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 DEL NIVEL DE SEGURIDAD DE LA INFORMACIÓN DE LA OFICINA DE INFORMATICA Y TELECOMUNICACIONES DE LA MUNICIPALIDAD DISTRITAL DE SAN JUAN BAUTISTA - 2023

PARA OBTAR EL TITÚLO PROFESIONAL

INGENIERO INFORMÁTICO Y DE SISTEMAS

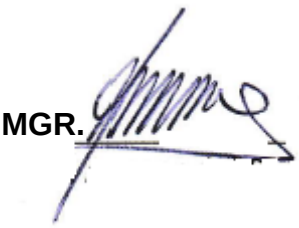
INGENIERO DE SISTEMAS DE INFORMACIÓN

AUTORES:

- **BACH. MARIA ENIHT DEL CARMEN DIAZ SANDOVAL**
- **BACH. CHARLES ALEJANDRO ROJAS PERLECHE**

ASESOR:

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



SAN JUAN BAUTISTA – MAYNAS – LORETO - PERÚ – 2023

DEDICATORIA

A mi madre Pilar, por tu apoyo que ha sido fundamental para lograr este sueño, por el amor y presencia en cada toma de decisiones que van encaminando mi vida, tus palabras que me ayudan siempre a seguir adelante y nunca rendirme. Gracias, madre mía mi amor y agradecimiento para ti por ser la mejor madre del mundo.

A mi Padre Telmo, esta tesis es un tributo por la eterna admiración y amor que siento por ti. Eres mi ejemplo de esfuerzo y trabajo. Gracias por ser el mejor padre del mundo.

A mi Abuelita Loyda, por todo su amor.

A mi querida hermana Dania, gracias por enseñarme que la vida es más feliz con una hermana como tú. ¡Este logro también te lo dedico a ti!

A mi amada hija Thamyra, por ser la luz de mi vida, por enseñarme con su existencia el camino que debo continuar, eres mi mayor motivación para no rendirme. ¡Lo estamos logrando! Y esta tesis te la dedico con todo mi amor.

BACH. MARIA ENIHT DEL CARMEN DIAZ SANDOVAL

DEDICATORIA

A mi madre Benny que ha sabido formarme con buenos sentimientos, hábitos y valores lo cual me ha ayudado a seguir adelante en los momentos difíciles.

A mi padre Charles que se dedica a trabajar para darnos un estudio a todos mis hermanos y a mi.

A mi abuela Martha desde el cielo me ilumina a seguir adelante

A mi abuelo Jorge desde el cielo ilumina mi camino.

BACH. CHARLES ALEJANDRO ROJAS PERLECHE

AGRADECIMIENTO

El principal agradecimiento a Dios, que nos ha guiado y nos ha dado fortaleza para seguir adelante.

A nuestras familias por la comprensión y estimulo constante, además su apoyo incondicional a lo largo de nuestros estudios y a todas las personas que de uno y otra forma nos apoyaron en la realización de este trabajo.

A nuestro Asesor por haber brindado su guía en la elaboración y ejecución de esta tesis.

A la Universidad Científica del Perú, por ser nuestra alma mater.

BACH. MARIA ENIHT DEL CARMEN DIAZ SANDOVAL

BACH. CHARLES ALEJANDRO ROJAS PERLECHE

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 DEL NIVEL DE SEGURIDAD DE LA INFORMACIÓN DE LA OFICINA DE INFORMATICA Y TELECOMUNICACIONES DE LA MUNICIPALIDAD DISTRITAL DE SAN JUAN BAUTISTA - 2023"

De los alumnos: **MARIA ENIHT DEL CARMEN DIAZ SANDOVAL Y CHARLES ALEJANDRO ROJAS PERLECHE,** de la Facultad de Ciencias e Ingeniería, pasó satisfactoriamente la revisión por el Software Antiplagio, con un porcentaje de **18% de similitud**.

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

San Juan, 11 de enero del 2024.

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

CJRA/ri-a
18-2024

Resultados_UCP_SistemasInformacion_2023_Tesis_Maria Diaz_AlejandroRojas_V1

INFORME DE ORIGINALIDAD

18%	18%	1%	8%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	repositorio.uisek.edu.ec Fuente de Internet	2%
2	www.ii.unam.mx Fuente de Internet	2%
3	dspace.ucacue.edu.ec Fuente de Internet	1%
4	www.xmlogindemo.com Fuente de Internet	1%
5	openigo.com Fuente de Internet	1%
6	Submitted to Universidad Internacional de la Rioja Trabajo del estudiante	1%
7	repositorio.unapiquitos.edu.pe Fuente de Internet	1%
8	cn.coursera.org Fuente de Internet	<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:	Maria Eniht Del Carmen Diaz Sandoval
Título del ejercicio:	Quick Submit
Título de la entrega:	Resultados_UCP_SistemasInformacion_2023_Tesis_Maria Dia...
Nombre del archivo:	Informe_Final_de_Tesis_-_Alejandro_Rojas_y_Maria_Diaz_2.pdf
Tamaño del archivo:	215.17K
Total páginas:	27
Total de palabras:	6,198
Total de caracteres:	34,471
Fecha de entrega:	11-ene.-2024 02:42p. m. (UTC-0500)
Identificador de la entre...	2269552882

RESUMEN

En este estudio, se adopta un enfoque de "Investigación Descriptiva" con un diseño no experimental - transaccional para examinar a fondo la seguridad de la información en la Municipalidad Distrital de San Juan Bautista. La metodología detalla la población y muestra, abarcando activos informáticos, componentes físicos y lógicos, la recolección de datos se lleva a cabo mediante check list, observación directa y revisión documental que abordo aspectos clave relacionados con la seguridad informática. La evaluación de vulnerabilidades y amenazas específicas identifica activos críticos y niveles de riesgo por componente, los resultados destacan riesgos potenciales por ataques, con niveles de riesgo específicos para diversas pruebas de seguridad. Se destaca la ausencia y capacitación en ciberseguridad del personal, aunque se identifican oportunidades de mejora en la comprensión de conceptos clave. La mayoría ha recibido capacitación en seguridad de la información en los últimos 12 meses, principalmente a través de cursos presenciales, y la mayoría califica la capacitación como efectiva, las conclusiones subrayan la importancia de abordar activos críticos, mejorar la implementación de controles y fortalecer la conciencia del personal. Se proponen recomendaciones específicas, como la implementación de medidas de seguridad, evaluaciones periódicas de riesgos y programas continuos de capacitación. Palabras clave: hacking ético, seguridad de la información, municipalidad.

Palabras claves: seguridad informática, riesgo, activos informáticos.

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° 705-2023-UCP-FCEI del 26 de octubre del 2023, la FACULTAD DE CIENCIAS E INGENIERÍA DE LA UNIVERSIDAD CIENTÍFICA DEL PERÚ - UCP designa como Jurado Evaluador de la sustentación de 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: Ing. Ronald Melchor Infantes, Mtro.

En la ciudad de Iquitos, siendo las 9:00 am del día miércoles 31 enero del 2024, supervisado por la Secretaria Académica 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 ***ANÁLISIS DEL NIVEL DE SEGURIDAD DE LA INFORMACIÓN DE LA OFICINA INFORMÁTICA Y TELECOMUNICACIONES DE LA MUNICIPALIDAD DISTRITAL DE SAN JUAN BAUTISTA-2023***

Presentado por los sustentantes: **DIAZ SANDOVAL MARIA ENIHT DEL CARMEN** y **ROJAS PERLECHE CHARLES ALEJANDRO**

Como requisito para optar el título profesional de:

- **INGENIERO INFORMÁTICO Y DE SISTEMAS**
- **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 UNANIMIDAD

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

Ing. Jimmy Max Ramírez Villacorta, Mtro
Presidente

Ing. Tonny Eduardo Bardales Lozano, Mgr.
Miembro

Ing. Christian Alfredo Arévalo Jesús, Mtro.
Miembro

APROBACIÓN

UNIVERSIDAD CIENTÍFICA DEL PERÚ

HOJA DE APROBACIÓN

PROGRAMA ACADÉMICO DE INGENIERÍA INFORMÁTICA Y DE SISTEMAS
PROGRAMA ACADÉMICO DE INGENIERÍA DE SISTEMAS DE INFORMACIÓN
TESISTAS: DIAZ SANDOVAL MARIA ENIHT DEL CARMEN
ROJAS PERLECHE CHARLES ALEJANDRO

Tesis sustentada en acto publico el día miércoles 31 de enero del 2024, a las 9:00 am , 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

Contenido

INDICE DE TABLAS

Pagina

RESUMEN

En este estudio, se adopta un enfoque de "Investigación Descriptiva" con un diseño no experimental - transeccional para examinar a fondo la seguridad de la información en la Municipalidad Distrital de San Juan Bautista. La metodología detalla la población y muestra, abarcando activos informáticos, componentes físicos y lógicos, la recolección de datos se lleva a cabo mediante chek list, observación directa y revisión documental que aborda aspectos clave relacionados con la seguridad informática, La evaluación de vulnerabilidades y amenazas específicas identifica activos críticos y niveles de riesgo por componente, los resultados destacan riesgos potenciales por ataques, con niveles de riesgo específicos para diversas pruebas de seguridad. Se destaca la conciencia y capacitación en ciberseguridad del personal, aunque se identifican oportunidades de mejora en la comprensión de conceptos clave. La mayoría ha recibido capacitación en seguridad de la información en los últimos 12 meses, principalmente a través de cursos presenciales, y la mayoría califica la capacitación como efectiva, las conclusiones subrayan la importancia de abordar activos críticos, mejorar la implementación de controles y fortalecer la conciencia del personal. Se proponen recomendaciones específicas, como la implementación de medidas de seguridad, evaluaciones periódicas de riesgos y programas continuos de capacitación. Palabras clave: hacking ético, seguridad de la información, municipalidad.

Palabras claves: seguridad informática, riesgo, activos informáticos

ABSTRACT

In this study, a "Descriptive Research" approach with a non-experimental - transactional design is adopted to thoroughly examine information security at the Municipalidad Distrital de San Juan Bautista. The methodology outlines the population and sample, encompassing computer assets, physical and logical components. Data collection is carried out through checklists, direct observation, and documentary review, addressing key aspects related to computer security. The assessment of specific vulnerabilities and threats identifies critical assets and risk levels per component, the results highlight potential risks from attacks, with specific risk levels for various security tests. Employee awareness and training in cybersecurity are emphasized, although opportunities for improvement in understanding key concepts are identified. The majority have received information security training in the last 12 months, primarily through in-person courses, and most rate the training as effective, the conclusions underscore the importance of addressing critical assets, improving control implementation, and strengthening employee awareness. Specific recommendations are proposed, such as the implementation of security measures, periodic risk assessments, and ongoing training programs. Keywords: ethical hacking, information security, municipality.

Key terms: computer security, risk, computer assets.

CAPÍTULO I: MARCO TEÓRICO

1.1 Antecedentes de Estudio

✓ Antecedentes Internacionales

- Hurtado, Martínez & Jenifer Tamara (2022), El objetivo principal de la investigación monográfica titulada "Política de Seguridad de la Información para la Universidad Indígena y Caribeña de Bluefields (BICU)" es diseñar políticas de seguridad de la información para salvaguardar los datos y el equipo informático gestionado por la universidad y sus diferentes departamentos. Para lograr este objetivo, se deben identificar las vulnerabilidades de los datos de la universidad. Esta identificación servirá como base para minimizar riesgos como la dispersión de datos, la pérdida de tiempo y otros relacionados con los recursos de TIC (Tecnologías de la Información y la Comunicación) que posee la institución. Además, se propuso una estructura organizativa para garantizar el cumplimiento de las políticas de seguridad de la información. Las políticas de seguridad descritas en este documento son una herramienta fundamental para salvaguardar los recursos de TIC de la universidad y buscan desarrollar el conocimiento tecnológico del capital humano que es esencial para el correcto funcionamiento y utilización de estos activos. Esta investigación fue descriptiva ya que se describieron las características y cualidades de las variables con un corte transversal, también se señaló a un tiempo definido, la población de estudio estuvo constituida por 9 trabajadores permanentes, 3 pasantes y 6 monitores, con un total de 18 participantes. La medición se realizó a través de instrumentos de entrevista y encuesta, que se aplicaron después de informar el propósito. Los resultados obtenidos mostraron que no existe en la instalación un documento que describa las políticas de seguridad necesarias para la protección de los recursos de TIC, por lo que se hizo una propuesta al respecto.

- Ochoa, Lissette (2022), El objetivo principal de la investigación monográfica titulada "Política de Seguridad de la Información para la Universidad Indígena y Caribeña de Bluefields (BICU)" es diseñar políticas de seguridad

de la información para salvaguardar los datos y el equipo informático gestionado por la universidad y sus diferentes departamentos. Para lograr este objetivo, se deben identificar las vulnerabilidades de los datos de la universidad. Esta identificación servirá como base para minimizar riesgos como la dispersión de datos, la pérdida de tiempo y otros relacionados con los recursos de TIC (Tecnologías de la Información y la Comunicación) que posee la institución. Además, se propuso una estructura organizativa para garantizar el cumplimiento de las políticas de seguridad de la información. Las políticas de seguridad descritas en este documento son una herramienta fundamental para salvaguardar los recursos de TIC de la universidad y buscan desarrollar el conocimiento tecnológico del capital humano que es esencial para el correcto funcionamiento y utilización de estos activos. Esta investigación fue descriptiva ya que se describieron las características y cualidades de las variables con un corte transversal, también se señaló a un tiempo definido, la población de estudio estuvo constituida por 9 trabajadores permanentes, 3 pasantes y 6 monitores, con un total de 18 participantes. La medición se realizó a través de instrumentos de entrevista y encuesta, que se aplicaron después de informar el propósito. Los resultados obtenidos mostraron que no existe en la instalación un documento que describa las políticas de seguridad necesarias para la protección de los recursos de TIC, por lo que se hizo una propuesta al respecto.

- Cedeño, Marco (2022), Este proyecto tiene como objetivo establecer un marco de referencia para la implementación de controles de seguridad informática en una empresa que se dedica a la fabricación, comercialización y exportación de muebles. Este marco de referencia comienza con el análisis de los antecedentes de seguridad informática de la organización, lo cual permite determinar que las pocas medidas de seguridad tomadas en la compañía no cubren todos los activos que deberían protegerse, y no están articuladas entre sí. Por lo tanto, es necesario implementar los controles dictados por algún estándar de la industria. En este caso, se eligió la norma CIS versión 8, ya que sugiere puntos de control específicos para pequeñas empresas que están en una

etapa temprana de implementación de controles de seguridad informática. El desarrollo del marco de referencia tiene como objetivo proporcionar a la organización pautas claras para implementar los controles de CIS versión 8, para que en el futuro pueda gestionar su ciberseguridad de manera formal.

✓ Antecedentes Nacionales:

- Moron, Peredo & Kristopher Renzo (2023), en su tesis cuyo propósito principal es diseñar un Sistema de Gestión de Seguridad de la Información que cumpla con estándares internacionales ajustados a las nuevas tecnologías de la información, para ayudar a mejorar la seguridad de la información en la empresa Rash Perú S.A.C. Para lograrlo, se realizó una investigación de campo que permitió desarrollar una propuesta de modelo viable para resolver los problemas de seguridad de la información en la empresa, tomando como caso de estudio a la mencionada compañía. La metodología utilizada se basó en el ciclo de Deming, tomando como referencia la Norma ISO 27002 y utilizando 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 midieron con un valor promedio del Pre test de 69,90% y un valor promedio del Post test de 14,00%. Además, se encontró que el valor mínimo del Pre test fue del 50%, el valor máximo fue del 88%, y el valor mínimo del post test fue del 0%, mientras que el máximo fue 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, lo que indica que el indicador se ajusta a una distribución normal o paramétrica (P > 0,05). La tesis se compone de seis capítulos, en los que se desarrolla cada tema relacionado con la propuesta de diseño, sus resultados y su aplicación.

- Asurza, Josue (2022), El propósito del proyecto consiste en demostrar cómo el diseño de una arquitectura de seguridad informática puede aumentar la protección de la información de la empresa BAFING S.A.C. Esta investigación es de naturaleza experimental, ya que manipula la variable independiente

"Arquitectura de Seguridad Informática" para impactar en la variable dependiente "Seguridad de Información", reforzando sus efectos. BAFING S.A.C. se dedica al desarrollo de proyectos informáticos de seguridad de información y está conformada por consultores expertos en la gestión de riesgos e implementación de sistemas de administración de software informático. La arquitectura propuesta ofrece una mayor cobertura para proteger la información como un activo valioso para las empresas que trabajan con equipos informáticos. Para lograr este objetivo, se evaluaron diferentes propuestas de software de seguridad utilizando un perfil de características previamente establecido y se juzgó cada una de ellas en función del cumplimiento de la integridad, confidencialidad y disponibilidad, que son los pilares fundamentales de la protección de información. Esto permitió al equipo administrativo planificar la adquisición o renovación del software en función de la información recopilada. Las herramientas de evaluación utilizadas en el proyecto fueron recopiladas a partir de entrevistas con especialistas en la protección de información y activos informáticos y están disponibles para futuras evaluaciones de otros productos de seguridad informática. Los resultados obtenidos demostraron mejoras en las dimensiones de seguridad de la información analizadas en comparación con la situación actual de la empresa auditada, BAFING S.A.C.

- ✓ Antecedentes Locales:
  No se encontraron antecedentes locales

1.2 Bases Teóricas

- Seguridad Informática:

  Morales (2022), 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. La seguridad informática se ha vuelto cada vez más importante a medida que los sistemas informáticos se han vuelto más complejos y las amenazas informáticas se han vuelto más sofisticadas.

En los últimos años, la seguridad informática ha ganado relevancia como un tema de interés público. Tanto expertos en la materia como usuarios comunes utilizan términos como "clave de usuario", "contraseña", "fraude informático" y "hacker", entre otros. En la actualidad, es indispensable tener conocimientos sólidos en este tema para evitar poner en peligro la información, el equipo y la integridad del usuario.

Según Gómez (2006), la seguridad informática se refiere a cualquier medida 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. Por su parte, Kissel (2012) la define como 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.

Existen numerosas medidas preventivas para proteger estos elementos, como respaldos de información, controles de acceso, programas antivirus y antispyware, firewalls, actualizaciones continuas del sistema operativo, mantenimiento del equipo de cómputo y protección física en las áreas de operaciones de red.

Para un usuario, la protección de su información es generalmente más importante que la protección del software o el equipo. Para garantizar la seguridad de los datos, es esencial cumplir con tres componentes fundamentales: integridad, disponibilidad y confidencialidad.

- Tipos de Seguridad Informática

Hay varios tipos de seguridad informática utilizados para proteger los sistemas y redes de posibles amenazas. A continuación, se describen algunos de los tipos más comunes:

La seguridad física se refiere a la protección de los dispositivos físicos y el acceso a ellos, lo que incluye restringir el acceso a las instalaciones, usar cerraduras, controlar el acceso a las áreas críticas y proteger los equipos de cómputo.

La seguridad lógica es la protección del software y los datos que se encuentran en un sistema o red. Esto incluye el uso de contraseñas, la autenticación de usuarios, la gestión de permisos, la implementación de firewalls y el cifrado de datos.

La seguridad de red se enfoca en proteger las redes informáticas y los datos que se transmiten a través de ellas. Esto incluye el uso de firewalls, la autenticación de usuarios, la implementación de VPNs, el monitoreo del tráfico de red y la prevención de ataques de denegación de servicio (DoS).

La seguridad de la información es la protección de la información que se encuentra en un sistema o red. Esto incluye la implementación de políticas de seguridad, la gestión de acceso a la información y la prevención de la pérdida de datos.
La seguridad de aplicaciones es la protección de las aplicaciones de software utilizadas en un sistema o red. Esto incluye el uso de técnicas de codificación segura, la gestión de permisos y la prevención de vulnerabilidades de seguridad.

Hay muchos más tipos de seguridad informática, y este campo está en constante evolución, con nuevas amenazas y técnicas emergentes. Por lo tanto, es importante mantenerse actualizado con las últimas tendencias y mejores prácticas en seguridad informática para proteger adecuadamente los sistemas y redes.

- Objetivos de la Seguridad Informática

  Se pueden identificar diversos objetivos de seguridad informática que pueden variar según el contexto y las necesidades específicas de cada organización. En términos generales, estos objetivos incluyen garantizar la confidencialidad de la información para que solo sea accesible por personas autorizadas y se mantenga en secreto, asegurar la integridad de la información para que no sea modificada de manera no autorizada y se mantenga exactamente como se creó o modificó por última vez, y garantizar la disponibilidad de la información para que esté disponible para los usuarios autorizados cuando la necesiten. Otros objetivos importantes incluyen la autenticación para verificar la identidad de los usuarios que acceden al sistema o a la información, la autorización para garantizar que los usuarios solo tengan acceso a la información y los recursos que estén autorizados a utilizar, y la responsabilidad para asegurar que se pueda rastrear y responsabilizar a los usuarios por sus acciones en el sistema. También se busca asegurar el no repudio para garantizar que una entidad no pueda negar haber realizado una acción en el sistema, y se debe proteger la seguridad física del hardware y los dispositivos que dependen de la seguridad informática. En resumen, los objetivos de la seguridad informática buscan proteger la información, los sistemas y las redes de posibles amenazas, y garantizar la confidencialidad, integridad, disponibilidad y autenticidad de la información, así como la responsabilidad y la no repudio de las acciones de los usuarios.

1.3 Definición de Términos Básicos:

- Seguridad: La seguridad se refiere a la condición de estar libre de peligros, daños o riesgos, que se logra mediante la implementación de medidas preventivas y de protección frente a posibles amenazas.

- Informática: Es una disciplina que se encarga del procesamiento, almacenamiento y transmisión de información utilizando tecnologías y sistemas computacionales.

- Amenaza: se refiere a cualquier posible evento o acción que podría causar daño, pérdida o interrupción de los recursos o activos de una organización o individuo.

- Riesgo: Es la posibilidad de que ocurra un evento no deseado o un resultado no esperado, y las consecuencias negativas que podrían resultar de dicho evento o resultado.

- Planes: Son documentos o esquemas que establecen objetivos, estrategias, acciones y recursos necesarios para lograr un determinado fin o resolver una situación específica.

CAPÍTULO II: PLANTEAMIENTO DEL PROBLEMA

2.1 Descripción del Problema

El análisis del nivel de seguridad de la información en la Oficina de Informática y Telecomunicaciones de la Municipalidad Distrital de San Juan Bautista en 2023 revela una serie de problemáticas que requieren atención urgente. Estas problemáticas pueden tener graves consecuencias para la integridad, confidencialidad y disponibilidad de los datos y sistemas de la municipalidad. Aquí se presenta una realidad problemática basada en información general, pero es importante realizar una evaluación detallada y específica para obtener una comprensión completa de la situación, Falta de Políticas y Procedimientos de Seguridad de la Información, la Municipalidad carece de políticas y procedimientos adecuados para la gestión de la seguridad de la información. Esto incluye la ausencia de directrices claras sobre cómo proteger los datos sensibles, gestionar las contraseñas, manejar incidentes de seguridad y establecer responsabilidades claras para la seguridad de la información, Vulnerabilidades en la Infraestructura Tecnológica, la infraestructura tecnológica de la Oficina de Informática y Telecomunicaciones presenta vulnerabilidades conocidas que podrían ser explotadas por ciberdelincuentes. Esto incluye servidores obsoletos, falta de actualizaciones de software y falta de un sistema de detección y prevención de intrusiones, falta de Conciencia y Formación en Seguridad de la Información, el personal de la municipalidad no está adecuadamente capacitado en seguridad de la información y carece de conciencia sobre las mejores prácticas de seguridad cibernética. Esto aumenta el riesgo de que los empleados cometan errores que puedan comprometer la seguridad de los datos, gestión Inadecuada de Accesos y Contraseñas, la gestión de accesos y contraseñas es deficiente, lo que significa que no se están implementando controles adecuados para garantizar que solo las personas autorizadas tengan acceso a la información. Las contraseñas débiles y la falta de políticas de cambio de contraseñas regulares son preocupaciones importantes, falta de Respuesta ante Incidentes de Seguridad, la Municipalidad no tiene un plan de respuesta ante incidentes de seguridad de la información establecido. Esto significa que en caso de una

violación de seguridad, no hay un proceso claro para detectar, informar y mitigar el incidente de manera eficiente, falta de Auditorías y Evaluaciones de Seguridad, no se realizan auditorías regulares ni evaluaciones de seguridad de la información para identificar debilidades en el sistema y evaluar la eficacia de las medidas de seguridad existentes, estas problemáticas representan un riesgo significativo para la Municipalidad Distrital de San Juan Bautista en términos de pérdida de datos, interrupciones en los servicios y posibles sanciones legales. Es esencial que la municipalidad tome medidas inmediatas para abordar estas cuestiones, lo que incluye la adopción de políticas de seguridad de la información, la inversión en tecnología segura, la capacitación del personal y el establecimiento de un plan de respuesta ante incidentes. La seguridad de la información es fundamental para proteger los activos críticos y la confianza de los ciudadanos en la administración pública.

2.2 Formulación del Problema

2.2.1 Problema General

- ✓ ¿Cuál es el estado situacional de la seguridad de la información de la Oficina de informática y telecomunicaciones de la Municipalidad Distrital de San Juan Bautista?

1.3.2 Problemas Específicos

1. ¿Cuál es el nivel de implementación de políticas y procedimientos de seguridad de la información?
2. ¿Cuál es el nivel de implementación de seguridad de las redes de datos?
3. ¿Cuál es el nivel de implementación de gestión de incidencias?
4. ¿Cuál es el nivel de riesgos que presenta la seguridad de la información?

2.3 Objetivos

2.3.1 Objetivo General

- ✓ Evaluar estado situacional de la gestión de seguridad de la información en la Informática de la Oficina de Informática y Telecomunicaciones de la Municipalidad Distrital de San Juan Bautista en el Periodo 2023.

1.3.2 Objetivos Específicos

1. Evaluar el nivel de implementación de políticas y procedimientos de seguridad de la información de la Oficina de Informática y Telecomunicaciones de la Municipalidad Distrital de San Juan Bautista en el periodo 2023.
2. Evaluar el nivel de implementación de seguridad de las redes de datos de la Oficina de Informática y Telecomunicaciones de la Municipalidad Distrital de San Juan Bautista en el periodo 2023.
3. Evaluar el nivel de implementación de gestión de incidencias de la Oficina de Informática y Telecomunicaciones de la Municipalidad Distrital de San Juan Bautista en el periodo 2023.
4. Evaluar el nivel de riesgos que presenta la seguridad de la información de la Oficina de Informática y Telecomunicaciones de la Municipalidad Distrital de San Juan Bautista en el periodo 2023.

2.4 Hipótesis

- Ho: El nivel de aseguramiento de la información en la oficina de informática y telecomunicaciones de la Municipalidad Distrital de San Juan Bautista es bajo.

- H1: El nivel de aseguramiento de la información en la oficina de informática y telecomunicaciones de la Municipalidad Distrital de San Juan Bautista es alto.

2.5 Variables

2.5.1 Identificación de Variables

- Variable: Seguridad de la información

2.5.2 Definición Conceptual de las Variables

- Definición Conceptual de las Variables:

Variable	Definición Conceptual	Definición Operacional
Seguridad de la información	Se trata de salvaguardar la información y los sistemas contra amenazas, garantizar la integridad y disponibilidad de los datos, y cumplir con las normativas de seguridad para proteger los intereses de la municipalidad y sus ciudadanos.	Evaluar los niveles de cumplimiento en los procesos y actividades que intervienen en el manejo de la información dentro de la organización

2.5.3 Operacionalización de las Variables

Tabla 01

Operacionalización de Variables

Variables	Dimensiones	Indicadores	Instrumento de recolección de Datos
Seguridad de la información	Políticas y Procedimientos de seguridad	% Implementación	Documental, Ficha de Observación, Encuesta
	Seguridad en la red de datos	% Implementación	
	Gestión de incidencias	Tiempo de Respuesta	
	Riesgos	% de Impacto	

Fuente: Elaboración Propia

CAPÍTULO III: METODOLOGÍA

3.1 Tipo y Diseño de Investigación

- Tipo o enfoque de la Investigación

  Investigación Descriptiva". La investigación descriptiva tiene como objetivo principal describir de manera detallada una situación, fenómeno o problemática particular. En este caso, el objetivo es analizar y describir el estado actual de la seguridad de la información implementada por la Oficina de informática y Telecomunicaciones de la Municipalidad Distrital de San Juan Bautista.

  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 de la siguiente manera:

Para evaluar el nivel de implementación de políticas y procedimientos de seguridad de la información se tomó como población todas las políticas de seguridad informática que están implementadas en el área de sistemas de la municipalidad distrital de San Juan Bautista.

Para evaluar el nivel de implementación de seguridad de las redes de datos, se tomó como población a los equipos activos y pasivos de la red de datos de la municipalidad distrital de San Juan Bautista.

Para evaluar el nivel de implementación de gestión de incidencias se tomó como población a los reportes de incidencias que cuenta el área de sistemas de la municipalidad distrital de San Juan Bautista.

Para evaluar el nivel de riesgos informáticos se tomó como población a todas las posibles amenazas que existen en la municipalidad distrital de San Juan Bautista.

Muestra

Para evaluar el nivel de implementación de políticas y procedimientos de seguridad de la información se tomó como muestra a 18 controles que son mínimos que se deben haber implementado en la municipalidad distrital de san Juan Bautista en el periodo 2023.

Para evaluar el nivel de implementación de seguridad de las redes se tomó como muestra 8 aspectos de seguridad que son mínimos con que debe contar la municipalidad distrital de San Juan Bautista en el periodo 2023.

Para evaluar el nivel de implementación de gestión de incidencias se tomó como muestra 6 tipos de incidencias más frecuentes que se suscitaron en la municipalidad distrital de San Juan Bautista en el periodo 2023.

Para evaluar el nivel de riesgos que presenta la seguridad de la información se tomó como muestra a 6 activos o procesos informáticos mas importantes que usa el área de sistemas de la municipalidad distrital de San Juan Bautista en el periodo 2023.

3.3 Técnicas, instrumentos y procedimientos de recolección de datos

- Técnica de Recolección de Datos:

  Para evaluar el nivel de implementación de políticas y procedimientos de seguridad de la información se utilizó el chek list a través de la revisión documental.

Para evaluar el nivel de implementación de seguridad de las redes de datos, se utilizó el 28heck list a través de la observación directa.

Para evaluar el nivel de implementación de gestión de incidencias se utilizó el 28heck list a través de la revisión documental.

Para evaluar el nivel de riesgos que presenta la seguridad de la información se utilizó una matriz de riesgo para valorar el nivel de riesgo que se encuentran los activos informáticos

- Instrumento de Recolección de Datos:

Check List: se empleo para la verificación o identificación de los factores o riesgos de la seguridad informática

- Procedimiento de Recolección de Datos:

Este proceso se llevo a cabo en un solo momento, realizando revisión documental y haciendo observación de la red de datos de la municipalidad distrital de San Juan Bautista.

3.4 Procesamiento y análisis de datos.

La Información se procesó en el software de estadística SPSS Versión 27, cuyos resultados se clasificaron en tablas y gráficos estadísticos de manera descriptiva.

CAPÍTULO IV: RESULTADOS

- ✓ Objetivo 01: Evaluar el nivel de implementación de políticas y procedimientos de seguridad de la información de la Oficina de Informática y Telecomunicaciones de la Municipalidad Distrital de San Juan Bautista en el periodo 2023.

Tabla 02

Nivel de implementación de políticas y procedimientos de seguridad de la información

Categoría	Aspectos a Evaluar	Nivel de Implementación (Escala del 1 al 5)
Gestión de Políticas	Existencia de políticas	3
	Actualización regular	2
Seguridad Física	Acceso físico a instalaciones	2
	Protección de activos físicos	2
Gestión de Accesos	Control de acceso lógico	4
	Gestión de privilegios	4
Protección contra Malware	Antivirus y antimalware	5
	Actualización regular	5
Cifrado de Datos	Datos en reposo	1
	Datos en tránsito	1
Gestión de Incidentes	Plan de respuesta a incidentes	1
	Registro y análisis de incidentes	1
Formación y Concientización	Programas de formación	2
	Concientización del personal	2
Respaldos de Datos	Programa de respaldos	1
	Verificación de respaldos	1
Auditorías y Evaluaciones	Auditorías internas	1
	Auditorías externas	1

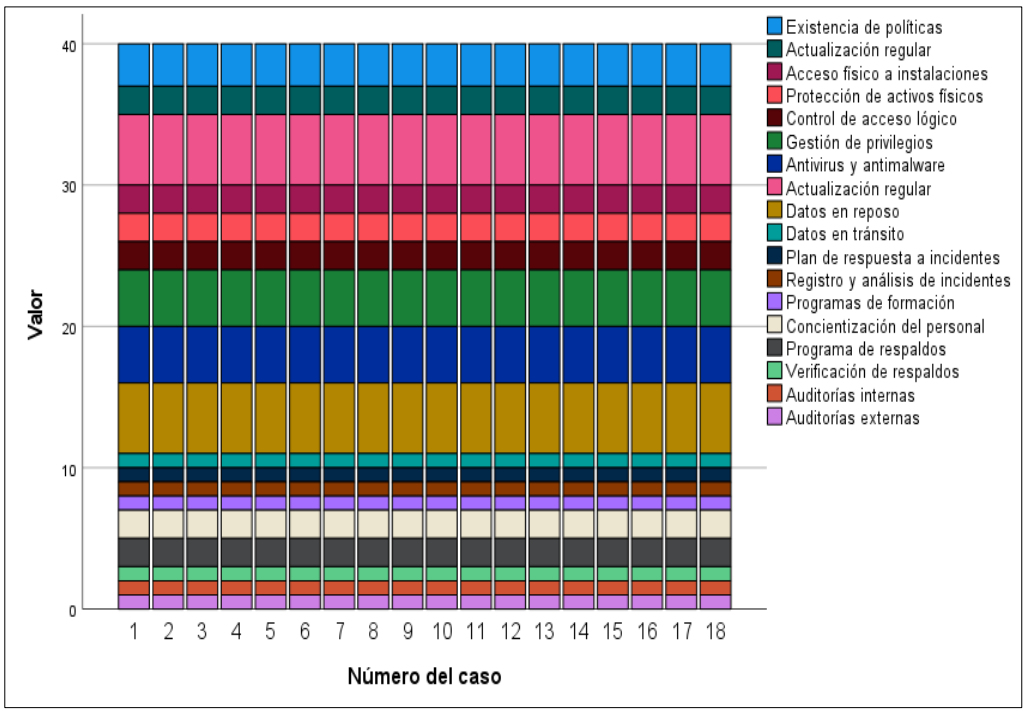
Fuente: Elaboración propia

Leyenda

Escala	Descripción
1	Nivel bajo
2	Nivel básico
3	Nivel moderado
4	Nivel avanzado
5	Nivel alto

Figura 01

Nivel de implementación de políticas y procedimientos de seguridad de la información



Interpretación: de la tabla 2 y figura 2 se puede evidenciar que luego de la evaluación la existencia de políticas se encuentran en el nivel moderado, la actualización regular se encuentra en el nivel básico, el acceso físico a instalaciones se encuentra en el nivel básico, la protección de activos físicos se encuentran en el nivel básico, el control de acceso lógico se encuentra en el nivel avanzado, la gestión de privilegios se encuentra en el nivel avanzado, la implementación de política de antivirus y antimalware se encuentra en el nivel alto, igual que la su actualización regular, en la políticas de seguridad sobre los datos en reposo y datos en tránsito se encuentran en el nivel bajo,

en lo que respecta a las políticas de los planes de respuesta a incidentes y el registro y análisis de incidentes, se encuentran en el nivel bajo, los programas de formación y la concientización del personal están en el nivel básico, los programa de respaldos, verificación de respaldos, auditorías internas y auditorías externas se encuentran en el nivel bajo.

- ✓ Objetivo 02: Evaluar el nivel de implementación de seguridad de las redes de datos de la Oficina de Informática y Telecomunicaciones de la Municipalidad Distrital de San Juan Bautista en el periodo 2023.

Tabla 03

Nivel de implementación de la seguridad de las redes de datos

Aspecto de Seguridad	Nivel de Implementación	Observaciones en la red cableada	Observaciones en la red inalámbrica	Acciones Recomendadas
Firewalls	Alto	Configurado y actualizado	Configurado y actualizado	Monitoreo regular e implementar nuevas reglas
Antivirus/Antimalware	Alto	Actualizado y funcionando en tiempo real	Actualizado y funcionando en tiempo real	Renovar las licencias en forma oportuna
Actualizaciones y Parches	Medio	No implementado	No implementado	Implementar servidor de memoria cache
Control de Acceso	Alto	Implementado, pero no totalmente optimizado	Implementado, pero no totalmente optimizado	Revisar y ajustar las políticas, también monitorear
Encriptación de Datos	Bajo	Implementado, pero no totalmente optimizado	Implementado, pero no totalmente optimizado	Realizar Monitoreo, actualizaciones y auditorias
Segmentación de Redes	Medio	Parcialmente implementado	Parcialmente implementado	Implementar V´Lans
Monitoreo y Registro de Actividad	Bajo	Parcialmente implementado	Parcialmente implementado	Realizar el monitoreo continuo para la detección de vulnerabilidades y amenazas
Autenticación	Medio	Implementada pero no en todos los sistemas	Implementada pero no en método mas seguro	Implementar en la red inalámbrica WPA2 (Wi-Fi Protected Access 2)

Fuente: Elaboración propia

Interpretación: de la tabla 03 se puede evidenciar que el nivel de implementación tanto en la red cableada como la red inalámbrica, predomina el nivel medio, además de ello se puede observar que existen aspectos de seguridad que están implementados a medias.

- ✓ Objetivo 03: Evaluar el nivel de implementación de gestión de incidencias de la Oficina de Informática y Telecomunicaciones de la Municipalidad Distrital de San Juan Bautista en el periodo 2023.

Tabla 04

Nivel de implementación de gestión de incidencias

Mes Año 2023	Número de incidencias reportadas	Número de incidencias resueltas	Tiempo promedio de solución	Nivel de implementación de gestión de incidencias
Enero	20	18	3	Alto
Febrero	15	14	2	Alto
Marzo	25	22	4	Medio
Abril	18	16	1	Alto
Mayo	22	20	2	Alto
Junio	17	15	3	Alto
Julio	21	19	2	Alto
Agosto	19	19	4	Medio
Setiembre	24	17	1	Alto
Octubre	16	15	1	Alto
Noviembre	23	19	2	Medio
Diciembre	18	17	1	Alto
Total	238	211	2	Medio

Fuente: Elaboración propia

Interpretación: de la tabla 4 se puede evidenciar que durante el periodo 2023 se han reportado 238 incidencias, de las cuales solo se resolvieron 211, en un tiempo promedio de 2 días y el nivel de gestión de incidencias implementada predomina el nivel alto.

- ✓ Objetivo 04: Evaluar el nivel de riesgos que presenta la seguridad de la información de la Oficina de Informática y Telecomunicaciones de la Municipalidad Distrital de San Juan Bautista en el periodo 2023.

Tabla 05

Matriz que evalúa el Nivel de riesgos

Amenazas	Probabilidad	RC	RI	RD
Daño por agua	3	Bajo	Bajo	Alto
Avería de origen físico o lógico	2	Bajo	Bajo	Medio
Corte del suministro eléctrico	4	Bajo	Bajo	Alto
Errores del administrador	2	Medio	Medio	Medio
Errores de mantenimiento / actualización de equipos (hardware)	2	Bajo	Bajo	Medio
Caída del sistema por agotamiento de recursos	2	Bajo	Bajo	Medio
Suplantación de la identidad del usuario	3	Alto	Alto	Bajo
Abuso de privilegios de acceso	2	Medio	Medio	Medio
Amenazas	**Probabilidad**	**RC**	**RI**	**RD**
Fallo de servicios de comunicaciones	2	Bajo	Bajo	Medio
Errores del administrador	2	Bajo	Bajo	Medio
Fugas de información	2	Medio	Bajo	Bajo
Caída del sistema por agotamiento de recursos	2	Bajo	Bajo	Medio
Suplantación de la identidad del usuario	3	Medio	Medio	Bajo
Abuso de privilegios de acceso	2	Medio	Medio	Medio
Divulgación de información	2	Bajo	Bajo	Bajo
Amenazas	**Probabilidad**	**RC**	**RI**	**RD**
Fallo de servicios de comunicaciones	2	Bajo	Bajo	Medio
Errores del administrador	2	Bajo	Bajo	Medio
Alteración accidental de la información	2	Bajo	Medio	Bajo
Fugas de información	2	Bajo	Bajo	Bajo
Caída del sistema por agotamiento de recursos	2	Bajo	Bajo	Medio
Suplantación de la identidad del usuario	3	Bajo	Bajo	Bajo
Abuso de privilegios de acceso	2	Medio	Medio	Medio

Divulgación de información	2	Bajo	Bajo	Bajo
Amenazas	**Probabilidad**	**RC**	**RI**	**RD**
Daño por agua	3	Bajo	Bajo	Alto
Avería de origen físico o lógico	2	Bajo	Bajo	Medio
Corte de suministro eléctrico	4	Bajo	Bajo	Alto
Errores de los usuarios	2	Medio	Medio	Medio
Errores del administrador	2	Medio	Medio	Medio
Errores de configuración	2	Bajo	Medio	Bajo
Escapes de información	2	Medio	Bajo	Bajo
Alteración accidental de la información	2	Bajo	Bajo	Bajo
Fugas de información	2	Medio	Bajo	Bajo
Errores de mantenimiento/actualización de equipo (hardware)	2	Bajo	Bajo	Medio
Errores de mantenimiento/actualización de equipo (software)	2	Bajo	Medio	Medio
Caída del sistema por agotamiento de recursos	2	Bajo	Bajo	Medio
Suplantación de la identidad del usuario	3	Alto	Alto	Bajo
Abuso de privilegios de acceso	2	Medio	Medio	Medio
Divulgación de la información	2	Medio	Bajo	Bajo
Manipulación de equipos	2	Medio	Bajo	Medio
Amenazas	**Probabilidad**	**RC**	**RI**	**RD**
Daños por agua	3	Bajo	Bajo	Alto
Avería de origen físico o lógico	2	Bajo	Bajo	Medio
Corte del suministro eléctrico	4	Bajo	Bajo	Alto
Errores del administrador	2	Medio	Medio	Medio
Errores de configuración	2	Bajo	Medio	Bajo
Escapes de información	2	Medio	Bajo	Bajo
Fugas de información	2	Bajo	Bajo	Bajo
Errores de mantenimiento/actualización de equipo (hardware)	2	Bajo	Bajo	Medio
Errores de mantenimiento/actualización de equipo (software)	2	Bajo	Bajo	Medio
Caída del sistema por agotamiento de recursos	2	Bajo	Bajo	Medio
Abuso de privilegios de acceso	2	Bajo	Medio	Medio

Manipulación de los equipos	2	Medio	Bajo	Medio
Amenazas Probabilidad		**RC**	**RI**	**RD**
Daños por agua	3	Bajo	Bajo	Bajo
Alteración accidental de la información	2	Bajo	Bajo	Bajo
Fugas de información	2	Medio	Bajo	Bajo
Divulgación de información	2	Medio	Bajo	Bajo
Amenazas	**Probabilidad**	**RC**	**RI**	**RD**
Daños por agua	3	Bajo	Bajo	Medio
Alteración accidental de la información	2	Bajo	Medio	Bajo
Fugas de información	2	Medio	Bajo	Bajo
Divulgación de información	2	Medio	Bajo	Bajo

Fuente: Elaboración propia

LEYENDAS Y SIGNIFICADOS

PROBABILIDAD

Criterio de ocurrencia	Valor
Una vez cada año	1
Una vez cada 6 meses	2
Una vez cada 3 meses	3
Una vez cada mes	4
Más de una vez al mes	5

NIVEL DEL RIESGO

Nivel del Riesgo	Descripción
Alto	Probabilidad muy frecuente e impacto critico
Medio	Probabilidad común e impacto moderado
Bajo	Probabilidad inusual e impacto mínimo

Interpretación: La evaluación de vulnerabilidades y amenazas particulares proporciona una visión detallada sobre la criticidad de los activos informáticos en la Municipalidad Distrital de San Juan Bautista. Se han identificado activos críticos, incluyendo información de contribuyentes y proveedores, con un nivel de criticidad elevado. Además, se ha llevado a cabo un análisis de riesgos por componentes, resaltando amenazas como daño por agua, fallas físicas o lógicas, interrupciones en el suministro eléctrico y errores administrativos, entre otros.

CAPÍTULO V: DISCUSIÓN, CONCLUSIONES Y RECOMENDACIONES

5.1 Discusiones

- Los antecedentes muestran una tendencia común de falta de políticas de seguridad de la información. En contraste, la Oficina de Informática y Telecomunicaciones ya tiene políticas establecidas, aunque con áreas de mejora identificadas, como la actualización regular y el acceso físico, por lo tanto, las investigaciones anteriores enfatizan la importancia de tener políticas, y la implementación actual destaca la necesidad de mantener y mejorar estas políticas con actualizaciones regulares y fortalecimiento de la seguridad física.

- La evaluación de la seguridad de las redes de datos en la Oficina muestra un nivel medio, con fortalezas en firewalls y antivirus, pero debilidades en encriptación y monitoreo de actividades. Esta situación se asemeja a los antecedentes, donde también se identifican áreas de implementación a medias, por lo tanto la presencia de fortalezas en firewalls y antivirus es alentadora, pero se debe priorizar la mejora de aspectos críticos como la encriptación y el monitoreo para lograr una seguridad más completa.

- La oficina muestra una alta capacidad en la gestión de incidencias, resolviendo la mayoría en un tiempo promedio de 2 días. Esta capacidad es superior a la media identificada en antecedentes similares, por lo tanto, los antecedentes destacan la importancia de una gestión eficaz de incidentes. La Oficina puede compartir prácticas exitosas con otras instituciones y seguir mejorando, incluso reduciendo aún más el tiempo de resolución.

- La matriz de riesgos en la Oficina identifica amenazas críticas como daño por agua, fallas físicas o lógicas, y errores administrativos. Este enfoque de evaluación de riesgos es similar al encontrado en antecedentes, por lo tanto la identificación de activos críticos y amenazas proporciona una base sólida

para la implementación de medidas preventivas. Los antecedentes subrayan la necesidad de acciones proactivas para reducir riesgos.

1.2 Conclusiones

1. La evaluación global indica que la oficina ha establecido una base robusta en la implementación de políticas y procedimientos de seguridad, destacándose en la gestión de accesos y privilegios.
2. No obstante, se identifican áreas críticas, como la encriptación de datos y el monitoreo de actividades, que demandan mejoras sustanciales.
3. La gestión de incidencias sobresale por su eficacia; no obstante, se sugiere un monitoreo continuo y la exploración de vías para perfeccionar aún más la resolución de incidencias.
4. La identificación y evaluación de riesgos proporcionan una orientación clara sobre las áreas que requieren atención prioritaria, permitiendo la implementación de medidas preventivas y correctivas específicas.

1.3 Recomendaciones

1. Reforzar la seguridad física y garantizar la actualización periódica de políticas constituye una estrategia crucial para atender las áreas de mejora identificadas.
2. Dar prioridad a la aplicación de medidas destinadas a la encriptación de datos y al monitoreo constante de actividades en las redes, emergiendo como acciones fundamentales.
3. Compartir experiencias exitosas en la gestión de incidencias con otras entidades y explorar vías para mejorar la eficacia se erige como una iniciativa recomendada.
4. Implementar medidas preventivas específicas dirigidas a reducir riesgos críticos, tales como daños por agua y fallos físicos o lógicos, constituye una necesidad imperante.

5.4 Referencias Bibliográficas:

- ✓ MORON PEREDO, Kristopher Renzo. Diseño e implementación de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27002 para mejorar el nivel de seguridad informática en la empresa Rash Perú SAC. 2023.
- ✓ HURTADO MARTÍNEZ, Jenifer Tamara; OCAMPO NÚÑEZ, Cesar Augusto. Política de seguridad informática para la Bluefields Indian & Caribbean University (BICU), sede central, 2021. 2022.
- ✓ OCHOA MORA, Lissette Verónica; VILLAGRÁN COLOMA, Diego Armando. Metodología de gestión de riesgos enfocado a la seguridad informática, aplicada al centro de datos de la carrera de Ingeniería de Software, utilizando la norma ISO 27005. 2022. Tesis de Licenciatura. Universidad de Guayaquil. Facultad de Ciencias Matemáticas y Físicas. Carrera de Ingeniería en Sistemas Computacionales.
- ✓ CEDEÑO GÓMEZ, Marco Vinicio. Marco de referencia para la implementación de controles de seguridad informática en una empresa de fabricación, comercialización y exportación de muebles. 2022.
- ✓ ASURZA CACERES, Josue David. Diseño de una arquitectura de seguridad informática para incrementar la seguridad de información en la empresa Bafing SAC en 2021. 2022.