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

TESIS

ANÁLISIS DEL NIVEL DE SEGURIDAD INFORMÁTICA DE LA E.P.S. SEDALORETO S.A.- 2023

PARA OBTAR EL TITÚLO PROFESIONAL

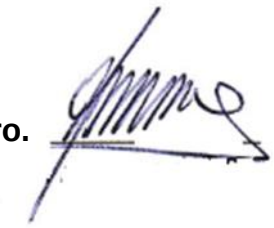
INGENIERO DE SISTEMAS DE INFORMACIÓN

AUTORES:

- **BACH. KAROLYN HILDA PATRICIA PÉREZ GONZÁLES**
- **BACH. MELISSA JANE BURGOS FLORES**

ASESOR:

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



SAN JUAN BAUTISTA – MAYNAS – LORETO - PERÚ – 2023

DEDICATORIA

A Dios por ser mi guía para ser un profesional de bien y a mis padres y sobre todo a mi tía luisa burgos por su apoyo incondicional

Bach. BURGOS FLORES MELISSA JANE

DEDICATORIA

A mi hija por ser la fuerza y soporte para salir adelante y lograr mi meta profesional.

Bach. KAROLYN HILDA PATRICIA PEREZ GONZALES

AGRADECIMIENTO

Expresamos nuestro agradecimiento a la propietaria de la empresa por habernos brindado las facilidades e información para el desarrollo de nuestra tesis

A los profesores con sus enseñanzas nos brindaron sabiduría y dirección en nuestra carrera.

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. Burgos Flores Melissa Jane

Bach. Karolyn Hilda Patricia Pérez Gonzales

CONSTANCIA DE ORIGINALIDAD DEL TRABAJO DE INVESTIGACIÓN

UNIVERSIDAD CIENTÍFICA DEL PERÚ

"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 INFORMÁTICA DE LA E.P.S. SEDALORETO S.A.- 2023"

De las alumnas: **KAROLYN HILDA PATRICIA PÉREZ GONZÁLES y MELISSA JANE BURGOS FLORES,** de la Facultad de Ciencias e Ingeniería pasó satisfactoriamente la revisión por el Software Antiplagio, con un porcentaje de **17% de similitud**.
Se expide la presente, a solicitud de la parte interesada para los fines que estime conveniente.

San Juan, 30 de enero del 2024.

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

CJRA/ri-a
35-2024

Resultados_UCP_SistemasInformacion_2023_Tesis_Karolyn...

INFORME DE ORIGINALIDAD

17%	14%	1%	11%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	alicia.concytec.gob.pe Fuente de Internet	2%
2	www.rte.espol.edu.ec Fuente de Internet	2%
3	Submitted to Corporación Universitaria Minuto de Dios, UNIMINUTO Trabajo del estudiante	1%
4	recursostic.educacion.es Fuente de Internet	1%
5	Submitted to Universidad Continental Trabajo del estudiante	1%
6	Submitted to Instituto Superior de Artes, Ciencias y Comunicación IACC Trabajo del estudiante	1%
7	Submitted to Universidad Cesar Vallejo Trabajo del estudiante	1%
8	bdigital.uncu.edu.ar 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:	Karolyn Hilda Patricia Pérez Gonzáles
Título del ejercicio:	Quick Submit
Título de la entrega:	Resultados_UCP_SistemasInformacion_2023_Tesis_KarolynPe...
Nombre del archivo:	PEREZ_GONZALES-BURGOS_FLOrES_INFORME_FINAL_DE_TES...
Tamaño del archivo:	382.3K
Total páginas:	33
Total de palabras:	7,099
Total de caracteres:	38,412
Fecha de entrega:	30-ene.-2024 06:54p. m. (UTC+0500)
Identificador de la entre...	2282047810

RESUMEN

La seguridad informática es de vital importancia en la actualidad, con el 70% de las empresas en el mundo implementando medidas extremas debido a la constante amenaza de ciberataques. Los ataques informáticos pueden causar daños significativos, como la pérdida de datos, la interrupción de servicios y la exposición de vulnerabilidades en los sistemas de seguridad. La Empresa de Agua Potable y Alcantarillado Sedaloreto S.A. se encuentra en riesgo debido a la falta de una política de seguridad informática, lo que la deja vulnerable a ataques cibernéticos y pérdida de información crítica, el problema principal que aborda esta investigación es el estado de seguridad informática en la E.P.S. Sedaloreto S.A. Se plantea como problema general "¿Cuál es el estado situacional de la seguridad informática de la E.P.S. Sedaloreto S.A.?", y se desglosa en problemas específicos relacionados con el nivel de riesgo y vulnerabilidades de seguridad informática. para abordar estos problemas, se propone una serie de objetivos, incluyendo la evaluación del nivel de riesgo de seguridad informática y la identificación de vulnerabilidades en la empresa, se aplicaron diversas técnicas de recolección de datos, como observación y encuestas, para evaluar diferentes aspectos de la seguridad informática en la organización. Los resultados muestran que el nivel de seguridad informática en la E.P.S. Sedaloreto S.A. es muy bajo, con altos niveles de ocurrencia de riesgos, falta de implementación de controles de seguridad y tiempos de recuperación prolongados en caso de catástrofe. Además, se identificaron numerosas vulnerabilidades y un alto porcentaje de frecuencia de amenazas o incidentes, en base a estos hallazgos, se hacen recomendaciones para mejorar la seguridad informática en la E.P.S. Sedaloreto S.A., incluyendo el desarrollo de políticas de seguridad, la implementación de controles de seguridad, la realización de evaluaciones periódicas de riesgos y la optimización de los tiempos de recuperación. las conclusiones resaltan la importancia de abordar la seguridad informática de manera proactiva y la necesidad de tomar medidas inmediatas para proteger la integridad, confidencialidad y disponibilidad de la información en la organización, en resumen, esta investigación destaca la urgencia de fortalecer la seguridad informática en la E.P.S. Sedaloreto S.A. y proporciona recomendaciones específicas para lograrlo

Palabras Claves: Seguridad Informática, Riesgos, Controles de seguridad

11

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° 341-2023-UCP-FCEI del 25 de abril 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. Ángel Alberto Marthans Ruíz. Mgr. — Miembro
- Ing. Tonny Eduardo Bardales Lozano, Mtro. — Miembro

Como Asesor: Ing. Ronald Melchor Infantes, Mtro

En la ciudad de Iquitos, siendo las **23 de febrero de 2024, a las 9:30 am**, 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 INFORMÁTICA DE LA E.P.S. SEDALORETO S.A. 2023***

Presentado por los sustentantes: **PEREZ GONZALES KAROLYN HILDA PATRICIA y BURGOS FLORES MELISSA JANE,**

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 MAYORÍA

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

Ing. Jimmy Max Ramírez Villacorta, Mtro
Presidente

Ing. Ángel Alberto Marthans Ruíz. Mgr
Miembro

Ing. Tonny Eduardo Bardales Lozano, Mtro.
Miembro

APROBACIÓN

HOJA DE APROBACIÓN

PROGRAMA ACADÉMICO DE INGENIERÍA DE SISTEMAS DE INFORMACIÓN
TESISTAS: PEREZ GONZALES KAROLYN HILDA PATRICIA y BURGOS FLORES MELISSA JANE

Tesis sustentada en acto publico el día 23 de febrero del 2024, a las 9:30 am , en las instalaciones de la UNIVERSIDAD CIENTÍFICA DEL PERÚ.

Ing. JIMMY MAX RAMIREZ VILLACORTA, Mtro.
PRESIDENTE DE JURADO

ING. ÁNGEL ALBERTO MARTHANS RUÍZ. Mgr
.MIEMBRO DE JURADO

TONNY EDUARDO BARDALES LOZANO, Mtro.
MIEMBRO DE JURADO

ING. RONALD MELCHOR INFANTES, Mtro
ASESOR

INDICE DEL CONTENIDO

Pagina

INDICE DE TABLAS

INDICE DE GRÁFICOS

INDICE DE FIGURAS

RESUMEN

La seguridad informática es de vital importancia en la actualidad, con el 70% de las empresas en el mundo implementando medidas extremas debido a la constante amenaza de ciberataques. Los ataques informáticos pueden causar daños significativos, como la pérdida de datos, la interrupción de servicios y la exposición de vulnerabilidades en los sistemas de seguridad. La Empresa de Agua Potable y Alcantarillado Sedaloreto S.A. se encuentra en riesgo debido a la falta de una política de seguridad informática, lo que la deja vulnerable a ataques cibernéticos y pérdida de información crítica, el problema principal que aborda esta investigación es el estado de seguridad informática en la E.P.S. Sedaloreto S.A. Se plantea como problema general "¿Cuál es el estado situacional de la seguridad informática de la E.P.S. Sedaloreto S.A.?" y se desglosa en problemas específicos relacionados con el nivel de riesgo y vulnerabilidades de seguridad informática, para abordar estos problemas, se propone una serie de objetivos, incluyendo la evaluación del nivel de riesgo de seguridad informática y la identificación de vulnerabilidades en la empresa, se aplicaron diversas técnicas de recolección de datos, como observación y encuestas, para evaluar diferentes aspectos de la seguridad informática en la organización. Los resultados muestran que el nivel de seguridad informática en la E.P.S. Sedaloreto S.A. es muy bajo, con altos niveles de ocurrencia de riesgos, falta de implementación de controles de seguridad y tiempos de recuperación prolongados en caso de catástrofe. Además, se identificaron numerosas vulnerabilidades y un alto porcentaje de frecuencia de amenazas o incidentes, en base a estos hallazgos, se hacen recomendaciones para mejorar la seguridad informática en la E.P.S. Sedaloreto S.A., incluyendo el desarrollo de políticas de seguridad, la implementación de controles de seguridad, la realización de evaluaciones periódicas de riesgos y la optimización de los tiempos de recuperación, las conclusiones resaltan la importancia de abordar la seguridad informática de manera proactiva y la necesidad de tomar medidas inmediatas para proteger la integridad, confidencialidad y disponibilidad de la información en la organización, en resumen, esta investigación destaca la urgencia de fortalecer la seguridad informática en la E.P.S. Sedaloreto S.A. y proporciona recomendaciones específicas para lograrlo.

Palabras Claves: Seguridad Informática, Riesgos, Controles de seguridad

ABSTRACT

nformation security is of paramount importance today, with 70% of companies worldwide implementing extreme measures due to the constant threat of cyberattacks. Cyberattacks can lead to significant damages, such as data loss, service interruptions, and exposure of vulnerabilities in security systems. The Water and Sewerage Company Sedaloreto S.A. is at risk due to the lack of an information security policy, leaving it vulnerable to cyberattacks and critical information loss. The main problem addressed by this research is the state of information security in E.P.S. Sedaloreto S.A. The general problem is posed as "What is the current state of information security at E.P.S. Sedaloreto S.A.?" and is broken down into specific issues related to the level of risk and information security vulnerabilities.

To address these issues, a series of objectives are proposed, including evaluating the level of information security risk and identifying vulnerabilities within the company. Various data collection techniques, such as observation and surveys, were employed to assess various aspects of information security within the organization. The results indicate that the level of information security at E.P.S. Sedaloreto S.A. is very low, with high levels of risk occurrence, a lack of security control implementation, and extended recovery times in case of disaster. Additionally, numerous vulnerabilities were identified, along with a high percentage of threat or incident frequency.

Based on these findings, recommendations are made to enhance information security at E.P.S. Sedaloreto S.A., including the development of security policies, the implementation of security controls, conducting periodic risk assessments, and optimizing recovery times. The conclusions emphasize the importance of proactively addressing information security and the immediate need to safeguard the integrity, confidentiality, and availability of information within the organization.

In summary, this research underscores the urgency of strengthening information security at E.P.S. Sedaloreto S.A. and provides specific recommendations to achieve this.

Keywords: Information Security, Risks, Security Controls

CAPÍTULO I: MARCO TEÓRICO

1.1 Antecedentes de Estudio

Cutin, Alipio (2020), Esta tesis se inscribe en la línea de investigación de sistemas de gestión de calidad y seguridad de la información en la Municipalidad Distrital de Canchaque, específicamente en el área de secretaría y fotocopiado. Se observa que los procesos de modificación de información, tanto de los trabajadores como de los ciudadanos, son altamente riesgosos debido a la constante rotación de personal. Además, los trabajadores de escritorio que utilizan computadoras están expuestos al robo de información, ya sea por la posibilidad de acceso de otros empleados a sus equipos o por la eliminación accidental de datos importantes. El objetivo principal de esta investigación consistió en analizar y diseñar un plan de seguridad informática en la Municipalidad Distrital de Canchaque con el fin de mejorar el control de datos e información, el enfoque de esta investigación se basó en un modelo cuantitativo de investigación descriptiva con un diseño no experimental de corte transversal. La población de estudio comprendió 10 trabajadores, seleccionados por conveniencia del investigador. Las técnicas utilizadas incluyeron encuestas y observaciones. Los resultados indicaron que el 90.00% de los trabajadores no estaban satisfechos con el sistema actual, la investigación concluyó con éxito al analizar y diseñar un plan de seguridad informática, que obtuvo una tasa de aceptación del 100%, de esta manera, se logró alcanzar satisfactoriamente el objetivo general propuesto.

Sisti, Maria (2019), El estudio se lleva a cabo mediante un análisis correlacional, descriptivo y transversal. Los datos recopilados a partir de encuestas, entrevistas al personal de la empresa y observación directa se interpretan y analizan para evaluar el nivel de seguridad informática en la empresa de producción de vino. Los resultados obtenidos evidencian que el grado de seguridad informática en esta empresa se relaciona directamente con la calidad y cantidad de los mecanismos de seguridad implementados. En otras palabras, a medida que se mejoren estos mecanismos de seguridad, se elevará la protección de los recursos informáticos, y viceversa; a pesar de que se aplican ciertos controles y medidas de seguridad en la empresa, estos no son suficientes y algunos son susceptibles

de mejora, lo que sitúa el nivel de seguridad informática en un punto intermedio. Esta situación expone a la entidad a ciertas amenazas y riesgos. Por lo tanto, se hace necesario un proceso de mejora y fortalecimiento de la seguridad con el objetivo de garantizar una protección adecuada de la información y de todos los recursos informáticos de la empresa.

Rodríguez, William (2016), En el presente estudio, se busca comprender los problemas de seguridad informática que enfrentó la empresa pública Aguapen EP en el año 2016 y su impacto en la pérdida de productividad de los usuarios del parque de computadoras de esta entidad. A través de una investigación centrada en las herramientas tecnológicas para la seguridad informática, se pretende identificar la solución más efectiva para mejorar la seguridad de las computadoras en esta empresa pública, este estudio tiene como objetivo principal la implementación de la solución más adecuada para proteger los datos, los equipos de cómputo y la producción de la empresa pública Aguapen EP en la ciudad de Salinas durante el año 2016. Para alcanzar este objetivo, se utilizará el enfoque epistemológico de la Investigación Empirista. El diseño de investigación adoptado es de naturaleza no experimental y de tipo transaccional. Se trata de una investigación descriptiva que emplea el método Hipotético-Deductivo, ya que se formula una hipótesis y se realiza una encuesta con el fin de observar y verificar los resultados obtenidos en relación con la hipótesis planteada.

Ancajima, María (2016), La presente tesis se enmarca en la línea de investigación de tecnologías de información y comunicación (TIC) para la mejora continua de la calidad de las organizaciones en el contexto peruano, específicamente desde la perspectiva de la escuela profesional de Ingeniería de Sistemas. Este trabajo se centró en la elaboración de una propuesta de implementación de seguridad informática en el ámbito de las TIC de la Institución Educativa San Miguel Arcángel, ubicada en Catacaos, Piura, durante el año 2016, el enfoque de la investigación fue cuantitativo, con un nivel descriptivo y un diseño no experimental de corte transversal. El objetivo general fue llevar a cabo un estudio de los riesgos presentes en la institución, con la finalidad de ofrecer una sólida propuesta de implementación de seguridad informática para la I.E. San Miguel Arcángel. Esta propuesta tenía como finalidad mejorar el control de seguridad en

la institución y potenciar la competencia en el uso de herramientas tecnológicas por parte de docentes, personal administrativo y alumnos, la muestra de la población de estudio consistió en 60 personas, incluyendo docentes, alumnos y personal administrativo que utilizaban equipos tecnológicos en distintas áreas de la institución. Los resultados obtenidos revelaron que el 75.00% de los encuestados se mostraron satisfechos con el uso de las TIC en el proceso de enseñanza, mientras que el 73.00% expresó satisfacción con la formación y capacitación en el manejo de las TIC. Asimismo, el 73.00% de los encuestados se sintió satisfecho con la seguridad informática en el entorno de las TIC en la institución.

Solarte, Francisco; Rosero, Edgar; Del Carmen, Miriam (2015), El propósito del artículo es cultivar las capacidades de los ingenieros de sistemas, permitiéndoles liderar proyectos de diagnóstico destinados a la implementación y puesta en marcha de sistemas de seguridad de la información (SGSI) en conformidad con los estándares ISO/IEC 27001 y el marco de control propuesto en la norma ISO/IEC 27002. Los resultados de una experiencia aplicando fases de auditoría y una metodología de análisis y evaluación de riesgos se presentan, junto con la creación y aplicación de diversos instrumentos, como cuestionarios dirigidos a los administradores, claves de seguridad, entrevistas con el personal de TI y usuarios de los sistemas, pruebas de intrusión y evaluaciones que permiten establecer el estado actual de seguridad. Luego, se utiliza una lista de verificación basada en la norma para confirmar la presencia de controles de seguridad en los procesos organizacionales. Finalmente, basándose en los resultados del análisis y la evaluación de riesgos, se proponen medidas de seguridad para su integración futura en un SGSI que satisfaga las necesidades de seguridad de la información y la ciberseguridad.

1.2 Bases Teóricas

Seguridad Informática

La seguridad informática, según Morales (2022), se define como el conjunto de medidas técnicas, organizativas y legales destinadas a salvaguardar los sistemas informáticos, redes y dispositivos contra accesos no autorizados, modificaciones, divulgación, destrucción o interrupción de los servicios que brindan. Su objetivo principal es garantizar la integridad, confidencialidad y disponibilidad de los datos, así como prevenir interrupciones y fallos en los sistemas informáticos. La creciente complejidad de los sistemas y las amenazas informáticas sofisticadas han resaltado la importancia de la seguridad informática en la actualidad.

La seguridad informática se ha convertido en un tema de interés público en los últimos años, con términos como "clave de usuario", "contraseña", "fraude informático" y "hacker" siendo comunes tanto para expertos como para usuarios comunes. En la actualidad, contar con sólidos conocimientos en este campo es esencial para evitar poner en riesgo la información, el equipo y la integridad del usuario.

Gómez (2006) la define como cualquier medida que prevenga la ejecución de operaciones no autorizadas en sistemas o redes informáticas que puedan causar daños a la información, el equipo o el software.

Kissel (2012) la relaciona con la protección de la información y los sistemas de información de accesos no autorizados, involucrando tres elementos fundamentales: información, software y hardware.

Para garantizar la seguridad de los datos, es fundamental cumplir con tres componentes esenciales: integridad, disponibilidad y confidencialidad.

En cuanto a los tipos de seguridad informática, se pueden destacar:

Seguridad física: Enfocada en la protección de dispositivos físicos y el acceso a ellos, incluyendo medidas como el control de acceso a instalaciones, el uso de cerraduras y la protección de equipos de cómputo.

Seguridad lógica: Se centra en la protección del software y los datos, involucrando medidas como contraseñas, autenticación de usuarios, gestión de permisos, firewalls y cifrado de datos.

Seguridad de red: Orientada a proteger las redes y la información transmitida a través de ellas, utilizando firewalls, autenticación de usuarios, VPN, monitoreo del tráfico y prevención de ataques DoS.

Seguridad de la información: Su objetivo es la protección de la información en sistemas o redes, a través de políticas de seguridad, control de acceso y prevención de pérdida de datos.

Seguridad de aplicaciones: Dirigida a proteger las aplicaciones de software utilizadas en sistemas o redes, mediante prácticas de codificación segura, gestión de permisos y prevención de vulnerabilidades.

Estos tipos de seguridad informática son esenciales para proteger los sistemas y redes de posibles amenazas. Los objetivos de la seguridad informática, por su parte, incluyen la confidencialidad, integridad, disponibilidad, autenticación, autorización, responsabilidad, no repudio y protección física de hardware y dispositivos. Estos objetivos buscan garantizar la protección de la información, los sistemas y las redes, y asegurar que los usuarios autorizados puedan acceder a la información cuando sea necesario. La responsabilidad y la no repudio también son importantes para rastrear y responsabilizar a los usuarios por sus acciones en el sistema, mientras que la seguridad física protege el hardware y los dispositivos críticos. En resumen, la seguridad informática es un campo en constante evolución y su conocimiento es esencial para mantener seguros los sistemas y redes.

Bases de la Seguridad Informática

Una célebre cita que ha ganado renombre en el ámbito de la seguridad proviene de Eugene Spafford, destacado profesor de ciencias informáticas en la Universidad Purdue de Indiana, EEUU. Spafford expresó que "el único sistema seguro es aquel que está apagado y desconectado, enterrado en un refugio de cemento, rodeado por gas venenoso y custodiado por guardianes bien pagados y muy bien armados. Aún así, yo no apostaría mi vida por él.", Hablar de seguridad informática en términos absolutos resulta una empresa imposible, lo cual nos lleva a enfocarnos en la fiabilidad del sistema, que, en esencia, representa una perspectiva más realista.

La fiabilidad, en este contexto, se define como la probabilidad de que un sistema se comporte de acuerdo a las expectativas preestablecidas.

En términos generales, un sistema puede considerarse seguro y fiable si podemos garantizar tres elementos fundamentales:

1. Confidencialidad: Garantizar que el acceso a la información ocurra únicamente a través de autorización y de manera controlada.
2. Integridad: Asegurar que la modificación de la información solo sea posible con autorización, preservando su integridad original.
3. Disponibilidad: Mantener la información del sistema accesible mediante autorización, evitando interrupciones no autorizadas.

Estos son los pilares clave para evaluar y garantizar la seguridad y fiabilidad de los sistemas informáticos, reconociendo que la seguridad absoluta es una utopía y que la fiabilidad es un objetivo más realista en la práctica.

Figura 01: Principios de la seguridad de la información

Fuente: ISO/IEC 27001

Tipo de Seguridad Informática

Existen diversos tipos de seguridad informática empleados para salvaguardar los sistemas y redes de posibles amenazas. A continuación, se detallan algunos de los tipos más comunes:

1. Seguridad Física: Se refiere a la protección de los dispositivos físicos y la gestión del acceso a ellos. Esto incluye medidas como la restricción de acceso a instalaciones, el uso de cerraduras, el control de ingreso a áreas críticas y la seguridad de los equipos de cómputo.
2. Seguridad Lógica: Esta categoría se enfoca en la protección del software y los datos que residen en un sistema o red. Comprende elementos como el uso de contraseñas, la autenticación de usuarios, la gestión de permisos, la implementación de firewalls y el cifrado de datos.
3. Seguridad de Red: Su propósito principal es resguardar las redes informáticas y los datos que fluyen a través de ellas. Incluye la implementación de firewalls, autenticación de usuarios, configuración de VPNs (redes privadas virtuales), supervisión del tráfico de red y prevención de ataques de denegación de servicio (DoS).
4. Seguridad de la Información: Se centra en la protección de la información almacenada en un sistema o red. Implica la definición y aplicación de políticas de seguridad, la gestión del acceso a la información y la prevención de pérdida de datos.
5. Seguridad de Aplicaciones: Esta área se dedica a proteger las aplicaciones de software utilizadas en un sistema o red. Incluye la implementación de prácticas de codificación segura, la administración de permisos y la prevención de vulnerabilidades de seguridad.

Cabe señalar que existen numerosos otros tipos de seguridad informática, y este campo experimenta una constante evolución con la aparición de nuevas amenazas y técnicas. En consecuencia, resulta fundamental mantenerse actualizado respecto a las tendencias y mejores prácticas en seguridad informática para proteger eficazmente los sistemas y redes.

Políticas de seguridad

De acuerdo con las afirmaciones de Laudon, K. C. y Laudon, J. P. (2012), así como las de García Pierrat, G. y Vidal Ledo, M. J. (2016), para asegurar la protección de los activos informáticos frente a los riesgos identificados, es imperativo desarrollar una política de seguridad. Dicha política posibilita la utilización eficiente y segura de las tecnologías de la información y las comunicaciones al establecer las directrices sobre su empleo. Las políticas de seguridad establecen normativas para el personal involucrado en el sistema informático, definen el uso adecuado de los recursos informáticos, regulan el acceso a los mismos, gestionan la identidad de los usuarios, determinan la política de privacidad de la empresa, establecen la responsabilidad de los usuarios y regulan el uso de equipos y redes corporativas para fines personales.

De acuerdo con García Pierrat, G. y Vidal Ledo, M. J. (2016), las políticas de seguridad representan la estrategia global de la empresa, mientras que las medidas y procedimientos constituyen los pasos específicos necesarios para alcanzar la seguridad informática. Es fundamental que una política de seguridad eficaz pueda ser implementada a través de estas medidas y procedimientos.

Medidas de seguridad

A partir de la identificación de posibles eventos que puedan impactar a la empresa, las medidas y procedimientos de seguridad definen las acciones requeridas, los recursos necesarios y las responsabilidades pertinentes. No existe una combinación de controles universalmente óptima, ya que cada empresa es única y, por lo tanto, se necesita realizar un análisis de riesgos para identificar los activos más susceptibles en cada caso particular. En contraste con las políticas de seguridad generales, las medidas y procedimientos son específicos y se aplican de manera personalizada según las necesidades particulares de cada área (García Pierrat, G. y Vidal Ledo, M. J., 2016).

Conforme a la explicación de Saroka, R. H. (2002), las medidas de seguridad se pueden clasificar en tres categorías distintas:

Medidas preventivas: Orientadas a reducir la probabilidad de que las amenazas se materialicen mediante acciones destinadas a prevenir o minimizar su impacto.

Medidas de detección: Diseñadas para mitigar los efectos de las amenazas una vez que se han concretado y para identificar oportunamente los eventos que puedan surgir.

Medidas correctivas: Dirigidas a restaurar la capacidad de operación normal resolviendo los problemas que hayan surgido.

Figura 02: Tipos de medidas de seguridad

Fuente: García Pierrat, G. y Vidal Ledo, M. J. (2016).

1.3 Definición de Términos Básicos:

Firewall: Un firewall es un dispositivo o software que se utiliza para proteger una red o sistema informático al controlar y filtrar el tráfico de red. Su objetivo principal es prevenir accesos no autorizados y proteger contra amenazas externas.

Malware: Es un término genérico que abarca todo tipo de software malicioso, como virus, gusanos, troyanos y spyware, diseñados para infiltrarse en sistemas o redes, dañar datos o robar información.

Virus Informático: Un virus informático es un tipo de malware que se propaga al adjuntarse a archivos legítimos o programas y, cuando se ejecutan, infecta el sistema y puede causar daños.

Phishing: El phishing es una técnica utilizada por ciberdelincuentes para engañar a las personas y hacer que divulguen información confidencial, como contraseñas y datos bancarios, a menudo haciéndose pasar por entidades de confianza.

Cifrado: El cifrado es el proceso de convertir datos en un formato ilegible para proteger su confidencialidad. Solo las personas o sistemas autorizados pueden descifrar los datos y acceder a ellos.

Contraseña: Una contraseña es una secuencia de caracteres que se utiliza para autenticar a un usuario y permitir el acceso a una cuenta o sistema. Debe ser secreta y única para cada usuario.

Autenticación de Dos Factores (2FA): La autenticación de dos factores es un método que requiere que los usuarios proporcionen dos formas distintas de identificación para verificar su identidad, generalmente algo que conocen (como una contraseña) y algo que poseen (como un código generado en una aplicación).

Ingeniería Social: La ingeniería social es una técnica en la que los atacantes manipulan a las personas para obtener información confidencial o acceso a sistemas. Puede implicar el uso de la persuasión o el engaño.

Parche de Seguridad: Un parche de seguridad es una actualización de software que corrige vulnerabilidades o problemas de seguridad en un sistema o aplicación. Es importante aplicar parches de seguridad regularmente para protegerse contra amenazas conocidas.

Política de Seguridad: Una política de seguridad es un conjunto de directrices y reglas que define las prácticas de seguridad que deben seguirse en una organización. Ayuda a establecer un marco para proteger la información y los recursos.

VPN (Red Privada Virtual): Una VPN es una tecnología que permite establecer conexiones seguras a través de redes públicas como Internet. Se utiliza para proteger la privacidad y la seguridad de las comunicaciones.

Backup (Copia de Seguridad): Un backup es una copia de los datos que se realiza para poder restaurarlos en caso de pérdida o daño. Los backups son esenciales para la recuperación de datos en situaciones de desastre o incidentes de seguridad.

CAPÍTULO II: PLANTEAMIENTO DEL PROBLEMA

2.1 Descripción del Problema

En la actualidad la Seguridad Informática se ha convertido en una de las tareas fundamentales que tienen los profesionales de Tecnologías de la Información y Comunicaciones, el 70% de empresas en el mundo han implementado medidas extremas respecto a la seguridad de la información ya que constantemente recibieron ciber ataques, Los ataques informáticos son acciones malintencionadas realizadas por individuos o grupos con el propósito de acceder, dañar o robar información confidencial, interrumpir el funcionamiento de sistemas informáticos o causar daños a la reputación de una empresa u organización. Estos ataques pueden incluir virus y malware, phishing, ataques de denegación de servicio (DDoS), ransomware y hacking, entre otros. Las consecuencias de los ataques informáticos pueden ser graves, como la pérdida de datos, el robo de información personal y financiera, la interrupción de servicios críticos y la exposición de vulnerabilidades en los sistemas de seguridad. Por esta razón, es importante que las empresas y organizaciones implementen medidas proactivas para prevenir y mitigar los efectos de los ataques informáticos, como establecer políticas de seguridad informática, capacitar a los empleados en prácticas seguras y mantener los sistemas informáticos actualizados y protegidos con herramientas de seguridad adecuadas.

La E.P.S. Sedaloreto S.A. es una compañía peruana que se dedica a ofrecer servicios de suministro de agua potable y alcantarillado en la región de Loreto. Fundada en 1999 como una empresa estatal, en 2014 se transformó en una empresa mixta que cuenta con la participación del sector privado. La empresa tiene como propósito principal brindar servicios de alta calidad a sus clientes y fomentar el crecimiento sostenible de la región. Además de sus actividades principales, la compañía se enfoca en la gestión de residuos sólidos y en la protección del medio ambiente, esta entidad cuenta con la oficina de informática el cual tiene falta de una política de seguridad informática en la empresa de agua potable la deja vulnerable a ataques cibernéticos y a la posible pérdida de información crítica. La ausencia de protocolos para la gestión de contraseñas, permisos de usuario y actualizaciones de software, aumenta la probabilidad de

comprometer los sistemas de la empresa por parte de hackers o malware. Además, la empresa no realiza evaluaciones periódicas de riesgos ni implementa medidas de seguridad adecuadas para proteger su infraestructura tecnológica. Estas deficiencias podrían provocar pérdidas financieras y de reputación, así como la exposición de datos sensibles, la interrupción de los servicios y la disminución de la confianza de los clientes.

Las vulnerabilidades son debilidades o fallos en sistemas y aplicaciones informáticas, redes o software que pueden ser explotados por actores malintencionados para acceder, robar, alterar o destruir información sensible.

Los riesgos son amenazas que explote alguna vulnerabilidad de uno o varios activos y afecta el funcionamiento del un sistema

2.2 Formulación del Problema

2.2.1 Problema General

¿Cuál es el estado situacional de la seguridad Informática de la E.P.S. Sedaloreto S.A.?

2.2.2 Problemas Específicos

- ✓ ¿Cuál es el nivel de riesgo de la seguridad informática de la E.P.S. Sedaloreto S.A.?
- ✓ ¿Cuál es el nivel de vulnerabilidades de la seguridad informática de la E.P.S. Sedaloreto S.A.?

2.3 Objetivos

2.3.1 Objetivo General

Evaluar el estado situacional de la seguridad Informática de la E.P.S. Sedaloreto S.A.

2.3.2 Objetivos Específicos

- ✓ Evaluar el nivel de riesgo de la seguridad informática de la E.P.S. Sedaloreto S.A.

- ✓ Evaluar las vulnerabilidades de la seguridad informática de la E.P.S. Sedaloreto S.A.

2.4 Hipótesis

✓ Hipótesis General:

- H1: El nivel de seguridad informática de la E.P.S. Sedaloreto S.A. es muy bajo
- H0: El nivel de seguridad informática de la E.P.S. Sedaloreto S.A. es muy alto

2.5 Variables

2.5.1 Identificación de Variables

Variable 1: Nivel de seguridad informática.

2.5.2 Definición Conceptual de las Variables

Variable	Definición Conceptual	Definición Operacional
Nivel de 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.

2.5.3 Operacionalización de las Variables

Tabla N°01: Operacionalización de Variables

Variables	Dimensiones	Indicadores	Instrumento de Recolección de datos
Nivel de Seguridad Informática	Evaluación de Riesgos	% de Riesgo	Documental, Encuesta
		Nivel de Riesgo	
		Tiempo de Recuperación	
	Análisis de Vulnerabilidades	% Controles implementados	
		% Frecuencia de amenazas o incidentes	

Fuente: Elaboración Propia

Capítulo III: Metodología

3.1 Tipo y Diseño de Investigación

- Tipo de Investigación

Descriptiva porque vamos a describir el estado situacional de los activos informáticos de la E.P.S. Sedaloreto S.A., 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 informática de la E.P.S. Sedaloreto S.A. que haciende a 05 personas, distribuido de la siguiente manera:

Tabla 02: Distribución del Personal de la Oficina de Informática

Cargo	Cantidad
Jefe de Oficina	01
Analista Programador	01
Soporte Técnico	01
Soporte a Usuarios	01
Administrador de redes y servidores	01
Total	05

Muestra

Como la muestra es finita y no sobre pasa las 30 personas se tomó como muestra a toda la población, que son los 05 trabajadores.

3.3 Técnicas, instrumentos y procedimientos de recolección de datos

- Técnica de Recolección de Datos:

  Observación: La técnica de observación se erige como una herramienta fundamental para evaluar la seguridad informática de una organización, permitiendo realizar una evaluación directa de los controles y prácticas de seguridad en ejecución. A través de esta metodología, es posible descubrir áreas de mejora y detectar riesgos y vulnerabilidades que necesitan ser abordados con el fin de fortalecer la seguridad informática en una entidad como E.P.S. Sedaloreto S.A.

  Encuesta: Proporciona una visión importante de cómo se percibe y se practica la seguridad informática en E.P.S. Sedaloreto S.A. También puede identificar áreas que requieren atención y mejoras, y brindar datos cuantitativos que ayuden en la toma de decisiones estratégicas para fortalecer la seguridad en la organización.

- Instrumento de Recolección de Datos:
  Ficha de Observación: es un documento o formulario estructurado que se utiliza como una herramienta de registro y seguimiento durante una evaluación de seguridad informática. Esta ficha generalmente contiene campos específicos donde los evaluadores pueden anotar observaciones, hallazgos y datos relevantes relacionados con la seguridad informática en la organización. Las fichas de observación se utilizan para documentar de manera sistemática lo que se observa y se descubre durante el proceso de evaluación de seguridad.

  Cuestionario: Es un conjunto de preguntas estructuradas diseñadas para recopilar información específica sobre las prácticas, políticas, procedimientos y controles de seguridad informática en la organización. Estos cuestionarios se utilizan como una herramienta sistemática para evaluar y medir el estado actual de la seguridad de la información y la tecnología en la entidad.

- Procedimiento de Recolección de Datos:

  Para recolectar información para realizar el análisis de vulnerabilidades emplearemos la ficha de observación y un cuestionario a los trabajadores de la oficina de informática.

  Para recolectar la información para la evaluación de riesgo emplearemos una matriz de riesgo.

3.4 Procesamiento y análisis de datos.

La Información se procesó en software estadístico SPSS Versión 22, cuyos resultados se clasificaron en cuadros y gráficos estadísticos.

Capítulo IV: Resultados

Resultados de la Variable: Nivel de Seguridad Informática

Dimensión: Evaluación de Riesgo

Indicador1: Porcentaje de Ocurrencia

Tabla N°02
Porcentaje de Ocurrencias del Riesgo - E.P.S. Sedaloreto S.A.

N°	Riesgo de Seguridad	Probabilidad (0-1)	Impacto (0-1)	Riesgo (Probabilidad x Impacto)
1	Fuga de datos	0.3	0.9	0.27
2	Ataque de phishing	0.5	0.7	0.35
3	Falta de parches de seguridad	0.4	0.8	0.32
4	Políticas de seguridad débiles	0.6	0.6	0.36
5	Brecha de seguridad	0.2	0.9	0.18
6	Ataque de DDoS	0.3	0.7	0.21
7	Contraseñas débiles	0.4	0.7	0.28
8	Acceso no autorizado	0.5	0.8	0.4
9	Malware	0.2	0.9	0.18
10	Auditoría de seguridad deficiente	0.4	0.6	0.24

Fuente: Elaboración propia

Cálculo del Porcentaje de Riesgo de Seguridad:

Suma de los riesgos (Riesgo Total) = 0.27 + 0.35 + 0.32 + 0.36 + 0.18 + 0.21 + 0.28 + 0.4 + 0.18 + 0.24 = 2.59

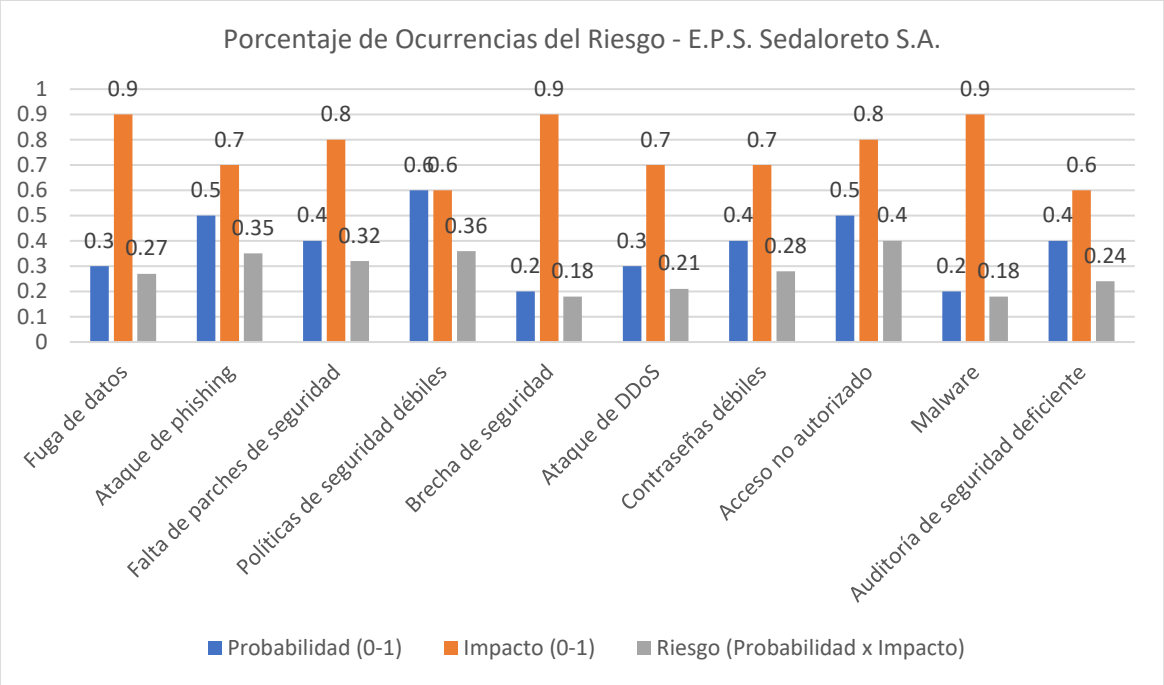
Número total de riesgos evaluados = 10

Porcentaje de Riesgo = (Riesgo Total / Número total de riesgos evaluados) * 100

Porcentaje de Riesgo = (2.59 / 10) * 100 = 25.9%

El porcentaje de riesgo de seguridad en la E.P.S. Sedaloreto S.A. es del 25.9%. Esto indica que, en la evaluación realizada, se identificaron riesgos que, en conjunto, representan un riesgo total del 25.9% para la seguridad de la organización.

Gráfico N°01
Porcentaje de Ocurrencias del Riesgo - E.P.S. Sedaloreto S.A.



Fuente: Elaboración propia

Dimensión: Evaluación de Riesgo

Indicador 2: Nivel de Riesgo de la Seguridad Informática

Tabla N°03

Nivel de Riesgo de la Seguridad Informática- E.P.S. Sedaloreto S.A.

N°	Riesgo de Seguridad	Probabilidad	Impacto	Riesgo	Severidad
1	Fuga de datos	Alta	Muy Alto	Crítico	Muy Alto
2	Ataque de phishing	Alta	Alto	Alto	Alto
3	Falta de parches de seguridad	Media	Alto	Medio	Medio
4	Políticas de seguridad débiles	Alta	Medio	Alto	Alto
5	Brecha de seguridad	Baja	Muy Alto	Alto	Alto
6	Ataque de DDoS	Baja	Alto	Bajo	Bajo
7	Contraseñas débiles	Media	Alto	Medio	Medio
8	Acceso no autorizado	Alta	Alto	Alto	Alto
9	Malware	Baja	Muy Alto	Alto	Alto
10	Auditoría de seguridad deficiente	Media	Medio	Medio	Medio

Fuente: Elaboración propia

En esta matriz de riesgo, se han evaluado 10 riesgos de seguridad informática en función de su probabilidad y su impacto. Cada riesgo se coloca en una de las siguientes categorías:

- Crítico: Riesgos que tienen una alta probabilidad y un impacto muy alto, lo que los convierte en amenazas críticas que deben abordarse de inmediato.
- Alto: Riesgos que tienen una alta probabilidad y un impacto alto, lo que los hace significativos y requiere atención.

- Medio: Riesgos con una probabilidad y un impacto moderados, que deben ser gestionados de manera adecuada.
- Bajo: Riesgos con una baja probabilidad y un impacto moderado, que aún requieren supervisión y gestión.
- Muy Bajo: Riesgos con una baja probabilidad y un impacto bajo, que pueden requerir seguimiento ocasional.

Dimensión: Evaluación de Riesgo

Indicador 3: Tiempo de Recuperación en Caso de Catástrofe - E.P.S. Sedaloreto S.A.

Tabla N°04
Tiempo de Recuperación en Caso de Catástrofes

Sistema o Servicio Crítico	Tiempo de Recuperación Objetivo
Dominio de la Red	12 horas
Sistema de Gestión Comercial	24 horas
Sistema de Gestión Administrativa AVALON	48 horas
Correo Electrónico	6 horas
Sistema de Gestión de Incidencias	36 horas
Sitio Web Público	72 horas
Red de Comunicación Interna	8 horas
Sistema de Atención al Cliente	24 horas
Sistema de Recursos Humanos	48 horas

Fuente: Elaboración propia

Estos son tiempos de recuperación en el que el área de informática de la E.P.S. Sedaloreto S.A. lograría solucionar los problemas de cada sistema o servicio. Los tiempos de recuperación se expresan en horas y representan el período máximo aceptable para recuperar la funcionalidad de cada sistema o servicio después de una catástrofe informática.

Dimensión: Análisis de Vulnerabilidades

Indicador 1: Porcentaje de Frecuencia de amenazas o incidentes

Tabla N°05

Porcentaje de Frecuencia de Amenazas o Incidentes - E.P.S. Sedaloreto S.A.

Tipo de Amenaza o Incidente	Número de Incidentes Reportados (en el año 2022)
Malware	12
Ataques de Phishing	6
Acceso no autorizado	8
Brechas de Seguridad	4
Fugas de Datos	3
Ataques de Denegación de Servicio (DDoS)	5

Fuente: Elaboración propia

Cálculo del Porcentaje de Frecuencia:

Suma de incidentes reportados en un año = 12 + 6 + 8 + 4 + 3 + 5 = 38 incidentes.

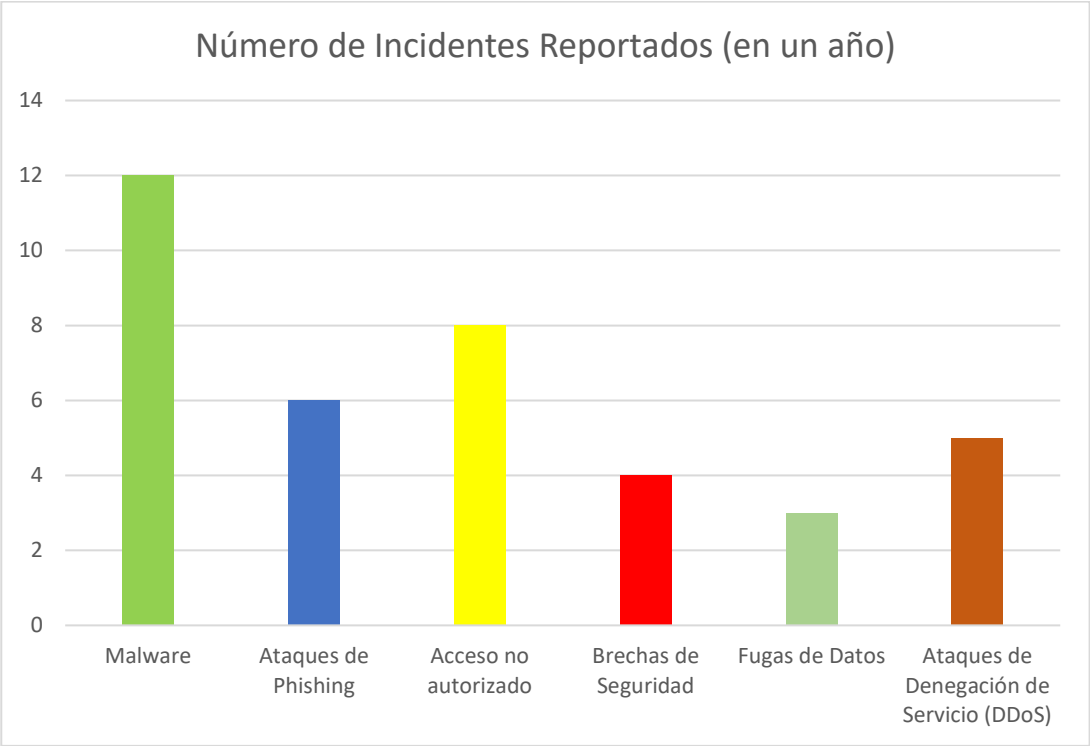
Número total de amenazas o incidentes evaluados = 6 tipos de amenazas o incidentes.

Porcentaje de Frecuencia = (Suma de incidentes reportados / Número total de amenazas o incidentes evaluados) * 100

Porcentaje de Frecuencia = (38 / 6) * 100 = 633.33%

El porcentaje de frecuencia de amenazas o incidentes en la E.P.S. Sedaloreto S.A. es del 633.33% en un período de un año, lo que indica que en promedio se han reportado aproximadamente 6.33 incidentes por cada tipo de amenaza o incidente evaluado.

Gráfico N°02
Número de Incidentes Reportados (2022)
- E.P.S. Sedaloreto S.A.



Fuente: Elaboración propia

Dimensión: Análisis de Vulnerabilidades

Indicador 2: Porcentaje de Controles Implementados

Tabla N°03

Porcentaje de Controles de Seguridad Implementados - E.P.S. Sedaloreto S.A.

N°	Control de Seguridad	Descripción	Estado de Implementación (Cumplido/En Progreso/No Cumplido)
1	Política de Contraseñas	Establece requisitos para contraseñas seguras y su cambio periódico.	Cumplido
2	Firewall	Filtra el tráfico de red para proteger contra amenazas y ataques.	Cumplido
3	Sistema de Detección de Intrusos	Monitorea el tráfico de red en busca de actividades sospechosas.	No Cumplido
4	Auditoría de Seguridad	Registra y revisa eventos de seguridad para detectar intrusiones.	No Cumplido
5	Plan de Continuidad del Negocio	Define procedimientos para mantener operaciones en caso de desastres.	No Cumplido
6	Control de Acceso	Gestiona quién tiene acceso a recursos y datos críticos.	No Cumplido
7	Copias de Seguridad	Realiza respaldos de datos críticos para la recuperación de desastres.	Cumplido
8	Seguimiento de Eventos	Monitorea y alerta sobre eventos y actividades inusuales en tiempo real.	No Cumplido
9	Encriptación de Datos	Protege datos confidenciales mediante la conversión en información incomprensible.	No Cumplido
10	Políticas de Seguridad	Establece directrices y reglas para garantizar la seguridad de la información.	No Cumplido

11	Capacitación de Empleados	Educa a los empleados sobre prácticas de seguridad informática.	No Cumplido
12	Pruebas de Penetración	Evalúa la seguridad de sistemas mediante simulación de ataques.	No Cumplido
13	Actualización de Sistemas	Mantiene los sistemas y software actualizados con parches de seguridad.	Cumplido
14	Control de Dispositivos Móviles	Gestiona y protege dispositivos móviles utilizados en la organización.	No Cumplido
15	Filtros de Correo	Filtra correos electrónicos para detectar y bloquear amenazas.	En Proceso
16	Sistema de Detección de Malware	Identifica y bloquea malware y virus en sistemas y redes.	Cumplido
17	Control de Acceso a Redes	Regula el acceso a la red y los recursos en función de roles y políticas.	En Proceso
18	Auditoría de Acceso a Datos	Registra y revisa quién accede y modifica datos sensibles.	No Cumplido
19	Autenticación de Múltiples Factores	Requiere varias formas de autenticación para el acceso.	No Cumplido
20	Política de Limpieza de Datos	Establece procedimientos para eliminar datos de manera segura.	No Cumplido

Fuente: Elaboración propia

Porcentaje de Controles de Seguridad Implementados:

Conteo de los controles implementados.
5 controles que se consideran "Cumplidos".

Calcular el total de controles evaluados.
hay un total de 20 controles en la lista.

Para Calcular el porcentaje de controles implementados.
Dividir el número de controles implementados por el total de controles evaluados y multiplicar por 100.

En este caso:

Porcentaje = (Número de controles implementados / Total de controles evaluados) * 100
Porcentaje = (5 / 20) * 100
Porcentaje = 25%

El porcentaje de controles de seguridad implementados en la E.P.S. Sedaloreto S.A. es del 25%. Esto indica que se han implementado aproximadamente el 25% de los controles de seguridad evaluados,

Prueba de Hipótesis General:

De acuerdo a los resultados de porcentaje de ocurrencia el cual se demuestra que los índices de ocurrencia son muy altos, el nivel de riesgo de la seguridad informática, el cual predomina la probabilidad alta, el impacto alto, el riesgo alto y la severidad alta, el porcentaje de frecuencia de amenazas o incidentes es de 6,33&, Porcentaje de Controles Implementados es de solo 25% del total, podemos determinar que el nivel de seguridad informática de la E.P.S. Sedaloreto S.A. es muy bajo, por lo tanto se rechaza la hipótesis nula y se acepta la hipótesis alternativa.

CAPÍTULO V: DISCUSIÓN, CONCLUSIONES Y RECOMENDACIONES

Discusiones

Al igual que la tesis de Cutin, Alipio (2020), donde se evalúa el sistema de gestión de calidad y seguridad de la información en la Municipalidad Distrital de Canchaque, específicamente en el área de secretaría y fotocopiado. Utilizando las técnicas utilizadas incluyeron encuestas y observaciones se pudo evidenciar que los niveles de seguridad informática se encuentran con niveles bajos de implementación, en nuestra investigación se puedo determinar que la E.P.S. Sedaloreto también presenta niveles bajos de implementación de actividades y controles de seguridad.

Al igual que la tesis de Sisti, Maria (2019), donde se evalúa el nivel de seguridad informática en la empresa de producción de vino donde se evidencian que el grado de seguridad informática en esta empresa se relaciona directamente con la calidad y cantidad de los mecanismos de seguridad implementados, donde se demuestra que están en niveles muy bajos, coincidiendo con nuestra investigación.

Al igual que la tesis de Rodríguez, William (2016), donde se busca comprender los problemas de seguridad informática que enfrentó la empresa pública Aguapen EP en el año 2016 y su impacto en la pérdida de productividad de los usuarios del parque de computadoras de esta entidad, el cual se trata de una investigación descriptiva que emplea el método Hipotético-Deductivo, el cual sus resultados coinciden con nuestra investigación el cual señala que los problemas de seguridad informática persisten de manera continua coincidiendo con nuestra investigación el cual demuestra la falta de implementación de medidas de seguridad para asegurar la integridad, disponibilidad y confidencialidad de la información.

Conclusiones

Se logró evaluar el porcentaje de ocurrencia del riesgo ejecutada a la E.P.S. Sedaloreto el cual permitirá ayudar a la organización a priorizar y enfocarse en los riesgos más críticos y tomar medidas para mitigarlos, con la finalidad de implementar un sistema de gestión de seguridad informática más efectivo.

Se logró elaborar una matriz de riesgo el cual determino que los niveles de riesgo son muy alarmantes por lo tanto la organización deberá priorizar sus esfuerzos en la gestión de riesgos y a enfocarse en los riesgos más críticos y significativos para la seguridad informática.

Se logro evaluar los tiempos en la que la E.P.S. Sedaloreto S.A. le puede tomar para recuperarse de una catástrofe, encontrando tiempos de recuperación muy prolongados que pueden paralizar los procesos mucho tiempo, y ello significa que estos tiempos son muy críticos que afectan a la continuidad de los servicios y por ende puede causar molestias a los usuarios y pérdidas económicas para la empresa.

Se logró evaluar el nivel de cumplimiento en cuanto a seguridad informática teniendo como resultado que existen controles pendientes de implementación lo cuales deben abordarse para fortalecer aún más la seguridad.

Recomendaciones

- ✓ Se recomienda a la E.P.S. Sedaloreto S.A., Desarrollar e implementar políticas de seguridad informática sólidas que aborden la gestión de contraseñas, el acceso a los sistemas, la seguridad de los datos, la gestión de incidentes, y la concienciación en seguridad entre los empleados.

- ✓ Se recomienda a la E.P.S. Sedaloreto S.A., realizar evaluaciones o auditorias constantes para ver si se cumplen las medidas de seguridad implementadas con la finalidad de asegurar la integridad, confidencialidad y disponibilidad de su información.

- ✓ Se recomienda a la E.P.S. Sedaloreto S.A., mantener actualizados todos los sistemas y software para mitigar vulnerabilidades conocidas. Establece un proceso de gestión de parches efectivo.

- ✓ Se recomienda a la E.P.S. Sedaloreto S.A., reestructurar sus metodologías de tiempo de recuperación en caso de desastres para evitar la paralización de sus procesos a través de mecanismos mas efectivos que permitan optimizar el tiempo y así asegurar la continuidad de los procesos de la empresa.

Referencias Bibliográficas:

- CUTIN ZAPATA, Alipio. Análisis y diseño de un plan de seguridad informática en la municipalidad distrital de Canchaque–Piura; 2020.

- SISTI, María Agustina. Seguridad informática. 2019. Tesis Doctoral. Universidad Nacional de Cuyo. Facultad de Ciencias Económicas.

- RODRÍGUEZ PLAZA, William Marcelo. Análisis de vulnerabilidades a nivel de seguridad informática en el parque computacional de Aguapen Ep en el 2016.-1cd. 2016. Tesis Doctoral.

- ANCAJIMA MENDOZA, María Alejandra. Propuesta de implementación de seguridad informática en las tic de la IE San Miguel Arcángel, Catacaos-Piura; 2016. 2019.

- GARCIA VEGA, Ana Rebeca; MORALES BAREN, Dayana Jamileth. Seguridad informática mediante hacking ético en la aplicación de pentesting para el análisis de vulnerabilidades en las redes de datos de la cooperativa SIERRA CENTRO sucursal La Maná, provincia de Cotopaxi. 2022. Tesis de Licenciatura. Ecuador: La Mana: Universidad Técnica de Cotopaxi (UTC).

- GÓMEZ ARCILA, Carolina; MONCAYO VIVEROS, Steven. Sistema de gestión de incidentes de seguridad basado en norma ISO 17799: 2005 aplicado a pequeñas y medianas empresas en Colombia, orientado a sistemas operativos Linux y Windows. 2006.

- KISSEL, Richard (ed.). Glossary of key information security terms. Diane Publishing, 2011.

- Solarte Solarte, F. N., Enriquez Rosero, E. R., & Benavides, M. del C. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. Revista Tecnológica - ESPOL, 28(5). Recuperado a partir de http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456

- GUANÍN MACKENCIE, Cristhian Joel. Sitio web adaptativo para mejorar la gestión de ventas de la Funeraria Guanín del Cantón Quevedo. 2022. Tesis de Licenciatura.

- ESPINOZA ÑAUPARY, Walter Victor; VALLEJOS TORRES, Moises. “Adquisición e Implantación de un Sistema Web Para Mejorar la Gestión de Ventas en la Empresa OSITEC en el Distrito de Independencia el Año 2021. 2023.

- Granados R. (2015) Despliegue y puesta en funcionamiento de componentes software,ICEditorial, España
- Jacobson, I. Booch G, y Rumbaug J. (2006) El lenguaje unificado de modelado UML 2° Ed. Pearson Educación. Madrid España.

- Linares Cambero, D. (2015) Diseño e implementación de un sistema de compra venta, para mejorar el proceso de ventas de la empresa “MEGASERVICE.NET SAC” (tesis pregrado) Universidad Nacional de la Amazonia Peruana. Iquitos, Perú.

- López M y Lobato F. (2006) Operaciones de ventas, Editorial Paraninfo, Madrid España.

- Lujan S. (2002) Programación de aplicaciones web: historia, principios básicos y clientes web, Editorial.

- Club Universitario, Barcelona, España.

- Martinez J. y Rojas F. (2016) Comercio electrónico, Editorial Paraninfo 1° Edición, Madrid España.

- Moliner F. (2005) Grupo A y B de Informática Bloque Especifico Volumen II, Mad, Barcelona, España

Anexo 1. Matriz de consistencia.

PROBLEMA	OBJETIVOS	HIPOTESIS	VARIABLES	DIMENSIÓN	INDICADORES	METODOLOGIA
Problema General ¿Cuál es el estado situacional de la seguridad Informática de la E.P.S. Sedaloreto S.A.? **Problemas Específicos** ¿Cuál es el nivel de riesgo de la seguridad informática de la E.P.S. Sedaloreto S.A.? ¿Cuál es el nivel de vulnerabilidades de la seguridad informática de la E.P.S. Sedaloreto S.A.?	General Evaluar el estado situacional de la seguridad Informática de la E.P.S. Sedaloreto S.A. Específicos Evaluar el nivel de riesgo de la seguridad informática de la E.P.S. Sedaloreto S.A. Evaluar las vulnerabilidades de la seguridad informática de la E.P.S. Sedaloreto S.A.	**Hipótesis General:** .H1: El nivel de seguridad informática de la E.P.S. Sedaloreto S.A. es muy bajo H0: El nivel de seguridad informática de la E.P.S. Sedaloreto S.A. es muy alto	Variable Nivel de Seguridad Informática	Evaluación de Riesgos	% de Riesgo Nivel de Riesgo Tiempo de Recuperación	Tipo de Investigación Descriptiva El diseño de la investigación No Experimental, Transversal El diseño tuvo el siguiente diagrama: M -→ O Población y Muestra Población La población para esta investigación estará conformada por el personal que labora en la oficina de informática de la E.P.S. Sedaloreto S.A. que haciende a 05 personas Muestra .Toda la Población por ser menor a 30 Técnica de Recolección de Datos: La Observación La encuesta Instrumento de Recolección de Datos:
				Análisis de Vulnerabilidades	% Controles implementados % Frecuencia de amenazas o incidentes	

						Ficha de Observación Cuestionario Procedimiento de Recolección de Datos: La Información será procesada en software estadístico, cuyos resultados serán clasificados en cuadros y gráficos estadísticos.

Anexo 2. Carta de Autorización para la evaluación del Nivel de Seguridad Informática de la E.P.S. Sedaloreto S.A.

CARTA DE AUTORIZACIÓN PARA EVALUACIÓN DEL NIVEL DE SEGURIDAD INFORMÁTICA DE LA E.P.S. SEDALORETO S.A.

El que suscribe, **Ing. James Iván Vásquez Acosta**, Jefe de la Oficina de Informática de la E.P.S. Sedaloreto S.A., autoriza a las Bachilleres **KAROLYN HILDA PATRICIA PÉREZ GONZÁLES** y **MELISSA JANE BURGOS FLORES**, para realizar una evaluación del nivel de seguridad informática de la empresa, como parte del desarrollo de sus tesis titulada ANÁLISIS DEL NIVEL DE SEGURIDAD INFORMÁTICA DE LA E.P.S. SEDALORETO S.A.- 2023, en la facultad de Ciencias e Ingeniería, programa académico de Ingeniería de Sistemas de Información.

Iquitos, 09 de Junio del 2023

Atentamente,

Firma y Sello del Jefe

Anexo 3. Fichas de Observación

FICHA PARA MEDIR EL PORCENTAJE DE OCURRENCIAS DEL RIESGO - E.P.S. SEDALORETO S.A.

N°	Riesgo de Seguridad	Probabilidad (0-1)	Impacto (0-1)	Riesgo (Probabilidad x Impacto)
1	Fuga de datos			
2	Ataque de phishing			
3	Falta de parches de seguridad			
4	Políticas de seguridad débiles			
5	Brecha de seguridad			
6	Ataque de DDoS			
7	Contraseñas débiles			
8	Acceso no autorizado			
9	Malware			
10	Auditoría de seguridad deficiente			

FICHA PARA MEDIR EL NIVEL DE RIESGO DE LA SEGURIDAD INFORMÁTICA - E.P.S. SEDALORETO S.A.

N°	Riesgo de Seguridad	Probabilidad	Impacto	Riesgo	Severidad
1	Fuga de datos				
2	Ataque de phishing				
3	Falta de parches de seguridad				
4	Políticas de seguridad débiles				
5	Brecha de seguridad				
6	Ataque de DDoS				
7	Contraseñas débiles				
8	Acceso no autorizado				
9	Malware				
10	Auditoría de seguridad deficiente				

- Crítico: Riesgos que tienen una alta probabilidad y un impacto muy alto, lo que los convierte en amenazas críticas que deben abordarse de inmediato.
- Alto: Riesgos que tienen una alta probabilidad y un impacto alto, lo que los hace significativos y requiere atención.
- Medio: Riesgos con una probabilidad y un impacto moderados, que deben ser gestionados de manera adecuada.
- Bajo: Riesgos con una baja probabilidad y un impacto moderado, que aún requieren supervisión y gestión.
- Muy Bajo: Riesgos con una baja probabilidad y un impacto bajo, que pueden requerir seguimiento ocasional.