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 DE SISTEMAS DE INFORMACIÓN

INFORME FINAL DE TESIS

ANÁLISIS DE LA SEGURIDAD INFORMÁTICA DE LA OFICINA DE SISTEMAS Y TECNOLOGÍAS DE LA INFORMACIÓN DE LA MUNICIPALIDAD PROVINCIAL DE MAYNAS – 2023

PARA OBTAR EL TITÚLO PROFESIONAL

INGENIERO DE SISTEMAS DE INFORMACIÓN

AUTORES:

- **BACH. TICIO BARDALES SINARAHUA**
- **BACH. ROBIN ANTONY CASTRO PLACIDO**

ASESOR:

- **ING. RONALD PERCY MELCHOR INFANTES, MGR.**

SAN JUAN BAUTISTA – MAYNAS – LORETO - PERÚ – 2024

DEDICATORIA

Para mis padres, cuyos sacrificios y amor han sido mi mayor inspiración y motivación en cada paso que he dado. A mis asesor y profesores, quienes con paciencia y dedicación han sembrado en mi el conocimiento y la pasión por aprender. A mis amigos, los cómplices de mis aventuras y las veces que siempre han resonado en mis momentos de alegrías y tristezas. A todos ustedes, mi profundo agradecimiento por ser los pilares de mi vida.

.BACH. TICIO BARDALES SINARAHUA

DEDICATORIA

A mis padres, por ser mi fuente inagotable de amor, apoyo y ejemplo de perseverancia. A mi hermano, por su constante inspiración y aliento en cada paso del camino. A mis amigos/as, por su inquebrantable compañía y complicidad en las buenas y en las malas. A mi asesor de tesis, por su invaluable guía y sabiduría que han marcado mi camino académico. A todos aquellos que de alguna manera han contribuido a este logro, ¡gracias!

Esta tesis está dedicada a ustedes, quienes han sido mi motivación constante.

BACH. ROBIN ANTONY CASTRO PLACIDO

AGRADECIMIENTO

A mis queridos padres, cuyo amor incondicional y apoyo constante han sido el motor que impulso cada paso de mi camino. A todos los que me brindaron su aliento y apoyo incondicional en este viaje, gracias por creer en mi incluso cuando yo dudaba. Vuestra confianza y aliento han sido el combustible que me ah llevado a alcanzar mis metas. Mi gratitud hacia ustedes es infinita.

BACH. TICIO BARDALES SINARAHUA

Quiero expresar mi profundo agradecimiento a todas las personas que contribuyeron de alguna manera a la realización de esta tesis. En primer lugar, agradezco a mi asesor de tesis por su orientación, paciencia y apoyo constante a lo largo de este proceso. También quiero agradecer a mis profesores/as, compañeros/as y amigos/as que me brindaron su ayuda, consejos y ánimo en momentos clave. Sus aportaciones fueron invaluables para enriquecer este trabajo.

Además, quiero reconocer el apoyo de mi familia por su amor incondicional y su comprensión durante este tiempo de dedicación a la investigación.

BACH. ROBIN ANTONY CASTRO PLACIDO

CONSTANCIA DE ORIGINALIDAD DEL TRABAJO DE INVESTIGACIÓN

"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:

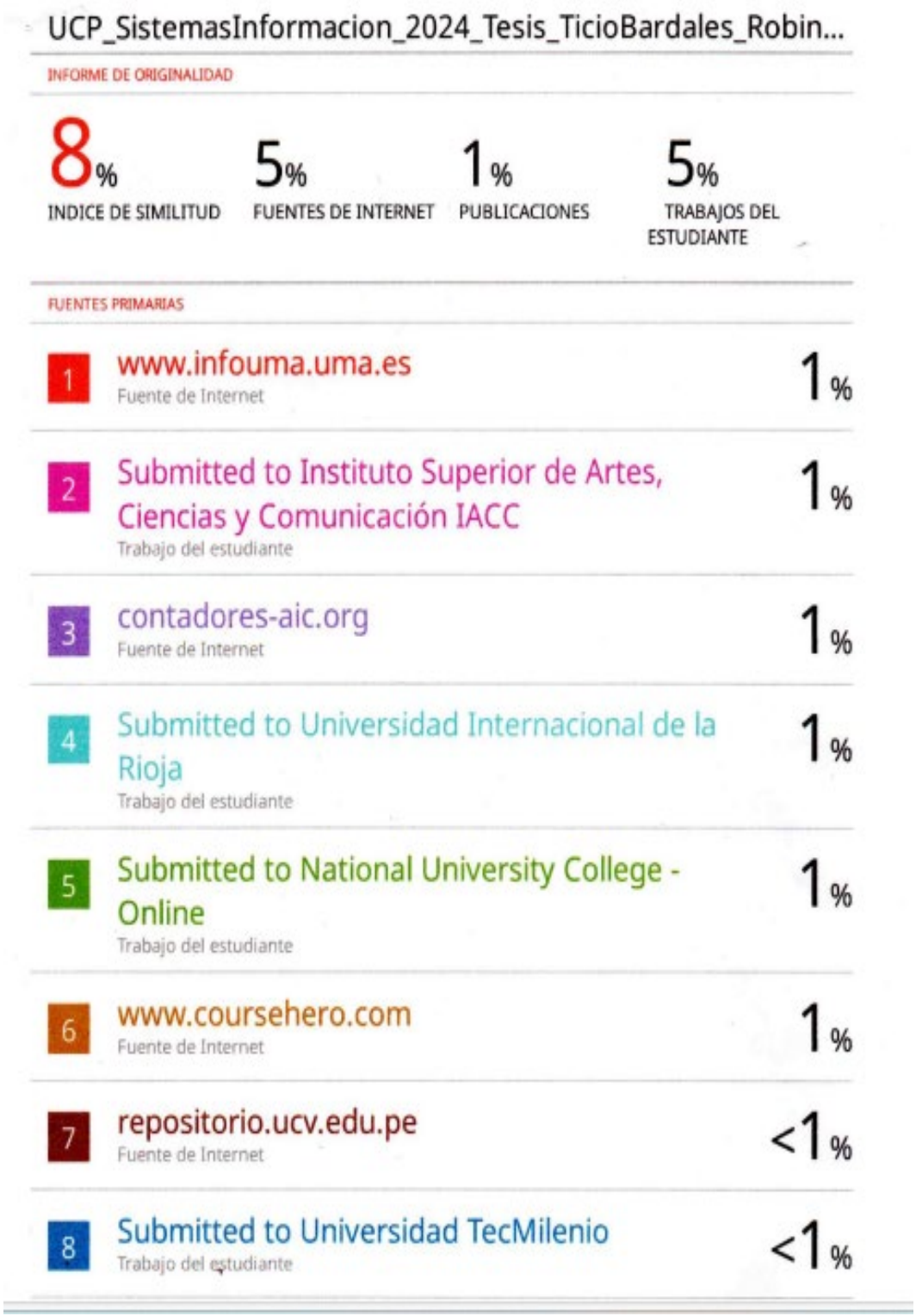
"ANÁLISIS DE LA SEGURIDAD INFORMÁTICA DE LA OFICINA DE SISTEMAS Y TECNOLOGÍAS DE LA INFORMACIÓN DE LA MUNICIPALIDAD PROVINCIAL DE MAYNAS – 2023"

De los alumnos: **TICIO BARDALES SINARAHUA Y ROBIN ANTONY CASTRO PLACIDO,** de la Facultad de Ciencias e Ingeniería, pasó satisfactoriamente la revisión por el Software Antiplagio, con un porcentaje de **8% de similitud**.
Se expide la presente, a solicitud de la parte interesada para los fines que estime conveniente.

San Juan, 24 de mayo del 2024.

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

JLTF/ri-a
199-2024



UCP_SistemasInformacion_2024_Tesis_TicioBardales_Robin...

INFORME DE ORIGINALIDAD

8%	5%	1%	5%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	www.infouma.uma.es Fuente de Internet	1%
2	Submitted to Instituto Superior de Artes, Ciencias y Comunicación IACC Trabajo del estudiante	1%
3	contadores-aic.org Fuente de Internet	1%
4	Submitted to Universidad Internacional de la Rioja Trabajo del estudiante	1%
5	Submitted to National University College - Online Trabajo del estudiante	1%
6	www.coursehero.com Fuente de Internet	1%
7	repositorio.ucv.edu.pe Fuente de Internet	<1%
8	Submitted to Universidad TecMilenio Trabajo del estudiante	<1%

turnitin

Recibo digital

Este recibo confirma quesu trabajo ha sido recibido por Turnitin. A continuación podrá ver la información del recibo con respecto a su entrega.

La primera página de tus entregas se muestra abajo.

Autor de la entrega:	Ticio Bardales Sinarahua
Título del ejercicio:	Quick Submit
Título de la entrega:	UCP_SistemasInformacion_2024_Tesis_TicioBardales_RobinC...
Nombre del archivo:	BARDALES_TICIO-CASTRO_ROBIN_Informe_Final_de_Tesis_EJ...
Tamaño del archivo:	259.21K
Total páginas:	33
Total de palabras:	7,710
Total de caracteres:	44,492
Fecha de entrega:	24-may.-2024 02:29a. m. (UTC+0700)
Identificador de la entre...	2386621903

ACTA DE SUSTENTACIÓN

FACULTAD DE CIENCIAS E INGENIERÍA

UNIVERSIDAD CIENTÍFICA DEL PERÚ

ACTA DE SUSTENTACIÓN DE TESIS

FACULTAD DE CIENCIAS E INGENIERÍA

Con Resolución Decanal N° 130-2024-UCP-FCEI del 22 de febrero del 2024, la Facultad de Ciencias e Ingeniería de la Universidad Científica del Perú - UCP designa como Jurado Evaluador de la tesis a los señores:

- Ing. Jimmy Max Ramírez Villacorta, Mtro. — Presidente
- Ing. Tonny Eduardo Bardales Lozano, Mgr. — Miembro
- Ing. Christian Alfredo Arévalo Jesús, Mtro. — Miembro

Como Asesor de la Tesis, Ing. Ronald Melchor Infantes Mtro

En la ciudad de Iquitos, siendo las **07:30 pm** del día **10 de junio de 2024,** supervisado por la Secretaria Académica del Programa de Ingeniería de Sistemas de Información de la Facultad de Ciencias e Ingeniería de la Universidad Científica del Perú, se constituyó el Jurado para escuchar la sustentación y defensa de la Tesis: ***ANALISIS DE LA SEGURIDAD INFORMÁTICA DE LA OFICINA DE SISTEMAS Y TECNOLOGÍAS DE LA INFORMACIÓN DE LA MUNICIPALIDAD PROVINCIAL DE MAYNAS 2023***

Presentado por las sustentantes

- BARDALES SINARAHUA TICIO

- CASTRO PLACIDO ROBIN ANTONY

Como requisito para optar el título Profesional de:

INGENIERO DE SISTEMAS DE INFORMACIÓN

Luego de escuchar la sustentación y formuladas las preguntas las que fueron: ABSUELTAS

El Jurado después de la deliberación en privado llegó a la siguiente conclusión:
Que la sustentación es APROBADA POR MAYORIA

En fe de lo cual los miembros del Jurado firman el acta.

Ing. Jimmy Max Ramírez Villacorta, Mtro.
Presidente

Ing. Christian Alfredo Arévalo Jesús, Mtro.
Miembro

Ing. Tonny Eduardo Bardales Lozano, Mgr
Miembro

HOJA DE APROBACIÓN

UNIVERSIDAD CIENTÍFICA DEL PERÚ

HOJA DE APROBACIÓN

PROGRAMA ACADÉMICO INGENIERÍA DE SISTEMAS INFORMACIÓN
TESISTAS: BARDALES SINARAHUA TICIO y CASTRO PLACIDO ROBIN ANTONY

Tesis sustentada en acto publico el 10 de junio de 2024, a las 7:30 pm en las instalaciones de la UNIVERSIDAD CIENTÍFICA DEL PERÚ.

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

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

ING. CHRISTIAN ALFREDO ARÉVALO JESÚS, MTRO.
MIEMBRO DE JURADO

ING. RONALD MELCHOR INFANTES MTRO.
ASESOR

INDICE DE CONTENIDO

Página

INDICE DE TABLAS

RESUMEN

La seguridad de la información se ha convertido en una preocupación creciente para organizaciones y entidades gubernamentales en la era digital, y la Oficina de Sistemas y Tecnologías de la Información de la Municipalidad Provincial de Maynas no es una excepción. La creciente amenaza de ciberataques y la necesidad de proteger los datos sensibles de la institución han destacado la importancia de evaluar y fortalecer su postura de seguridad informática, el objetivo principal de esta tesis fue evaluar el estado actual de la seguridad informática en la Oficina de Sistemas y Tecnologías de la Información de la Municipalidad Provincial de Maynas. Para lograr este objetivo, se plantearon una serie de objetivos específicos, que incluyeron evaluar la infraestructura tecnológica, analizar las políticas y procedimientos de seguridad informática, medir el nivel de cumplimiento de las normativas de seguridad, y evaluar la conciencia y capacitación en seguridad informática del personal, mediante un enfoque descriptivo y un diseño de investigación transversal, se recopilaron datos utilizando una combinación de encuestas, entrevistas y análisis de documentos. La población de estudio consistió en el personal de la Oficina de Sistemas y Tecnologías de la Información, con una muestra que incluyó a todos los empleados de la oficina, los resultados de la investigación revelaron una serie de áreas de mejora en la seguridad informática de la institución. Se identificaron vulnerabilidades en la infraestructura tecnológica, incluida una falta de actualizaciones de software, acceso privilegiado no controlado y dispositivos sin mantenimiento adecuado. Además, se encontró una falta de conciencia y capacitación en seguridad informática entre el personal, esta tesis destaca la importancia de abordar los desafíos de seguridad informática de manera integral en la Oficina de Sistemas y Tecnologías de la Información de la Municipalidad Provincial de Maynas. Se recomiendan medidas como la implementación de políticas de actualización proactiva, el fortalecimiento de los controles de acceso, la implementación de un sistema de monitoreo de incidentes y la promoción de la conciencia y capacitación en seguridad informática para mejorar la postura de seguridad de la institución.

Palabras claves: seguridad, informática, riesgos, vulnerabilidades.

ABSTRACT

Information security has become a growing concern for organizations and government entities in the digital age, and the Office of Systems and Information Technologies of the Provincial Municipality of Maynas is no exception. The increasing threat of cyberattacks and the need to protect sensitive data of the institution have highlighted the importance of evaluating and strengthening its cybersecurity posture. The main objective of this thesis was to assess the current state of information security in the Office of Systems and Information Technologies of the Provincial Municipality of Maynas. To achieve this objective, a series of specific goals were outlined, including evaluating the technological infrastructure, analyzing security policies and procedures, measuring compliance with security regulations, and assessing awareness and training in information security among personnel. Through a descriptive approach and a cross-sectional research design, data were collected using a combination of surveys, interviews, and document analysis. The study population consisted of personnel from the Office of Systems and Information Technologies, with a sample including all employees of the office. The research results revealed several areas for improvement in the institution's information security. Vulnerabilities in the technological infrastructure were identified, including a lack of software updates, uncontrolled privileged access, and devices without proper maintenance. Additionally, a lack of awareness and training in information security among personnel was found. This thesis underscores the importance of addressing information security challenges comprehensively in the Office of Systems and Information Technologies of the Provincial Municipality of Maynas. Measures such as implementing proactive update policies, strengthening access controls, implementing an incident monitoring system, and promoting awareness and training in information security are recommended to enhance the institution's security posture.

Keywords: security, information technology, risks, vulnerabilities.

CAPÍTULO I.- MARCO TEÓRICO:

1.1 Antecedentes de Estudio:

- ✓ Antecedentes Internacionales

Lissette Ochoa (2022) realizó una investigación centrada en diseñar políticas de seguridad de la información para la Universidad Indígena y Caribeña de Bluefields (BICU). El objetivo principal era proteger los datos y el equipo informático gestionado por la institución y sus diversos departamentos. La investigación se basó en identificar las vulnerabilidades de los datos universitarios para minimizar riesgos como la dispersión de datos y la pérdida de tiempo asociada a los recursos de TIC. Además, se propuso una estructura organizativa para garantizar el cumplimiento de estas políticas. Se destacó la importancia de estas políticas como herramientas fundamentales para proteger los recursos de TIC y fomentar el conocimiento tecnológico del personal. La investigación adoptó un enfoque descriptivo, con un diseño transversal que involucró a 9 trabajadores permanentes, 3 pasantes y 6 monitores, totalizando 18 participantes. La recolección de datos se realizó mediante entrevistas y encuestas, lo que reveló la falta de un documento que describiera las políticas de seguridad necesarias, lo que llevó a la propuesta de soluciones para abordar esta deficiencia.

Hurtado, Martínez y Jenifer Tamara (2022) realizaron una investigación monográfica con el objetivo principal de desarrollar políticas de seguridad de la información para la Universidad Indígena y Caribeña de Bluefields (BICU), con el fin de salvaguardar los datos y el equipo informático administrado por la institución y sus diversos departamentos. Para alcanzar este

propósito, era crucial identificar las vulnerabilidades de los datos universitarios, lo que serviría como punto de partida para mitigar riesgos relacionados con los recursos de TIC, como la dispersión de datos y la pérdida de tiempo. Además, se planteó la implementación de una estructura organizativa para asegurar el cumplimiento de estas políticas de seguridad de la información. Estas políticas fueron consideradas como herramientas esenciales para proteger los recursos de TIC de la universidad y promover el conocimiento tecnológico del personal, crucial para el adecuado funcionamiento y aprovechamiento de estos activos. El enfoque de la investigación fue descriptivo, detallando las características y cualidades de las variables con un diseño transversal enfocado en un período de tiempo definido. La población de estudio incluyó a 9 trabajadores permanentes, 3 pasantes y 6 monitores, con un total de 18 participantes. La recolección de datos se realizó mediante entrevistas y encuestas, aplicadas después de informar sobre el propósito de la investigación. Los resultados revelaron la carencia de un documento que delineara las políticas de seguridad necesarias para proteger los recursos de TIC en la institución, lo que llevó a la propuesta de abordar esta problemática.

Cedeño, Marco (2022), se dedicó a establecer un marco de referencia para la implementación de controles de seguridad informática en una empresa especializada en la fabricación, comercialización y exportación de muebles. Este marco se inició con un análisis de los antecedentes de seguridad informática de la organización, que reveló que las medidas de seguridad existentes no cubrían todos los activos que requerían protección ni estaban coordinadas entre sí. Por lo tanto, se planteó la necesidad de implementar controles basados en algún estándar

de la industria. Se eligió la norma CIS versión 8, que proporciona puntos de control específicos para pequeñas empresas en etapas iniciales de implementación de controles de seguridad informática. El objetivo del desarrollo del marco de referencia fue proporcionar a la organización pautas claras para implementar los controles de la versión 8 de CIS, permitiéndole gestionar formalmente su ciberseguridad en el futuro.

- ✓ Antecedentes Nacionales:

Asurza, Josue (2022), en su investigación adoptó un enfoque experimental, se evaluaron diversas propuestas de software de seguridad mediante un perfil de características predefinido, considerando el cumplimiento de la integridad, confidencialidad y disponibilidad, pilares esenciales de la protección de la información, los resultados obtenidos evidenciaron mejoras en las dimensiones de seguridad de la información en comparación con la situación actual de la empresa auditada.

Moron, Peredo & Kristopher Renzo (2023), Llevaron a cabo una investigación de campo que les permitió elaborar una propuesta de modelo viable para abordar los problemas de seguridad de la información en la empresa, utilizando a Rash Perú S.A.C. como caso de estudio. La metodología empleada se basó en el ciclo de Deming, haciendo referencia a la Norma ISO 27002 y empleando una combinación de metodologías para evaluar los riesgos y tomar decisiones informadas sobre las opciones de tratamiento adecuadas. Los resultados en seguridad de la información se evaluaron a través de un pre test, además, se observó que el valor mínimo del pre test fue del 50% y el máximo del 88%, mientras que en el post test el mínimo fue del 0% y el máximo del 27%. Se determinó que el nivel de significancia en el pre test fue de 0.265 y para el post test de 0.108,

indicando que el indicador se ajusta a una distribución normal o paramétrica (P > 0.05). La tesis está organizada en seis capítulos, donde se aborda cada tema relacionado con la propuesta de diseño, sus resultados y su aplicación.

- ✓ Antecedentes Locales:

No se encontraron antecedentes locales

1.2 Bases Teóricas:

Seguridad Informática:

La seguridad informática son las medidas que prevenga la ejecución de operaciones no autorizadas en un sistema o red informática que puedan ocasionar daños a la información, el equipo o el software. Gómez (2006).

Kissel (2012) es la protección de la información y los sistemas de información de accesos no autorizados. La seguridad informática se relaciona con tres elementos básicos: la información, el software y el hardware.

Es el conjunto de medidas técnicas, organizativas y legales destinadas a proteger los sistemas informáticos, redes y dispositivos contra el acceso no autorizado, la modificación, divulgación, destrucción o interrupción de los servicios que estos sistemas proporcionan.

La seguridad informática busca garantizar la integridad, confidencialidad y disponibilidad de los datos, así como prevenir la interrupción o el mal funcionamiento de los sistemas informáticos. Se ha vuelto cada vez más importante a medida que los sistemas informáticos se han vuelto más complejos y las amenazas informáticas más sofisticadas. Morales (2022)

Tipos de Seguridad Informática:

La seguridad lógica abarca la protección del software y los datos almacenados en sistemas o redes, englobando la utilización de contraseñas robustas, la verificación de la identidad de los usuarios, la gestión eficiente de permisos de acceso, la implementación de firewalls para filtrar el tráfico no autorizado y el cifrado de información sensible.

La seguridad física se concentra en resguardar los dispositivos físicos y restringir el acceso a ellos, mediante medidas como el control de acceso a instalaciones, el uso de cerraduras de alta seguridad, la vigilancia en áreas críticas y la protección física de equipos de cómputo contra robos o daños.

La seguridad de la información implica salvaguardar los datos almacenados en sistemas o redes, involucrando la aplicación de políticas de seguridad bien definidas, la gestión eficaz de accesos a la información y la implementación de medidas para prevenir la pérdida de datos, ya sea por causas internas o externas.

La seguridad de red se enfoca en proteger las infraestructuras informáticas y los datos que circulan a través de ellas, mediante la instalación de firewalls para controlar el flujo de datos, la autenticación de usuarios para evitar accesos no autorizados, el establecimiento de redes privadas virtuales (VPN) para garantizar la confidencialidad de la información transmitida, la monitorización del tráfico de red y la prevención de ataques de denegación de servicio (DoS).

La seguridad de aplicaciones se dedica a proteger las aplicaciones de software utilizadas en sistemas o redes, abarcando prácticas de codificación segura para evitar vulnerabilidades, la gestión adecuada de

permisos de acceso a las aplicaciones y la adopción de medidas para prevenir ataques informáticos dirigidos a estas aplicaciones.

El campo de la seguridad informática está en constante evolución, con la aparición continua de nuevas amenazas y técnicas maliciosas. Por lo tanto, es crucial mantenerse al día con las últimas tendencias y mejores prácticas en seguridad informática para garantizar una protección efectiva de los sistemas y redes.

Entre los objetivos clave se encuentra la autenticación, que se encarga de verificar la identidad de los usuarios que intentan acceder al sistema o a la información. Asimismo, la autorización es fundamental para asegurar que los usuarios solo puedan acceder a la información y recursos para los que están autorizados. Además, la responsabilidad es crucial para garantizar que se pueda rastrear y responsabilizar a los usuarios por sus acciones en el sistema.

Otro objetivo importante es asegurar el no repudio, que busca evitar que una entidad niegue haber realizado una acción en el sistema, lo que contribuye a mantener la integridad y confiabilidad de las operaciones realizadas. Por último, es esencial proteger la seguridad física del hardware y los dispositivos que dependen de la seguridad informática, ya que estos activos pueden ser vulnerables a riesgos como robos o daños físicos.

1.3 Definición de Términos Básicos:

- Informática: Disciplina que se ocupa del procesamiento, almacenamiento y transmisión de información mediante tecnologías y sistemas computacionales.
- Riesgo: Probabilidad de que ocurra un evento no deseado o un resultado inesperado, y las consecuencias negativas que podrían derivarse de ello.
- Amenaza: Cualquier evento o acción potencial que pueda provocar daño, pérdida o interrupción de los recursos o activos de una organización o individuo.

- Seguridad: Estado de estar libre de peligros, daños o riesgos, logrado mediante la implementación de medidas preventivas y de protección contra posibles amenazas.

CAPÍTULO II.- PLANTEAMIENTO DEL PROBLEMA:

2.1 Descripción del Problema:

La seguridad de la Tecnología de la Información y la protección de la información son temas de creciente preocupación tanto para organizaciones como para administraciones públicas. Los recientes ciberataques han expuesto la vulnerabilidad de muchas empresas, lo que ha llevado a una mayor valoración de la seguridad informática y la ciberseguridad. Estas medidas son cruciales para identificar y eliminar vulnerabilidades, protegerse contra intrusos y evitar que información confidencial, privilegiada y datos personales caigan en manos no autorizadas, en el caso específico de la municipalidad provincial de Maynas, se evidencia que los procesos de extracción, copia o borrado de información, tanto de los trabajadores como de los usuarios de la entidad, conllevan riesgos significativos. Dado que hay cambios frecuentes en el personal, la gestión de la seguridad se vuelve más compleja. Además, la situación se agrava debido a que 10 trabajadores tienen acceso a más de una computadora de las 16 disponibles en la oficina. Esto aumenta las posibilidades de robo o eliminación accidental de información crucial, para evitar pérdidas económicas y de información, es imperativo implementar medidas de seguridad adecuadas en la municipalidad. Es necesario establecer políticas y procedimientos claros para garantizar que solo el personal autorizado tenga acceso a información sensible. Asimismo, se deben tomar medidas para reforzar la protección de los equipos físicos y asegurar que los datos estén respaldados regularmente, la seguridad de la Tecnología de la Información y de la información en sí misma es un desafío que requiere una atención urgente en la municipalidad provincial de Maynas, al adoptar medidas efectivas de seguridad informática, la institución puede salvaguardar su información valiosa y proteger los intereses de los ciudadanos y trabajadores involucrados.

La Oficina de Sistemas y Tecnología de la Información de la Municipalidad Provincial de Maynas enfrenta desafíos significativos en cuanto a la seguridad informática. A medida que la dependencia se encarga de gestionar

la infraestructura tecnológica y la información crítica de la institución, la seguridad se convierte en una preocupación crucial. Los incidentes de ciberseguridad en el ámbito municipal han aumentado en los últimos años, lo que ha puesto en riesgo la confidencialidad, integridad y disponibilidad de los datos almacenados y procesados en sus sistemas.

El problema se centra en la falta de una estrategia integral de seguridad informática en la Oficina de Sistemas y Tecnología de la Información, lo que ha llevado a diversas vulnerabilidades y riesgos potenciales para la institución.

2.2 Formulación del Problema:

2.2.1 Problema General:

- ✓ ¿Cuál es el estado situacional de la seguridad Informática de la Oficina de Sistemas y Tecnologías de la Información de la Municipalidad Provincial de Maynas?

2.2.2 Problemas Específicos:

- ✓ ¿Cuál es el estado actual de la infraestructura tecnológica utilizada por la Oficina de Sistemas y Tecnologías de la Información en términos de actualización y protección contra vulnerabilidades en el año 2023?
- ✓ ¿Cuál es el estado actual de riesgos de seguridad informática en la Oficina de Sistemas y Tecnologías de la Información en términos de actualización y protección contra vulnerabilidades en el año 2023?
- ✓ ¿Cuál es el estado actual de las vulnerabilidades de seguridad informática en la Oficina de Sistemas y Tecnologías de la Información en términos de actualización y protección contra vulnerabilidades en el año 2023?

2.3 Objetivos:

2.3.1 Objetivo General:

- ✓ Evaluar estado situacional de la seguridad Informática de la Oficina de Sistemas y Tecnologías de la Información de la Municipalidad Provincial de Maynas.

2.3.2 Objetivos Específicos:

1. Evaluar el estado actual de la infraestructura tecnológica utilizada por la Oficina de Sistemas y Tecnologías de la Información en términos de actualización y protección contra vulnerabilidades en el año 2023.
2. Evaluar los riesgos de seguridad informática en la Oficina de Sistemas y Tecnologías de la Información de la Municipalidad Provincial de Maynas en el año 2023, y cómo han sido efectivos en la protección de los activos de información.
3. Evaluar las vulnerabilidades de seguridad informática en la Oficina de Sistemas y Tecnologías de la Información de la Municipalidad Provincial de Maynas en el año 2023.

2.4 Hipótesis:

- No Aplica.

2.5 Variables:

2.5.1 Identificación de Variables:

- **Variable:** Análisis de la seguridad informática

2.5.1.1 Definición conceptual:

Tabla N° 01.- Definición conceptual de la variable

Variable	Definición Conceptual	Definición Operacional
Análisis de la seguridad informática	Es el nivel de seguridad informática es una medida crítica para garantizar la protección de los activos y datos de una organización y minimizar los riesgos de los ciberataques.	Es la medición del grado de protección y resiliencia de los sistemas y datos de una organización contra posibles amenazas y ataques cibernéticos.

Fuente: Elaboración Propia

2.5.1.2 Operacionalización de las Variables:

Tabla N° 02.- Operacionalización de variables

Variables	Dimensiones	Indicadores	Instrumento de Recolección de Datos
Nivel de Seguridad Informática	Infraestructura tecnológica de Hardware y Software	Mantenimiento preventivo de dispositivos	Encuesta Documental
		Porcentaje de sistemas y aplicaciones actualizados	
		Porcentaje de usuarios con acceso privilegiado y control de acceso	
		Número de incidentes de seguridad reportados	
	Evaluación de Riesgos	Porcentaje de riesgos identificados	
		Grado de impacto de los riesgos	
		Eficacia de las medidas de mitigación	
	Análisis de Vulnerabilidades	Porcentaje de vulnerabilidades identificados	
		Nivel de criticidad de las vulnerabilidades	
		Tiempo de resolución de vulnerabilidades	

Fuente: Elaboración Propia

CAPÍTULO III.- METODOLOGÍA:

3.1 Tipo y Diseño de Investigación:

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

Descriptiva porque vamos a describir el estado situacional de los activos informáticos de la Municipalidad Provincial de Maynas., en términos cuantitativos para ellos recopilaremos y análisis de datos numéricos mediante encuestas, cuestionarios, observaciones y análisis de datos secundarios.

- **Diseño de la Investigación:**

Diseño transversal: Este diseño se utiliza para recopilar datos en un solo punto en el tiempo. Los participantes se seleccionan en un momento específico y se recopilan datos de ellos en ese momento.

3.2 Población y Muestra:

Población

La población para esta investigación estará conformada por el personal que labora en la oficina de sistemas y tecnologías de la información de la Municipalidad Provincial de Maynas que haciende a 05 personas, distribuido de la siguiente manera:

Tabla 03: Población de la investigación

Cargo	Cantidad
Jefe de Oficina	01
Analista de sistemas	01
Programador de sistemas	01
Técnico en soporte informático	02
Total	05

Muestra

Como la muestra es finita y no sobre pasa las 30 personas se tomará como muestra a toda la población, osea los 5 trabajadores de la oficina de sistemas y tecnologías de la información de la Municipalidad Provincial de Maynas

3.3 Técnicas, instrumentos y procedimientos de recolección de datos:

- **Técnica de Recolección de Datos:**

Encuestas: Diseñar y distribuir encuestas entre el personal de la oficina de sistemas y tecnologías de la información para recopilar información sobre su percepción de la seguridad informática, nivel de conciencia y capacitación, y cumplimiento de políticas y procedimientos de seguridad.

Entrevistas estructuradas: Realizar entrevistas estructuradas con los responsables de la seguridad informática y otros miembros clave del personal para obtener información detallada sobre el estado actual de la infraestructura tecnológica, políticas de seguridad implementadas y desafíos enfrentados.

Observación directa: Observar directamente las prácticas y procedimientos en la oficina de sistemas y tecnologías de la información para evaluar la implementación de políticas de seguridad, el manejo de datos y el acceso a la infraestructura tecnológica.

- **Instrumento de Recolección de Datos:**

Cuestionario de seguridad informática: Diseñar un cuestionario estructurado que aborde aspectos específicos de la seguridad informática, como la infraestructura tecnológica, políticas y procedimientos de

seguridad, conciencia y capacitación del personal, y cumplimiento de normativas.

Guía de entrevista: Elaborar una guía de entrevista con preguntas específicas sobre temas relevantes para la seguridad informática, que pueda ser utilizada durante las entrevistas con el personal y los responsables de seguridad informática.
Lista de verificación de observación: Preparar una lista de verificación detallada que contenga los aspectos clave a observar durante la observación directa en la oficina de sistemas y tecnologías de la información, como el acceso físico a los equipos, la gestión de contraseñas y el cumplimiento de políticas de seguridad.

- **Procedimiento de Recolección de Datos:**

Diseño y distribución de encuestas: Crear encuestas en línea o en papel, y distribuirlas entre el personal de la oficina de sistemas y tecnologías de la información. Establecer un período de tiempo para la recopilación de respuestas y enviar recordatorios si es necesario.

Entrevistas estructuradas: Programar entrevistas con los responsables de seguridad informática y otros miembros del personal relevante. Registrar las respuestas de manera sistemática y asegurarse de cubrir todos los temas relevantes según la guía de entrevista.

Observación directa: Realizar observaciones directas en la oficina de sistemas y tecnologías de la información durante un período de tiempo determinado. Tomar notas detalladas sobre las prácticas y procedimientos observados, y registrar cualquier hallazgo relevante.

3.4 Procesamiento y análisis de datos:

Procesamiento de datos:

Organización de datos: Reúne todos los datos recolectados de las encuestas, entrevistas y observaciones en un único lugar, ya sea una hoja de cálculo, una base de datos o un software de análisis estadístico. Asegúrate de que los datos estén organizados de manera clara y estructurada.

Limpieza de datos: Revisa los datos para identificar y corregir posibles errores, inconsistencias o valores atípicos que puedan afectar la calidad de los resultados. Esto podría incluir la eliminación de respuestas incompletas o ambiguas, así como la estandarización de formatos.

Codificación de datos: Asigna códigos o etiquetas a los datos para facilitar su análisis posterior. Por ejemplo, puedes asignar códigos numéricos a las respuestas de las encuestas o categorías a las respuestas de las entrevistas.

Análisis de datos:

Análisis descriptivo: Comienza con un análisis descriptivo para obtener una visión general de los datos. Esto podría incluir la creación de tablas y gráficos para visualizar la distribución de respuestas, calcular medidas de tendencia central y dispersión, y explorar relaciones entre variables.

Análisis cualitativo: Si has recolectado datos cualitativos a través de entrevistas o observaciones, realiza un análisis temático para identificar patrones, tendencias y temas recurrentes en los datos. Puedes utilizar técnicas como la codificación abierta, axial y selectiva para organizar y categorizar los datos.

Análisis comparativo: Si has recolectado datos de diferentes grupos o momentos en el tiempo, realiza un análisis comparativo para identificar diferencias significativas entre ellos. Esto podría implicar comparar respuestas entre diferentes departamentos o períodos de tiempo, o identificar tendencias a lo largo del tiempo.

Interpretación de resultados: Una vez que hayas completado el análisis de los datos, interpreta los resultados en función de tus objetivos de investigación y preguntas de investigación. Identifica hallazgos clave, patrones emergentes y áreas de interés para profundizar en futuras investigaciones o acciones.

Generación de conclusiones: Finalmente, genera conclusiones basadas en tus análisis y presenta los hallazgos de manera clara y concisa. Destaca las implicaciones prácticas de tus resultados y ofrece recomendaciones para mejorar la seguridad informática en la Oficina de Sistemas y Tecnologías de la Información de la Municipalidad Provincial de Maynas.

CAPÍTULO IV.- RESULTADOS:

Objetivo 1: Evaluar el estado actual de la infraestructura tecnológica utilizada por la Oficina de Sistemas y Tecnologías de la Información en términos de actualización y protección contra vulnerabilidades en el año 2023.

Dimensión: Infraestructura tecnológica.

Indicador: Mantenimiento preventivo de dispositivos

Tabla 04: Dispositivos que han recibido mantenimiento preventivo

Dispositivos	Fecha	Descripción del mantenimiento	Evaluación de la seguridad de la información
Servidores de aplicaciones	29/06/2023	Actualización de firmware y revisión de componentes	Alta - Se han realizado acciones de mantenimiento que contribuyen a la seguridad de la información en estos servidores.
Servidor de base de datos	10/08/2023	Actualización de firmware y revisión de componentes	Alta - El mantenimiento preventivo ha mejorado la seguridad de la información en el servidor de base de datos.
Servidor de dominio	10/08/2023	Actualización de firmware y revisión de componentes	Alta - El mantenimiento preventivo ha mejorado la seguridad de la información en el servidor de dominio.
Servidor web	21/09/2023	Actualización de firmware y revisión de componentes	Alta - Se han tomado medidas para garantizar la seguridad de la información en el servidor web.
Servidor de antivirus	20/09/2023	Actualización de firmware y revisión de componentes	Alta - El servidor de antivirus está actualizado y protegido, lo que contribuye a la seguridad de la información.
Servidor de respaldo	15/03/2023	Limpieza de polvo, verificación de software y antivirus	Media - Aunque se ha realizado mantenimiento, se recomienda realizar una actualización adicional del software de respaldo.
Estaciones de trabajo	01/12/2023	Limpieza de polvo, verificación de software y antivirus	Media - Se ha realizado mantenimiento básico, pero se recomienda una evaluación más exhaustiva de la seguridad de la información.
Lap Tops	No se ha realizado mantenimiento		Baja - La falta de mantenimiento puede dejar vulnerabilidades en la seguridad de la información.
Impresoras	No se ha realizado mantenimiento		Baja - La falta de mantenimiento puede dejar vulnerabilidades en la seguridad de la información.
Switches	No se ha realizado mantenimiento		Baja - La falta de mantenimiento puede dejar vulnerabilidades en la seguridad de la información.

Fuente: Elaboración Propia

Interpretación: Esta tabla 04 se proporciona una visión detallada del mantenimiento preventivo realizado en los diversos dispositivos de la red de la Oficina de Sistemas y Tecnologías de la Información. Además, incluye una

evaluación de la situación actual en términos de seguridad de la información para cada dispositivo, basada en el mantenimiento realizado o la falta del mismo.

Dimensión: Infraestructura tecnológica.

Indicador: Porcentaje de sistemas y aplicaciones actualizados.

Tabla 05: Porcentajes de sistemas y aplicaciones actualizados

Sistema / Aplicación	Porcentaje de actualización	Nivel de protección
Sistemas Operativos (Windows)	95%	Media
Paquete de Office	40%	Baja
Sistema de rentas	100%	Alta
Sistema de tramite documentario	100%	Alta
Sistema de recaudación	100%	Alta
SIAF	100%	Alta
SIGA	100%	Alta
Sistema de logística	100%	Alta
Base de Datos (SQL Server)	100%	Alta
Servidor Web	100%	Alta
Servidor de dominio	100%	Alta
Software Antivirus	100%	Alta

Fuente: Elaboración Propia

Interpretación: La tabla 05 muestra que la mayoría de los sistemas y aplicaciones están actualizados y tienen un nivel de protección alto, lo que es fundamental para garantizar la seguridad de la información en la Oficina de Sistemas y Tecnologías de la Información. Sin embargo, hay áreas de mejora identificadas, como la necesidad de actualizar el paquete de Office para mejorar la protección general.

Dimensión: Infraestructura tecnológica.

Indicador: Porcentaje de usuarios con acceso privilegiado y control de acceso.

Tabla 06: Usuarios con acceso privilegiado y control de acceso

Sistema	Acceso privilegiado	Control de acceso normal	Control de acceso limitado
Sistema de gestión de bases de datos	90%	5%	5%
Sistema de correo electrónico	80%	15%	5%
Sistema de gestión de usuarios	85%	10%	5%
Sistema de gestión de archivos	75%	20%	5%
Sistema de monitoreo de redes	95%	3%	2%

Fuente: Elaboración Propia

Interpretación:

En el Sistema de Gestión de Bases de Datos, el 90% de los usuarios tienen acceso privilegiado, lo que indica un alto nivel de usuarios con permisos amplios en este sistema. Solo el 5% de los usuarios tienen un control de acceso normal, mientras que otro 5% tiene un control de acceso limitado.

Para el Sistema de Correo Electrónico, el 80% de los usuarios tienen acceso privilegiado, lo que sugiere una cantidad significativa de usuarios con amplios permisos en este sistema. Un 15% de los usuarios tienen un control de acceso normal, y un 5% tienen un control de acceso limitado.

En el Sistema de Gestión de Usuarios, el 85% de los usuarios tienen acceso privilegiado, mostrando una cantidad considerable de usuarios con permisos elevados. El 10% de los usuarios tienen un control de acceso normal, mientras que el 5% restante tiene un control de acceso limitado.

En cuanto al Sistema de Gestión de Archivos, el 75% de los usuarios tienen acceso privilegiado, lo que indica que la mayoría de los usuarios tienen permisos amplios en este sistema. Un 20% de los usuarios tienen un control de acceso normal, y otro 5% tiene un control de acceso limitado.

Finalmente, en el Sistema de Monitoreo de Redes, el 95% de los usuarios tienen acceso privilegiado, lo que sugiere un alto número de usuarios con permisos

elevados en este sistema. Solo el 3% de los usuarios tienen un control de acceso normal, mientras que el 2% restante tiene un control de acceso limitado.

Dimensión: Infraestructura tecnológica.

Indicador: Número de incidentes de seguridad reportados.

Tabla 07: Número de incidentes de seguridad reportados

Mes	Tipo de incidente	Número de incidentes reportados
Enero	Intentos de Intrusión	2
	Malware	8
	Pérdida de Datos	2
Febrero	Intentos de Intrusión	3
	Malware	10
Marzo	Pérdida de Datos	1
Abril	Intentos de Intrusión	4
	Malware	4
	Pérdida de Datos	1
Mayo	Intentos de Intrusión	2
	Malware	18
	Pérdida de Datos	1
Junio	Intentos de Intrusión	3
	Malware	15
	Pérdida de Datos	2
Julio	Intentos de Intrusión	1
	Malware	17
	Pérdida de Datos	1
Agosto	Intentos de Intrusión	0
	Malware	11
	Pérdida de Datos	0
Setiembre	Intentos de Intrusión	0
	Malware	18
	Pérdida de Datos	0
Octubre	Malware	5
	Pérdida de Datos	1
Noviembre	Intentos de Intrusión	0
	Malware	6
	Pérdida de Datos	0
Diciembre	Intentos de Intrusión	0
	Malware	9
	Pérdida de Datos	1

Fuente: Elaboración Propia

Interpretación: la tabla 07 detalla el número de incidentes reportados a la Oficina de Sistemas y Tecnologías de la Información en cada mes del año 2023,

especificando el tipo de incidente, que incluye intentos de intrusión, malware y pérdida de datos.

Objetivo 2: Evaluar los riesgos de seguridad informática en la Oficina de Sistemas y Tecnologías de la Información de la Municipalidad Provincial de Maynas en el año 2023, y cómo han sido efectivos en la protección de los activos de información.

Dimensión: Evaluación de Riesgos

Indicador: Porcentaje de riesgos identificados

Tabla 08: Porcentaje de riesgos identificados

Área de riesgo	Porcentaje
Seguridad de la Red	25%
Seguridad de los Sistemas	30%
Gestión de Identidad y Acceso	15%
Seguridad de la Información	20%
Seguridad Física	10%

Fuente: Elaboración Propia

Interpretación:

Seguridad de la Red: Este área se refiere a los posibles riesgos asociados con la infraestructura de red, incluidos ataques de denegación de servicio (DDoS), intrusiones, interceptación de datos y vulnerabilidades en el enrutamiento de red. Los riesgos pueden surgir debido a configuraciones incorrectas, falta de actualizaciones de seguridad en los dispositivos de red y fallas en la detección de intrusiones.

Seguridad de los Sistemas: Este riesgo se relaciona con posibles vulnerabilidades en los sistemas operativos, aplicaciones y servicios utilizados en la infraestructura tecnológica. Puede incluir amenazas como malware, exploits de software, fallos de seguridad en sistemas operativos no parcheados y configuraciones inseguras en servidores y estaciones de trabajo.

Gestión de Identidad y Acceso: Este riesgo aborda las amenazas relacionadas con la autenticación, autorización y control de acceso a los recursos de la red.

Puede incluir riesgos como contraseñas débiles, acceso no autorizado a sistemas y datos, falta de autenticación de múltiples factores y gestión inadecuada de privilegios de usuario.

Seguridad de la Información: Se refiere a la protección de la confidencialidad, integridad y disponibilidad de la información almacenada y procesada en los sistemas de la organización. Los riesgos en esta área pueden incluir fugas de datos, acceso no autorizado a información confidencial, falta de cifrado de datos y brechas de seguridad en aplicaciones y bases de datos.

Seguridad Física: Este riesgo se relaciona con posibles amenazas físicas a la infraestructura tecnológica, como robo, daños por agua o fuego, acceso no autorizado a áreas restringidas y fallas en los sistemas de control de acceso físico. La falta de medidas de seguridad física adecuadas puede exponer los equipos y datos sensibles a riesgos significativos.

Dimensión: Evaluación de Riesgos

Indicador: Grado de impacto de los riesgos

Tabla 09: Grado de impacto de los riesgos

Área de riesgo	Impacto	Nivel
Seguridad de la Red	Pérdida de conectividad, interrupción del servicio, acceso no autorizado a la red.	Alto
Seguridad de los Sistemas	Pérdida de datos, interrupción del servicio, compromiso de la integridad de los sistemas.	Muy Alto
Gestión de Identidad y Acceso	Acceso no autorizado a datos y sistemas críticos, pérdida de la confidencialidad.	Muy Alto
Seguridad de la Información	Fuga de información confidencial, pérdida de la confianza de los clientes.	Alto
Seguridad Física	Daño o robo de equipos, interrupción del servicio debido a daños en la infraestructura.	Medio

Fuente: Elaboración Propia

Interpretación: En la tabla 09 proporciona una evaluación del impacto de los riesgos identificados en la Oficina de Sistemas y Tecnologías de la Información.

Cada riesgo se describe brevemente junto con su impacto potencial en términos de interrupción del servicio, pérdida de datos, acceso no autorizado y otros factores relevantes para la seguridad de la información y la operación de los sistemas.

Los niveles de impacto están categorizados como "Alto", "Muy Alto" y "Medio", lo que indica el grado de gravedad que cada riesgo representa para la organización.

Dimensión: Evaluación de Riesgos

Indicador: Eficacia de las medidas de mitigación

Tabla 10: Eficacia de las medidas de mitigación

Riesgo	Medida de mitigación	Eficacia
Vulnerabilidades de software desactualizado	Implementación de actualizaciones automáticas	Alta
Acceso no autorizado a sistemas	Autenticación de dos factores	Media
Pérdida de datos debido a fallos de hardware	Implementación de copias de seguridad regulares	Alta
Ataques de malware y ransomware	Instalación de software antivirus y antimalware	Alta
Acceso físico no autorizado a equipos	Implementación de medidas de seguridad física	Alta

Fuente: Elaboración Propia

Interpretación: En la tabla 10 se muestra las diferentes medidas de mitigación implementadas para abordar los riesgos identificados en cuanto a seguridad informática. La eficacia de cada medida se evalúa en términos de su capacidad para reducir o eliminar el riesgo asociado. Se observa que la mayoría de las medidas tienen una eficacia alta, lo que sugiere que están bien diseñadas y aplicadas para mitigar los riesgos específicos. Sin embargo, hay una medida con una eficacia media, lo que indica que puede ser necesario revisar y fortalecer esa medida para mejorar su capacidad para mitigar el riesgo correspondiente. En general, la tabla refleja un enfoque proactivo y bien estructurado para abordar los riesgos de seguridad informática en la organización.

Objetivo 3: Evaluar las vulnerabilidades de seguridad informática en la Oficina de Sistemas y Tecnologías de la Información de la Municipalidad Provincial de Maynas en el año 2023.

Dimensión: Evaluación de vulnerabilidades.

Indicador: Porcentaje de vulnerabilidades identificados

Tabla 11: Porcentaje de vulnerabilidades identificados

Vulnerabilidad	Vulnerabilidad especifica	Descripción	Porcentaje
Vulnerabilidades de red	Falta de filtrado de paquetes	La red no filtra adecuadamente los paquetes, lo que puede permitir que paquetes maliciosos ingresen a la red.	85%
	Configuraciones de firewall inadecuadas	La configuración incorrecta del firewall puede permitir el tráfico no autorizado a través de la red.	75%
	Puertos abiertos no necesarios	Los puertos abiertos que no son necesarios pueden dejar la red vulnerable a ataques.	70%
	Protocolos de red no seguros	El uso de protocolos de red no seguros puede exponer los datos a interceptación y manipulación.	80%
Vulnerabilidades de software	Falta de actualizaciones de software	Los sistemas no se mantienen actualizados, lo que deja abierta la posibilidad de explotar vulnerabilidades conocidas.	90%
	Uso de software obsoleto o sin soporte	El uso de software desactualizado o que ya no recibe soporte puede dejar sistemas vulnerables a nuevas amenazas.	85%
	Errores de programación y codificación	Los errores en el desarrollo de software pueden introducir vulnerabilidades que pueden ser explotadas por atacantes.	70%
	Uso de bibliotecas o componentes vulnerables	La inclusión de bibliotecas o componentes con vulnerabilidades conocidas puede comprometer la seguridad del sistema.	75%
Vulnerabilidades de acceso	Contraseñas débiles o predeterminadas	El uso de contraseñas fáciles de adivinar o contraseñas predeterminadas puede facilitar el acceso no autorizado.	80%
	Uso de credenciales compartidas	Compartir credenciales entre usuarios puede dificultar el seguimiento de la actividad del usuario y aumentar el riesgo de acceso no autorizado.	60%
	Falta de autenticación multifactor	La autenticación de un solo factor puede ser vulnerable a ataques de suplantación de identidad, mientras que la autenticación multifactor proporciona una capa adicional de seguridad.	90%
	Acceso no autorizado a sistemas o datos	La falta de controles de acceso adecuados puede permitir que usuarios no autorizados accedan a sistemas o datos sensibles.	75%
Vulnerabilidades de configuración	Configuraciones por defecto no modificadas	No cambiar las configuraciones predeterminadas puede dejar sistemas abiertos a ataques.	65%
	Permisos excesivos o mal configurados	Asignar permisos excesivos a usuarios o configurarlos incorrectamente puede permitir un acceso no autorizado a recursos sensibles.	70%
	Servicios o funciones innecesarias habilitadas	Habilitar servicios o funciones que no son necesarios puede aumentar la superficie de ataque del sistema.	80%
	Falta de auditoría de configuración	No realizar auditorías de configuración periódicas puede dejar sistemas vulnerables a cambios no autorizados.	75%
Vulnerabilidades físicas	Acceso físico no autorizado a equipos	La falta de controles de acceso físico puede permitir que personas no autorizadas accedan a hardware sensible.	85%
	Robo o pérdida de dispositivos de almacenamiento	La pérdida o robo de dispositivos de almacenamiento puede resultar en la exposición de datos sensibles.	80%

	Falta de controles de acceso físico	La ausencia de medidas de seguridad física puede permitir que personas no autorizadas accedan a instalaciones o equipos.	70%
	Daño accidental o intencional a hardware	Los daños causados por accidentes o acciones malintencionadas pueden afectar la disponibilidad y confidencialidad de los datos almacenados.	75%

Fuente: Elaboración Propia

Interpretación: En la tabla 11 se muestra diferentes tipos de vulnerabilidades identificadas en la Oficina de Sistemas y Tecnologías de la Información, junto con el porcentaje de identificación de cada una durante el período evaluado.

En general, se observa que las vulnerabilidades de acceso, como contraseñas débiles o predeterminadas y la falta de autenticación multifactor, tienen un alto porcentaje de identificación, lo que sugiere que la conciencia sobre estos problemas es relativamente alta.

Las vulnerabilidades relacionadas con la configuración, como configuraciones por defecto no modificadas y permisos excesivos o mal configurados, también muestran un porcentaje considerable de identificación.

Por otro lado, las vulnerabilidades físicas, como el acceso físico no autorizado a equipos y el robo o pérdida de dispositivos de almacenamiento, también son identificadas en un alto porcentaje, lo que indica una preocupación por la seguridad física de los activos.

Dimensión: Evaluación de vulnerabilidades.

Indicador: Nivel de criticidad de las vulnerabilidades

Tabla 12: Nivel de criticidad de las vulnerabilidades

Tipo de Vulnerabilidad	Nivel de Criticidad
Contraseñas débiles	Alto
Configuraciones por defecto	Medio
Falta de autenticación multifactor	Alto
Permisos excesivos o mal configurados	Medio
Acceso físico no autorizado	Alto
Robo o pérdida de dispositivos de almacenamiento	Alto

Fuente: Elaboración Propia

Interpretación: La tabla 12 presenta una lista de diferentes tipos de vulnerabilidades junto con su nivel de criticidad asociado. Estos niveles de criticidad indican el grado de riesgo que representan estas vulnerabilidades para la seguridad de la información y los sistemas de la Oficina de Sistemas y Tecnologías de la Información.

En este caso, las vulnerabilidades relacionadas con contraseñas débiles, configuraciones por defecto y falta de autenticación multifactor se consideran de alto nivel de criticidad, lo que sugiere que representan riesgos significativos para la seguridad. Por otro lado, las vulnerabilidades relacionadas con permisos excesivos o mal configurados, acceso físico no autorizado y robo o pérdida de dispositivos de almacenamiento se clasifican como de nivel medio a alto, lo que también indica que requieren atención prioritaria para mitigar su impacto potencial.

Dimensión: Evaluación de vulnerabilidades.

Indicador: Tiempo de resolución de vulnerabilidades.

Tabla 13: Tiempo de resolución de vulnerabilidades

Tipo de Vulnerabilidad	Tiempo de resolución (días)
Contraseñas débiles	30
Configuraciones por defecto	10
Falta de autenticación multifactor	12
Permisos excesivos o mal configurados	3
Acceso físico no autorizado	1
Robo o pérdida de dispositivos de almacenamiento	7

Fuente: Elaboración Propia

Interpretación: La tabla muestra el tiempo promedio necesario para resolver diferentes tipos de vulnerabilidades identificadas en el sistema de información.

Las contraseñas débiles tienen un tiempo de resolución de 30 días.

Las configuraciones por defecto requieren un promedio de 10 días para ser corregidas.

La falta de autenticación multifactor se resuelve en aproximadamente 12 días.

Los permisos excesivos o mal configurados tienen un tiempo de resolución más rápido, solo 3 días en promedio.

El acceso físico no autorizado se soluciona en solo 1 día en promedio.

Por último, el robo o pérdida de dispositivos de almacenamiento requiere 7 días para ser abordado.

Estos datos proporcionan información crucial sobre la eficiencia y la rapidez con la que se manejan las vulnerabilidades una vez identificadas en el sistema de información.

CAPÍTULO V.- DISCUSIÓN:

En comparación con los estudios de Hurtado, Martínez & Jenifer Tamara (2022) y Ochoa, Lissette (2022), se observa que, al igual que en la Universidad Indígena y Caribeña de Bluefields (BICU), la Oficina de Sistemas y Tecnologías de la Información de la Municipalidad Provincial de Maynas también enfrenta desafíos en la implementación de políticas de seguridad de la información. Ambas investigaciones destacan la importancia de diseñar políticas de seguridad efectivas y establecer una estructura organizativa para garantizar su cumplimiento.

Por otro lado, el estudio de Cedeño, Marco (2022) sobre la implementación de controles de seguridad informática en una empresa de fabricación y exportación de muebles resalta la necesidad de adoptar estándares de la industria y marcos de referencia para fortalecer la ciberseguridad. Este hallazgo es relevante para la Oficina de Sistemas y Tecnologías de la Información de la Municipalidad Provincial de Maynas, ya que también requiere un enfoque estructurado y basado en estándares para mejorar su postura de seguridad.

Al comparar los resultados con los estudios nacionales de Moron, Peredo & Kristopher Renzo (2023) y Asurza, Josue (2022), se puede apreciar que la implementación de un Sistema de Gestión de Seguridad de la Información puede ser beneficioso para mejorar la seguridad de la información en una organización. Este enfoque podría ser relevante para la Oficina de Sistemas y Tecnologías de la Información de la Municipalidad Provincial de Maynas, ya que podría proporcionar un marco estructurado y procesos definidos para gestionar la seguridad de la información de manera efectiva.

CAPÍTULO VI. - CONCLUSIONES:

- Se ha identificado que la mayoría de los sistemas y aplicaciones están actualizados, lo que contribuye a un nivel alto de protección contra vulnerabilidades. Sin embargo, se han observado algunas áreas de mejora, como la baja tasa de actualización en el paquete de Office, lo que podría representar un riesgo para la seguridad de la información.
- La mayoría de los usuarios tienen acceso privilegiado a los sistemas, lo que podría aumentar el riesgo de brechas de seguridad si no se gestionan adecuadamente. Además, se ha observado una falta de control de acceso normal y limitado en algunos sistemas, lo que indica una necesidad de mejorar las políticas de acceso.
- Aunque no se han proporcionado cifras concretas en esta investigación, se ha constatado la existencia de incidentes de seguridad reportados a la Oficina de Sistemas y Tecnologías de la Información en el año 2023. Esto sugiere la importancia de implementar medidas adicionales para prevenir y gestionar estos incidentes de manera efectiva.
- Se han identificado varios riesgos de seguridad de la información, como contraseñas débiles, configuraciones por defecto y acceso físico no autorizado. Estos riesgos pueden representar amenazas significativas para la confidencialidad, integridad y disponibilidad de los datos de la organización.
- Aunque se han implementado medidas de mitigación para abordar algunos de los riesgos identificados, su eficacia puede variar. Es necesario realizar una evaluación continua de estas medidas para garantizar que sigan siendo efectivas frente a las amenazas emergentes.

CAPÍTULO VII.- RECOMENDACIONES:

- Implementar políticas de actualización proactiva: Se recomienda establecer políticas formales que promuevan la actualización regular de todos los sistemas y aplicaciones utilizados por la Oficina de Sistemas y Tecnologías de la Información. Esto incluye sistemas operativos, software de productividad (como paquetes de Office) y cualquier otro software utilizado en la infraestructura tecnológica. Estas políticas deberían incluir procedimientos claros para garantizar que las actualizaciones se realicen de manera oportuna y se monitoreen de forma regular.
- Fortalecer la gestión de acceso de usuarios: Es crucial implementar controles de acceso adecuados para garantizar que solo los usuarios autorizados tengan acceso privilegiado a los sistemas y datos sensibles. Esto puede lograrse mediante la implementación de políticas de control de acceso basadas en roles, la revisión regular de los privilegios de usuario y la implementación de autenticación multifactor para aumentar la seguridad de las cuentas de usuario.
- Establecer un sistema de monitoreo de incidentes de seguridad: Se recomienda implementar un sistema de monitoreo de seguridad robusto que pueda detectar y responder rápidamente a posibles incidentes de seguridad. Esto podría incluir la implementación de herramientas de detección de intrusiones, registros de eventos de seguridad y protocolos claros para la notificación y gestión de incidentes de seguridad.
- Realizar evaluaciones de riesgos regulares: Es importante realizar evaluaciones de riesgos de manera regular para identificar y mitigar posibles vulnerabilidades en la infraestructura tecnológica. Esto puede incluir evaluaciones de vulnerabilidades de software, pruebas de penetración y evaluaciones de riesgos físicos para garantizar una visión integral de los riesgos de seguridad.

- Promover la conciencia y capacitación en seguridad informática: Se debe proporcionar capacitación regular sobre seguridad informática a todo el personal de la Oficina de Sistemas y Tecnologías de la Información para aumentar la conciencia sobre las amenazas de seguridad y fomentar prácticas seguras en el uso diario de la tecnología. Esto puede incluir sesiones de capacitación sobre buenas prácticas de seguridad, procedimientos de manejo de datos sensibles y cómo reconocer y reportar posibles incidentes de seguridad.

CAPÍTULO VIII.- REFERENCIAS BIBLIOGRÁFICAS:

- Limones, G. & Muñoz B., tesis titulada “Diseño e Implementación para el control y gestión de pagos de pensiones para la fundación Niños con futuro de la ciudad de Guayaquil – Ecuador 2017, disponible en:
- https://dspace.ups.edu.ec/bitstream/123456789/14163/1/UPS-GT001842.pdf

- Muñoz, P.; Tesis titulada “Implementación de una Aplicación Web para el Control de inventario y facilitación de material de trabajo para Empresa Maderas BSC Ltda., disponible en:
- http://repobib.ubiobio.cl/jspui/bitstream/123456789/675/1/Mu%C3%B1oz%20Mondaca%2C%20Pablo%20Ignacio.pdf

- Ipanaqué, Y.; Tesis titulada “Desarrollo de una aplicación web para la mejora del proceso de venta de equipos informáticos en la empresa suministros tecnológicos Terabyte, disponible en:
- http://repositorio.uigv.edu.pe/handle/20.500.11818/1762

- Chávez, J.; Tesis titulada “Implementación de un Sistema Web para Optimizar el Proceso de Gestión de Cobranza en la Empresa Service Collection; disponible en: http://repositorio.ulasamericas.edu.pe/bitstream/handle/upa/258/IMPLEMENTACI%C3%93N%20DE%20UN%20SISTEMA%20WEB%20PARA%20OPTIMIZAR%20EL%20PROCESO%20DE%20GESTI%C3%93N%20DE%20COBRANZA%20EN%20LA%20EMPRESA%20SERVICE.pdf?sequence=1&isAllowed=y

- Cross, Robert (1997). Revenue Management: Hard-Core Tactics for Market Dominatio. Crown Business. p. 288. ISBN 0767900332.

- Talluri, K; van Ryzin, G. (1999). «Revenue Management: Research Overview and Prospects». Transportation Science 33: 233-256.

- Nagle, Thomas (2010). The Strategy and Tactics of Pricing: A Guide to Growing More Profitably. Prentice Hall. p. 352. ISBN 0136106811.

ANEXOS:

Anexo 1.- Documento de autorización:

CARTA DE AUTORIZACIÓN

ANÁLISIS DE LA SEGURIDAD INFORMÁTICA DE LA OFICINA DE SISTEMAS Y TECNOLOGÍAS DE LA INFORMACIÓN DE LA MUNICIPALIDAD PROVINCIAL DE MAYNAS – 2023

El que suscribe, Ingeniero de Sistemas e Informática José Abel Arbildo Paz, jefe de la oficina de sistemas y tecnologías de información, autoriza a los Bachilleres TICIO BARDALES SINARAHUA y ROBIN ANTONY CASTRO PLACIDO, para realizar una evaluación de la red de datos, como parte del desarrollo de su tesis titulada "**ANÁLISIS DE LA SEGURIDAD INFORMÁTICA DE LA OFICINA DE SISTEMAS Y TECNOLOGÍAS DE LA INFORMACIÓN DE LA MUNICIPALIDAD PROVINCIAL DE MAYNAS – 2023**", en la facultad de Ciencias e Ingeniería, programa académico de Ingeniería de Sistemas de Información.

Iquitos, 28 de diciembre del 2023

Atentamente,

_____

Ing. José Abel Arbildo Paz

Jefe de Oficina de Sistemas y Tecnologías de Información