acceso físico son insuficientes y no hay registros detallados de las actividades realizadas en la red, lo que limita el monitoreo y la trazabilidad de posibles fallas o amenazas.

Las mejoras propuestas tienen como finalidad solucionar las vulnerabilidades detectadas y reducir los riesgos en la red. Entre estas, se recomienda actualizar los equipos y sistemas, implementar un firewall, un IDS y establecer controles de acceso más estrictos. También se destaca la necesidad de desarrollar políticas de seguridad claras, diseñar procedimientos para gestionar incidentes y

capacitar al personal en ciberseguridad. Estas acciones no solo fortalecerán la infraestructura de la red, sino que también incrementarán la eficiencia operativa y garantizarán la protección de los datos e información sensibles de la municipalidad.

CAPÍTULO VII.- RECOMENDACIONES:

- Implementar un firewall y un sistema de detección de intrusos (IDS): Es crucial instalar y configurar un firewall junto con un IDS para monitorear, detectar y bloquear cualquier intento de acceso no autorizado o actividad maliciosa en la red. Esto permitirá un nivel de seguridad más robusto frente a ciberataques.

- Actualizar el software y el firmware de los equipos de red: Todos los dispositivos de la red deben ser actualizados de manera periódica para corregir vulnerabilidades conocidas y mejorar su rendimiento. Esto incluye switches, routers y demás componentes esenciales.

- Establecer políticas de seguridad claras y procedimientos de gestión de incidentes: Se deben redactar y aplicar políticas específicas sobre el manejo seguro de la información y la gestión de accesos. Además, es fundamental definir protocolos para actuar rápidamente en caso de un incidente de seguridad.

- Segmentar la red y reforzar los controles de acceso: Es importante dividir la red en subredes según las funciones o áreas operativas, lo cual reducirá los riesgos de propagación de ataques. Asimismo, se deben implementar medidas de autenticación más estrictas, como contraseñas robustas y autenticación multifactor.

- Capacitar al personal en ciberseguridad: Los usuarios y administradores de la red necesitan formación constante en prácticas seguras y en la identificación de posibles amenazas. La capacitación reducirá los errores humanos y fortalecerá la cultura de seguridad en la organización.

CAPÍTULO VIII.- REFERENCIAS BIBLIOGRÁFICAS:

Alvarez De La Fuente, C. A. Propuesta de reestructuración de cableado estructurado para la unidad de seguros del hospital Eleazar Guzmán Barrón-Nuevo Chimbote; 2021.

Fonseca Heras, J. W. (2021). Implementación de un esquema de seguridad para la red de datos de la empresa Eurodiesel (Bachelor's thesis).

Lino, E. A. M., Hernández, M. M. O., Zambrano, J. M. Y., & Rodríguez, A. (2021). Análisis de seguridad de las redes inalámbricas en la carrera de Tecnologías de Información. Serie Científica de la Universidad de las Ciencias Informáticas, 14(9), 139-147.

Susanibar, M., & Mirella, K. (2021). Evaluación de la seguridad de la red de datos del Hospital Regional de Huacho.

Zúñiga, C. D. A. (2020). Auditoría de la red inalámbrica en la Facultad de Artes y Comunicación. Anuario de Investigación UM, 1(1), 11-22.

Stallings, W. (2013). Data and Computer Communications. Pearson.

IT Governance Institute. (2012). COBIT 5: A Business Framework for the Governance and Management of Enterprise IT.

International Organization for Standardization. (2013). ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements.

Rittinghouse, J. W., & Ransome, J. F. (2017). Cybersecurity Operations Handbook. CRC Press.

Lyon, G. F. (2009). Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning. Insecure.Com LLC.

Orebaugh, A., Ramirez, G., Beale, J., & Wright, J. (2006). Wireshark & Ethereal Network Protocol Analyzer Toolkit. Syngress.

Peltier, T. R. (2013). Information Security Risk Analysis. CRC Press.

Johnson, R. (2015). Security Controls Evaluation, Testing, and Assessment Handbook. Syngress.

Souppaya, M., & Scarfone, K. (2008). Guide to Enterprise Telework and Remote Access Security (NIST Special Publication 800-46). National Institute of Standards and Technology.

Smith, A., & Brooks, D. J. (2012). Security Science: The Theory and Practice of Security. Butterworth-Heinemann.

Souppaya, M., & Scarfone, K. (2008). Guide to Enterprise Telework and Remote Access Security (NIST Special Publication 800-46). National Institute of Standards and Technology.

Erickson, J. (2008). Hacking: The Art of Exploitation. No Starch Press.

Calder, A., & Watkins, S. (2019). IT Governance: An International Guide to Data Security and ISO27001/ISO27002. Kogan Page Publishers.

Anexos.

- Matriz de consistencia

PROBLEMA	OBJETIVOS	HIPOTESIS	VARIABLES	DIMENSIÓN	INDICADORES	METODOLOGIA
Problema General ¿Cómo puede mejorar la Municipalidad Distrital de Punchana la seguridad de su red de datos mediante una auditoría exhaustiva que identifique y mitigue vulnerabilidades, evalúe la efectividad de las medidas actuales y proponga mejoras tecnológicas y procedimentales en el contexto de crecientes amenazas cibernéticas?	General ¿Cuáles son las vulnerabilidades y amenazas potenciales presentes en la red de datos de la Municipalidad Distrital de Punchana, y qué medidas correctivas y preventivas pueden implementarse para mitigar estos riesgos? ¿Qué tan efectivas y adecuadas son las políticas, procedimientos y controles de seguridad existentes en la municipalidad frente a las	No aplica	Auditoria de la red de datos	Identificación de Vulnerabilidades	Número de vulnerabilidades identificadas	Tipo y Diseño de la Investigación se clasifica como una investigación aplicada, descriptiva y exploratoria. Este enfoque permite identificar y evaluar de manera exhaustiva las vulnerabilidades de la red de datos, describir detalladamente el estado actual de la infraestructura y prácticas de seguridad, y explorar soluciones prácticas basadas en la evidencia recopilada. Población y Muestra Población: Incluye toda la infraestructura de red (dispositivos de red, servidores, estaciones de trabajo), el personal relacionado (empleados de TI y administrativos) y las políticas y
				Evaluación de Riesgos	Riesgo total asignado a cada vulnerabilidad	
				Revisión de Políticas y Procedimientos	Número de políticas y procedimientos evaluados	
					Porcentaje de cumplimiento con estándares de seguridad	

Problemas Específicos	normativas internacionales, nacionales y locales, y qué mejoras son necesarias? ¿Qué mejoras tecnológicas y procedimentales, incluyendo la actualización de herramientas de seguridad y la capacitación del personal, pueden recomendarse e implementarse para fortalecer la infraestructura de red y asegurar el cumplimiento de los estándares de seguridad? Específicos.					procedimientos de seguridad de la Municipalidad Distrital de Punchana. Muestra: Selección representativa de dispositivos críticos (2 routers, 2 switches, firewall principal), todos los servidores principales, 10 estaciones de trabajo seleccionadas aleatoriamente, todo el personal de TI (aproximadamente 5 personas) y 10 empleados administrativos de diferentes niveles y áreas, junto con todas las políticas de seguridad y procedimientos documentados. Técnicas de Recolección de Datos Entrevistas: Con el personal de TI y

						administrativo para entender prácticas de seguridad y uso de la red. Observación Directa: De prácticas operativas y configuraciones de dispositivos. Revisión Documental: Análisis de políticas de seguridad, procedimientos y registros de incidentes. Herramientas Automatizadas: Uso de Nmap, Nessus, Metasploit y Wireshark para escaneo y monitoreo de la red. Instrumentos de Recolección de Datos Guías de Entrevista: Conjuntos de preguntas predefinidas para entrevistas estructuradas y semiestructuradas. Listas de Verificación: Checklists para la observación directa.

						Software de Escaneo y Monitoreo: Nmap, Nessus, Metasploit, Wireshark. Documentos y Registros: Políticas de seguridad, procedimientos operativos, registros de configuración de red y logs de incidentes. Procedimiento de Recolección de Datos Planificación: Definición del cronograma y asignación de responsabilidades. Ejecución: Realización de entrevistas, observaciones y ejecución de herramientas de escaneo según lo planificado. Documentación: Registro sistemático de respuestas, observaciones y resultados de escaneos, y archivado de documentos revisados.

						Procesamiento y Análisis de Datos Organización de Datos: Clasificación y almacenamiento seguro de datos recolectados. Limpieza de Datos: Revisión y corrección de datos inconsistentes o incompletos. Análisis Cualitativo: Análisis de contenido de entrevistas y observaciones para identificar temas recurrentes y anomalías. Análisis Cuantitativo: Métodos estadísticos para analizar resultados de escaneos de vulnerabilidades. Evaluación de Riesgos: Uso de matrices de riesgo para clasificar y priorizar vulnerabilidades. Elaboración de Informes: Desarrollo de informes detallados con hallazgos y

						recomendaciones específicas. Presentación de Resultados: Preparación de presentaciones y resúmenes ejecutivos para comunicar resultados y recomendaciones.