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

EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN CON HACKING ÉTICO EN LA MUNICIPALIDAD DISTRITAL DE SAN JUAN BAUTISTA – 2023

PARA OBTAR EL TITÚLO PROFESIONAL

INGENIERO INFORMÁTICO Y DE SISTEMAS

AUTOR:

- **BACH. EDGARD RUBENS RIOS RIOS**

ASESOR:

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

SAN JUAN BAUTISTA – MAYNAS – LORETO - PERÚ – 2023

DEDICATORIA

A Dios quien me da fortaleza espiritual para poder enfrentar las dificultades de la vida, guiarme para ser un profesional de bien, a mi familia por su apoyo incondicional y sacrificio en mi carrera universitaria. a mis padres, a mi hijo **RUBENS WILLIAMS**, Gracias por ser siempre mi impulso para seguir adelante.

BACH. EDGARD RUBENS RIOS RIOS

AGRADECIMIENTO

En primer lugar, agradezco a la Universidad Científica del Perú y a su majestuosa Facultad de Ciencias e Ingeniería para el Programa Académico de Ingeniería de Sistemas e Información y a los catedráticos por compartir sus conocimientos para ser buenos profesionales.

Expreso mi gratitud al Ing. HENRY MANUEL ORELLANA RÍOS, por haberme brindado las facilidades e información para el desarrollo de la presente tesis.

Mi especial y sincero agradecimiento al Ing. RONALD PERCY MELCHOR INFANTES, Mgr. por su apoyo incondicional y motivador en el asesoramiento de la Tesis.

BACH. EDGARD RUBENS RIOS RIOS

"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:

"EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN CON HACKING ÉTICO EN LA MUNICIPALIDAD DISTRITAL DE SAN JUAN BAUTISTA – 2023"

Del alumno: EDGARD RUBENS RIOS RIOS, de la Facultad de Ciencias e Ingeniería, pasó satisfactoriamente la revisión por el Software Antiplagio, con un porcentaje de **21% de similitud.**

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

San Juan, 03 de enero del 2024.

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

CJRA/ri-a
06-2024

Resultados_Tesis - Edgard Rubens Rios Rios_V1

INFORME DE ORIGINALIDAD

21%	19%	4%	11%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	repositorio.ucv.edu.pe Fuente de Internet	3%
2	repositorio.ug.edu.ec Fuente de Internet	2%
3	Submitted to Instituto Superior de Artes, Ciencias y Comunicación IACC Trabajo del estudiante	1%
4	bibdigital.epn.edu.ec Fuente de Internet	1%
5	repositorio.uss.edu.pe Fuente de Internet	1%
6	pt.slideshare.net Fuente de Internet	1%
7	revistas.uniguajira.edu.co Fuente de Internet	1%
8	Submitted to Corporación Universitaria Minuto de Dios, UNIMINUTO Trabajo del estudiante	1%

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:	Edgard Rubens Rios Rios
Título del ejercicio:	Quick Submit
Título de la entrega:	Resultados_Tesis - Edgard Rubens Rios Rios_V1
Nombre del archivo:	Tesis_-_Edgard_Rubens_Rios_Rios.pdf
Tamaño del archivo:	642.45K
Total páginas:	47
Total de palabras:	7,456
Total de caracteres:	40,707
Fecha de entrega:	03-ene.-2024 09:11a. m. (UTC-0500)
Identificador de la entre...	2266413048

RESUMEN

En la tesis se describe la metodología utilizada para llevar a cabo la investigación. Se emplea un enfoque de "investigación/descriptiva" con un diseño no experimental - transaccional, centrándose en analizar y describir el estado actual de la seguridad de la información implementada en la Municipalidad Distrital de San Juan Bautista. Se detalla la población y muestra que serán evaluadas, considerando tanto activos informáticos y componentes físicos y lógicos como el personal que utiliza equipos de cómputo en la municipalidad. La técnica de recolección de datos seleccionada es la encuesta, con un cuestionario estructurado que aborda aspectos clave relacionados con la seguridad de la información y el hacking ético, los resultados obtenidos a partir de los objetivos planteados. Se analizan las vulnerabilidades y amenazas específicas a las que se enfrenta la Municipalidad Distrital de San Juan Bautista en términos de seguridad de la información, clasificando activos críticos y niveles de riesgo por componentes, asimismo, se analiza la implementación de controles, revelando un bajo promedio total del 0.2%, lo que sugiere áreas de mejora en políticas y prácticas de seguridad en la municipalidad. Se identifican riesgos por dominios, con niveles de riesgo para diferentes pruebas de hacking ético, en relación con la conciencia y capacitación en ciberseguridad del personal municipal, se destaca un nivel razonable de conocimiento, 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 resaltan 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.

FACULTAD DE CIENCIAS E INGENIERÍA

UNIVERSIDAD CIENTÍFICA DEL PERÚ

ACTA DE SUSTENTACIÓN DE TESIS

FACULTAD DE CIENCIAS E INGENIERÍA

Con Resolución Decanal N° 703-2023-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. Lee Frank Mendoza López. Mtro. — Miembro
- Lic. Carlos Enrique Marthans Ruiz, Mgr. — Miembro

Como Asesor: Ing. Ronald Melchor Infantes, Mtro.

En la ciudad de Iquitos, siendo las 9:00 am del día jueves 25 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 ***EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN CON HAKING ÉTICO EN LA MUNICIPALIDAD DISTRITAL DE SAN JUAN BAUTISTA*** Presentado por el Sustentante **RIOS RIOS EDGARD RUBENS**

Como requisito para optar el título profesional de: **INGENIERO INFORMÁTICO Y DE SISTEMAS**

Luego de escuchar la sustentación y formuladas las preguntas las que fueron: ABSUELTAS
El Jurado después de la deliberación en privado llegó a la siguiente conclusión
Que la sustentación es APROBADA POR MAYORIA

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

Ing. Jimmy Max Ramírez Villacorta, Mtro
Presidente

Ing. Lee Frank Mendoza López. Mtro
Miembro

Lic. Carlos Enrique Marthans Ruiz, Mgr
Miembro

UNIVERSIDAD CIENTÍFICA DEL PERÚ

HOJA DE APROBACIÓN

PROGRAMA ACADÉMICO DE INGENIERÍA INFORMÁTICA Y DE SISTEMAS

TESISTA: RIOS RIOS EDGARD RUBENS

Tesis sustentada en acto publico el día jueves 25 de enero del 2024, a las 9:00 am , en las instalaciones de la UNIVERSIDAD CIENTÍFICA DEL PERÚ.

. JIMMY MAX RAMÍREZ VILLACORTA, MTRO.
PRESIDENTE DE JURADO

. ING. LEE FRANK MENDOZA LÓPEZ. MTRO
.MIEMBRO DE JURADO

LIC. CARLOS ENRIQUE MARTHANS RUIZ, MGR.
MIEMBRO DE JURADO

ING. RONALD MELCHOR INFANTES
ASESOR

INDICE DE CONTENIDO

Página

INDICE DE TABLAS

Página

INDICE DE FIGURAS

Página

RESUMEN

En la tesis se describe la metodología utilizada para llevar a cabo la investigación. Se emplea un enfoque de "Investigación Descriptiva" con un diseño no experimental - transeccional, centrándose en analizar y describir el estado actual de la seguridad de la información implementada en la Municipalidad Distrital de San Juan Bautista, Se detalla la población y muestra que serán evaluadas, considerando tanto activos informáticos y componentes físicos y lógicos como el personal que utiliza equipos de cómputo en la municipalidad. La técnica de recolección de datos seleccionada es la encuesta, con un cuestionario estructurado que aborda aspectos clave relacionados con la seguridad de la información y el hacking ético, los resultados obtenidos a partir de los objetivos planteados. Se evalúan las vulnerabilidades y amenazas específicas a las que se enfrenta la Municipalidad Distrital de San Juan Bautista en términos de seguridad de la información, destacando activos críticos y niveles de riesgo por componentes, asimismo, se analiza la implementación de controles, revelando un bajo promedio total del 6.2%, lo que sugiere áreas de mejora en políticas y prácticas de seguridad en la municipalidad. Se identifican riesgos por ataques, con niveles de riesgo para diferentes pruebas de hacking ético, en relación con la conciencia y capacitación en ciberseguridad del personal municipal, se destaca un nivel razonable de conocimiento, 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 resaltan 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 claves: hacking ético, seguridad de la información, municipalidad.

ABSTRACT

The thesis describes the methodology used to conduct the research. A "Descriptive Research" approach is employed with a non-experimental - cross-sectional design, focusing on analyzing and describing the current state of information security implemented in the District Municipality of San Juan Bautista. The population and sample to be evaluated are detailed, considering both computer assets and physical and logical components, as well as the personnel using computing equipment in the municipality. The selected data collection technique is a survey, utilizing a structured questionnaire addressing key aspects related to information security and ethical hacking. The results are obtained from the set objectives, Specific vulnerabilities and threats faced by the District Municipality of San Juan Bautista in terms of information security are assessed, highlighting critical assets and risk levels by components. Additionally, the implementation of controls is analyzed, revealing a low overall average of 6.2%, suggesting areas for improvement in municipality security policies and practices, Risks from attacks are identified, with risk levels for different ethical hacking tests, related to the awareness and cybersecurity training of municipal staff. A reasonable level of knowledge is emphasized, although opportunities for improvement in understanding key concepts are identified. Most have received information security training in the last 12 months, mainly through in-person courses, and the majority rates the training as effective, the conclusions underscore the importance of addressing critical assets, improving control implementation, and strengthening staff awareness. Specific recommendations are proposed, such as the implementation of security measures, regular risk assessments, and ongoing training programs.

Keywords: ethical hacking, information security, municipality.

CAPÍTULO I.- MARCO TEÓRICO:

1.1 Antecedentes de Estudio:

✓ Antecedentes Internacionales:

Bravo, Gabriela & Barrera Fernando (2020), El presente proyecto de tesis enfocado en la auditoría de seguridad informática, UTM PFSENSE y un correlacionado de eventos SIEM, ha identificado la presencia de vulnerabilidades en los sistemas de información de algunas empresas. Estas vulnerabilidades se originan principalmente debido a la desactualización de servicios como APACHE y la existencia de puertos abiertos que podrían permitir conexiones remotas no autorizadas, entre otros factores críticos, para abordar este problema, se ha diseñado un marco teórico conceptual que explora diversos conceptos clave relacionados con la seguridad informática, como el Sistema de Información y Gestión de Eventos de Seguridad (SIEM), auditorías de seguridad informática, procesos de Ethical Hacking, intranets, extranets, topologías físicas y lógicas, entre otros, en la propuesta tecnológica, se han definido los recursos necesarios en términos técnicos, operativos, económicos y legales para implementar soluciones efectivas. El proyecto incluye los resultados de la investigación, los entregables esperados, los criterios de validación de la propuesta, así como el procesamiento y análisis de los datos recopilados, para finalizar, se ha desarrollado una matriz que detalla la aceptación del producto, describiendo los criterios y alcances del proyecto. Este análisis concluye con las principales conclusiones y recomendaciones derivadas de la investigación, destinadas a mejorar la seguridad informática y

abordar las vulnerabilidades identificadas en las empresas estudiadas.

Huacon, Heyner (2022), Con la ejecución de este proyecto de investigación titulado "Análisis de Vulnerabilidades en la Seguridad de la Información y su Impacto en el Departamento de Sistemas del Municipio de Babahoyo", se busca abordar la problemática relacionada con las vulnerabilidades y sus efectos en el departamento de sistemas del Municipio de Babahoyo. El objetivo primordial de este estudio es optimizar la prestación de servicios, garantizando que sean eficientes y actualizados para satisfacer las metas establecidas para una gran cantidad de usuarios que utilizan estos servicios diariamente, esta investigación adopta un enfoque descriptivo para comprender la verdadera naturaleza de los desafíos que enfrenta el departamento de sistemas. Se obtiene información relevante a través de encuestas y preguntas dirigidas a los usuarios, lo que aporta datos necesarios para el análisis y la identificación de problemas e incongruencias. Como parte de las soluciones propuestas, se contempla la implementación de un escáner de vulnerabilidades con el fin de elevar la calidad de los servicios ofrecidos.

- ✓ **Antecedentes Nacionales:**

Piñasca, Roger (2022), El propósito de este estudio es evaluar las técnicas de hacking ético en el ámbito de la seguridad informática, con el objetivo de identificar vulnerabilidades en la Municipalidad Distrital de Los Olivos, ubicada en Lima. Esta investigación se enmarca en un enfoque cuantitativo y un diseño no experimental. La población de estudio comprende las ocho técnicas de hacking ético más comúnmente utilizadas, mientras

que la muestra se limita a tres de ellas: el ataque de denegación de servicio (DDOS), el escaneo de puertos y el ataque por fuerza bruta, la primera etapa del estudio involucró un análisis exhaustivo de las vulnerabilidades presentes en los servidores seleccionados como parte de la muestra. En este proceso, se recopiló información sobre los puertos y protocolos utilizados para identificar los servicios en funcionamiento. Es importante destacar que se llevó a cabo en colaboración con un equipo autorizado que tenía acceso directo a toda la red, los resultados obtenidos en este análisis revelaron la existencia de múltiples vulnerabilidades en la infraestructura informática actual de la Municipalidad de Los Olivos. Estas deficiencias se hicieron evidentes tanto en su configuración lógica como física, lo que la hace vulnerable a posibles ataques. Además, la evaluación del sistema indicó que el servidor se encontraba activo, como se corroboró durante el escaneo del host. El análisis también señaló que se registraron variadas latencias en diferentes direcciones IP, y se identificó que varios puertos se encontraban cerrados, en el transcurso de la investigación, se identificaron un total de seis vulnerabilidades, siendo CVE-2007-6750 la más predominante entre ellas. Estos hallazgos subrayan la necesidad urgente de mejorar la seguridad informática en la Municipalidad de Los Olivos para mitigar riesgos y fortalecer su infraestructura tecnológica.

Eche Jorge, Lizano, Anyi (2022), El propósito de esta investigación fue la mejora de la gestión de riesgos en Tecnologías de la Información (TI) en la Municipalidad de Sechura, a través de la implementación de medidas de seguridad de la información. Para alcanzar este objetivo, se empleó la metodología de Seguridad Cero, que consta de seis fases distintas: Reconocimiento, Escaneo, Enumeración, Análisis,

Explotación y Reporte, en el contexto de una investigación de tipo cuantitativa y un diseño experimental de tipo preexperimental relacionado con pruebas pre y post, se desarrolló la variable dependiente denominada "gestión de riesgos". La población de estudio abarcó un total de 300 equipos informáticos, incluyendo servidores, sistemas operativos, programas y equipos de cómputo. La muestra se conformó con 25 equipos informáticos, y se recopilaron datos a través de un cuestionario, los resultados obtenidos revelaron la identificación del cien por ciento de los riesgos, lo que incluyó un total de 28 vulnerabilidades y 11 amenazas. Posteriormente, se realizó un análisis que implicó calcular el nivel de riesgo mediante una multiplicación que generó valores numéricos en un rango de 0 a 10. Además, se evaluaron los niveles de probabilidad e impacto, que se categorizaron como muy alta, alta, moderada, baja y muy baja. Los hallazgos indicaron la existencia de 7 riesgos con un nivel de probabilidad y impacto muy alto, 13 riesgos de nivel alto, 7 riesgos de nivel moderado y 1 riesgo de nivel bajo, como último paso, se ofrecieron alternativas de solución con el propósito de fortalecer la seguridad en la Municipalidad de Sechura. Estas soluciones tienen como objetivo mitigar los riesgos identificados y mejorar la gestión de riesgos de TI en la institución.

- ✓ **Antecedentes Locales:**

No se encontraron antecedentes locales.

1.2 Bases Teóricas:

- **Seguridad de la información:**

La seguridad de la información es un conjunto de prácticas, políticas, procedimientos y tecnologías diseñadas para proteger la información de

una organización, garantizando su confidencialidad, integridad y disponibilidad. Su objetivo es prevenir y mitigar amenazas y riesgos que puedan comprometer la información, ya sea almacenada electrónicamente o en otros formatos. Esto implica salvaguardar los datos de acceso no autorizado, alteraciones no deseadas o pérdidas, ya sea por factores humanos o tecnológicos.

La seguridad de la información es esencial en la era digital, ya que la información es un activo crítico para organizaciones y personas. Garantiza que los datos sean manejados de manera segura y que los sistemas estén protegidos contra amenazas cibernéticas y físicas.

Este campo se apoya en una variedad de prácticas y estándares, como ISO 27001, que proporciona un marco para la gestión de la seguridad de la información. La seguridad de la información es un concepto amplio que abarca áreas como la gestión de riesgos, la protección de datos, la ciberseguridad, la continuidad del negocio y la educación y concientización en seguridad, entre otros.

La seguridad de la información es un campo multidisciplinario que se enfoca en la protección de la confidencialidad, integridad y disponibilidad de la información. Su objetivo principal es salvaguardar los datos y sistemas de cómputo contra amenazas internas y externas, así como garantizar que la información esté protegida de accesos no autorizados, alteraciones no deseadas y pérdidas, con el fin de asegurar que la información esté disponible y sea útil cuando sea necesario.

- **Componentes Clave de la Seguridad de la Información:**

- Confidencialidad: La confidencialidad asegura que la información solo esté disponible para personas o entidades autorizadas. Se refiere a la protección de datos sensibles de divulgación no autorizada.

- Integridad: La integridad garantiza que la información no se altere de manera no autorizada. Implica que los datos permanezcan precisos y consistentes a lo largo del tiempo.

- Disponibilidad: La disponibilidad se refiere a la accesibilidad y utilización de la información cuando sea necesaria. Los sistemas y datos deben estar disponibles de manera oportuna y fiable.

- Autenticación y Autorización: La autenticación se utiliza para verificar la identidad de los usuarios, mientras que la autorización controla el acceso a recursos en función de los permisos otorgados.

- Gestión de Riesgos: La gestión de riesgos se centra en identificar, evaluar y mitigar las amenazas y vulnerabilidades que pueden afectar la seguridad de la información.

- **Normativas y Estándares Relevantes:**

- ISO/IEC 27001: Un estándar internacional para la gestión de la seguridad de la información.

- GDPR (Reglamento General de Protección de Datos): Una regulación de la Unión Europea que establece normas para la protección de datos personales.

- HIPAA (Ley de Portabilidad y Responsabilidad del Seguro Médico): Una regulación en los Estados Unidos que establece estándares para la protección de la información médica.

- NIST (Instituto Nacional de Estándares y Tecnología): Publica estándares y pautas de seguridad informática ampliamente reconocidos.

- **Importancia de la Seguridad de la Información:**

  La seguridad de la información es fundamental en un mundo digital, ya que la información es un activo crítico para organizaciones y personas. La falta de seguridad puede resultar en la exposición a amenazas cibernéticas, pérdida de datos, daños a la reputación y costos significativos. La protección de la información es esencial para garantizar la confianza y la continuidad de las operaciones.

- **Hacking Ético:**

  Según la perspectiva de Astudillo (2017), su relevancia radica en la defensa integral contra todas las amenazas, ya que el propósito fundamental del Hacking Ético es salvaguardar los sistemas de información de las organizaciones y repeler cualquier tipo de amenaza.

  Por otra parte, según lo expresado por Astudillo (2017), el Hacking Ético persigue la evaluación de las posibles amenazas a las que los sistemas pueden estar sujetos a través de prácticas destinadas a analizar la seguridad de elementos como bases de datos, redes y aplicaciones, entre otros.

  La finalidad del hacking ético radica en emplear el conocimiento informático de manera ética para identificar y solucionar posibles vulnerabilidades, contribuyendo así a fortalecer la seguridad de una organización antes de que un potencial atacante pueda.

Pruebas del Hacking Ético:

A nivel organizacional las pruebas se organizan en tres fases:

- Preparación: Definición del acuerdo formal y alcance. Firma de confidencialidad.

- Evaluación de seguridad: El proceso en sí de simulación del ataque.

- Conclusión: Informe técnico y ejecutivo de las operaciones realizadas, vulnerabilidades localizadas y medidas de corrección y/o mitigación.

1.3 Definición de Términos Básicos:

- **Protección de la Confidencialidad:** La seguridad de la información garantiza que los datos confidenciales se mantengan protegidos contra accesos no autorizados. Esto es crucial para proteger información sensible, como datos personales, secretos comerciales y propiedad intelectual.

- **Integridad de los Datos:** La integridad de los datos asegura que la información no se altere de manera no autorizada. Evita la corrupción de datos y garantiza que la información sea precisa y confiable.

- **Disponibilidad de la Información:** La seguridad de la información también se centra en la disponibilidad de los datos y sistemas. Esto significa que la información esté disponible y sea accesible cuando sea necesaria, lo que es esencial para la continuidad de las operaciones.

- **Cumplimiento Legal y Regulatorio:** Muchas leyes y regulaciones requieren que las organizaciones protejan la información de sus clientes y empleados. No cumplir con estas regulaciones puede resultar en sanciones legales y financieras significativas.

- **Protección Contra Amenazas Cibernéticas:** En un entorno digital, las amenazas cibernéticas, como malware, ataques de hackers y phishing, son comunes. La seguridad de la información ayuda a prevenir y mitigar estos riesgos.

- **Confianza del Cliente:** La seguridad de la información es crucial para mantener la confianza de los clientes. Las empresas que protegen adecuadamente la información de sus clientes ganan una reputación de confiabilidad y responsabilidad.

- **Protección de la Reputación:** Una violación de la seguridad de la información puede dañar la reputación de una organización. La pérdida de datos o la falta de seguridad puede llevar a la pérdida de clientes y daños a la imagen de la empresa.

- **Reducción de Costos:** La inversión en seguridad de la información puede ayudar a prevenir incidentes costosos, como brechas de seguridad. A largo plazo, la seguridad adecuada puede ahorrar dinero y recursos.

- **Respaldo de la Continuidad del Negocio:** La seguridad de la información es esencial para garantizar la continuidad de las operaciones en caso de desastres o incidentes. Los planes de recuperación y respaldo son parte integral de la seguridad de la información.

- **Protección de Activos Críticos:** La información es uno de los activos más críticos para muchas organizaciones. La seguridad de la información asegura la protección de este activo vital.

CAPÍTULO II.- PLANTEAMIENTO DEL PROBLEMA:

2.1 Descripción del Problema:

La evaluación de la seguridad de la información con el enfoque del hacking ético en la Municipalidad Distrital de San Juan Bautista en 2023 plantea una serie de desafíos y consideraciones significativas en el ámbito de la ciberseguridad tales como escasez de Conciencia de Seguridad que es uno de los problemas comunes en muchas organizaciones, incluyendo municipalidades, es la falta de conciencia de seguridad. El personal puede no comprender completamente las amenazas cibernéticas y cómo mitigarlas. Esto puede llevar a una exposición significativa a riesgos de seguridad, datos sensibles ya que las municipalidades manejan una gran cantidad de datos sensibles, como información fiscal, datos personales y financieros de los ciudadanos. La falta de seguridad en la protección de estos datos puede tener consecuencias graves en términos de privacidad y confidencialidad, vulnerabilidades desconocidas donde a menudo, las organizaciones estatales no son conscientes de las vulnerabilidades presentes en su infraestructura de TI, los hackers éticos pueden identificar agujeros de seguridad desconocidos que podrían ser explotados por actores maliciosos, con existe cumplimiento Normativo, las municipalidades suelen estar sujetas a regulaciones y leyes específicas en cuanto a la protección de datos y la seguridad de la información. No cumplir con estas regulaciones puede resultar en sanciones financieras y daño a la reputación, falta de capacitación, el personal puede carecer de capacitación en seguridad cibernética, lo que aumenta la probabilidad de cometer errores que podrían ser explotados por ciberdelincuentes, amenazas emergentes la evolución constante de las amenazas cibernéticas significa que las municipalidades deben estar preparadas para hacer frente a nuevas formas de ataques, como el ransomware, el phishing y las

vulnerabilidades en aplicaciones web, presupuesto limitado, las municipalidades a menudo enfrentan restricciones presupuestarias, lo que puede dificultar la implementación de medidas de seguridad cibernética efectivas, evaluación o auditorias inadecuada, la evaluación de seguridad periódica es esencial para identificar y abordar vulnerabilidades. La falta de evaluaciones regulares puede dejar la puerta abierta a riesgos no detectados, falta de aplicación de políticas y procedimientos: La falta de políticas de seguridad y procedimientos bien definidos puede dificultar la respuesta eficaz ante incidentes de seguridad, para abordar estos desafíos, es fundamental realizar evaluaciones de seguridad de manera regular, implementar políticas y procedimientos de seguridad cibernética, y proporcionar capacitación en seguridad al personal.

2.2 Formulación del Problema:

2.2.1 Problema General:

- ✓ ¿Cuál es el estado actual de la seguridad de la información en la Municipalidad Distrital de San Juan Bautista en 2023?

2.2.2 Problemas Específicos:

- ✓ ¿Cuáles son las vulnerabilidades y amenazas específicas a las que se enfrenta la Municipalidad Distrital de San Juan Bautista en cuanto a la seguridad de la información?
- ✓ ¿Qué prácticas y políticas de seguridad de la información se aplican actualmente en la municipalidad, y son efectivas en la protección de datos y sistemas?

- ✓ ¿Cuál es el nivel de conciencia y capacitación en ciberseguridad del personal de la municipalidad, y en qué medida influye en la seguridad de la información?

2.3 Objetivos:

2.3.1 Objetivo General:

- ✓ Evaluar con hacking ético el estado actual de la seguridad de la información de la Municipalidad Distrital de San Juan Bautista en el Periodo 2023.

2.3.2 Objetivos Específicos:

- ✓ Evaluar las vulnerabilidades y amenazas específicas a las que se enfrenta la Municipalidad Distrital de San Juan Bautista en cuanto a la seguridad de la información.
- ✓ Evaluar que prácticas y políticas de seguridad de la información se aplican actualmente en la municipalidad, y son efectivas en la protección de datos y sistemas.
- ✓ Evaluar el nivel de conciencia y capacitación en ciberseguridad del personal de la municipalidad, y en qué medida influye en la seguridad de la información.

2.4 Hipótesis:

- No Aplica.

2.5 Variables:

2.5.1 Identificación de Variables:

- **Variable 1:** Seguridad de la información con hacking ético

2.5.2 Definición Conceptual de las Variables:

- **Definición Conceptual de las Variables:**

Variable	Definición Conceptual	Definición Operacional
Seguridad de la información con hacking ético	La seguridad de la información con hacking ético se refiere a la práctica de evaluar y fortalecer la protección de los datos y sistemas informáticos de una organización o entidad mediante el uso de técnicas y enfoques similares a los utilizados por hackers maliciosos, pero con la intención de identificar y corregir vulnerabilidades en lugar de explotarlas.	Realización de pruebas técnicas sistemáticas y controladas en los sistemas de información, incluyendo redes, aplicaciones, servidores y bases de datos, con el objetivo de identificar posibles vulnerabilidades.

2.5.3 Operacionalización de las Variables:

Tabla N° 01.- Operacionalización de variables:

Variables	Dimensiones	Indicadores	Instrumento de recolección de Datos
Seguridad de la información con hacking ético	Vulnerabilidades y amenazas específicas	Nivel de criticidad de los activos informáticos	Documental, Ficha de Observación, Encuesta
		Nivel de riesgo por componentes	
		Nivel de riesgo por ataques	
	Prácticas y políticas de seguridad de la información	% Implementación	
	Nivel de conciencia y capacitación	% de Evaluación	

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 en la Municipalidad Distrital de San Juan Bautista.

- **Diseño de la Investigación:**

  El diseño de investigación es no experimental - transeccional, porque se ha analizado el nivel de la seguridad informática con hacking ético de la municipalidad distrital de San Juan Bautista.

  Teniendo la siguiente representación gráfica:

  $$M \rightarrow O$$

  Donde M es la muestra de los procesos de seguridad de la información y O la observación del nivel o estado de la seguridad informática con Hacking ético.

3.2 Población y Muestra:

- **Población:**

  Para la evaluación con Hacking ético se analizará los activos informáticos y lo componentes físicos y lógicos, controles y políticas de seguridad de la información de la Municipalidad Distrital de San Juan Bautista.
  Para la encuesta la población para esta investigación estará conformada por el personal que labora y hace uso de un equipo de cómputo en la Municipalidad Distrital de San Juan Bautista.

- **Muestra:**

  Para la evaluación con Hacking ético se analizará 9 activos informáticos y 7 componentes físicos y lógicos, 15 controles y políticas de seguridad de la información de la Municipalidad Distrital de San Juan Bautista.
  Para la encuesta la muestra es finita y estará compuesta por 30 personas, que serán seleccionadas de manera no probabilística por conveniencia.

  Para lo cual se obtuvo mediante la siguiente formula:

  asumimos un nivel de confianza del 95% (lo que corresponde a un Z de aproximadamente 1.96 para una distribución normal estándar), un margen de error del 5%, y no tienes una estimación precisa de la proporción (p), podríamos usar un valor conservador de p=0.5.

  Simplificando la fórmula, puedes despejar N (tamaño de la población total) de la siguiente manera:

$$N = \frac{n \times E^2 + Z^2 \times p \times (1-p)}{Z^2 \times p \times (1-p)}$$

Sustituyendo los valores conocidos, obtenemos:

$$N = \frac{30 \times (0.05)^2 + (1.96)^2 \times 0.5 \times (1-0.5)}{(1.96)^2 \times 0.5 \times (1-0.5)}$$

Calculando esto nos dio el tamaño mínimo de la población total necesaria para tener una muestra de 30 personas con un nivel de confianza del 95% y un margen de error del 5%.

3.3 Técnicas, instrumentos y procedimientos de recolección de datos:

- **Técnica de Recolección de Datos:**

La técnica de recolección de datos seleccionada para evaluar la seguridad de la información con enfoque en hacking ético en la Municipalidad Distrital de San Juan Bautista es la encuesta. La encuesta permitirá recopilar información de manera estructurada y cuantificable, abordando diversas áreas relevantes para la seguridad informática y la ética en el hacking.

La encuesta consistirá en un conjunto de preguntas estructuradas que abarcan aspectos clave relacionados con la seguridad de la información, el hacking ético y las prácticas de seguridad en la Municipalidad. Se utilizarán preguntas cerradas para facilitar el análisis cuantitativo de los datos, así como preguntas abiertas para permitir a los participantes proporcionar información adicional y detallada.

- **Instrumento de Recolección de Datos:**

  El instrumento de recolección de datos será el cuestionario de la encuesta. Este cuestionario contendrá preguntas que aborden áreas específicas, como la conciencia de seguridad, políticas de seguridad, pruebas de penetración, conformidad con normativas, respuesta a incidentes, ética en hacking, herramientas y tecnologías utilizadas, colaboración y comunicación, conciencia de los empleados y evaluación de riesgos.

  El cuestionario se diseñará de manera clara y concisa, asegurándose de abordar los objetivos de la evaluación y de ser comprensible para los participantes. Se incluirán escalas de Likert.

- **Procedimiento de Recolección de Datos:**

- **Preparación del Cuestionario:** Se diseñará un cuestionario detallado basado en los objetivos de la evaluación y las áreas de interés, asegurándose de incluir preguntas específicas relacionadas con la seguridad de la información y el hacking ético.

- **Piloto de la Encuesta:** Se realizará un piloto con un grupo reducido de personas para identificar posibles problemas en las preguntas y garantizar la claridad y comprensión del cuestionario.

- **Distribución de la Encuesta:** El cuestionario se distribuirá a los empleados relevantes de la Municipalidad Distrital de San

Juan Bautista. Se proporcionarán instrucciones claras sobre cómo completar la encuesta.

- **Recopilación de Datos:** Una vez completada la encuesta por los participantes, se recopilarán los datos para su posterior análisis. Se garantizará la confidencialidad de las respuestas para fomentar la honestidad y la participación.

- **Análisis de Datos:** Los datos recopilados se analizarán de manera cuantitativa y cualitativa, identificando patrones, tendencias y áreas de mejora en relación con la seguridad de la información y el hacking ético en la Municipalidad.

- **Informe de Resultados:** Se preparará un informe detallado que presente los resultados de la encuesta, destacando hallazgos significativos, áreas de fortaleza y recomendaciones para mejorar la seguridad informática, con especial énfasis en el hacking ético, en la Municipalidad Distrital de San Juan Bautista.

3.4 Procesamiento y análisis de datos:

La Información se procesó en software estadístico SPSS Versión 27, cuyos resultados se clasificaron en cuadros y gráficos estadísticos.

CAPÍTULO IV.- RESULTADOS:

- ✓ **Resultados Objetivo 01:** Evaluar las vulnerabilidades y amenazas específicas a las que se enfrenta la Municipalidad Distrital de San Juan Bautista en cuanto a la seguridad de la información.

- Variable: Seguridad de la información con hacking ético.
  Dimensión: Vulnerabilidades y amenazas específicas.
  Indicador: Nivel de criticidad de los activos informáticos.

Tabla N° 02.- Nivel de criticidad de los activos informáticos:

Tipo de activo	Activo	Nivel de criticidad
Datos / Información	Datos del contribuyente (Predio, datos personales)	ALTO
	Datos de proveedores (contratistas, personal, compras)	ALTO
	Datos de solicitudes de servicio para el ciudadano	BAJO
	Datos biométricos del personal	BAJO
	Datos de imagen	BAJO
Servicios	Página web (informativa)	BAJO
Software / Aplicaciones Informáticas	Clarisa y Melisa (Sistema Administrativo)	BAJO
	SIAF	MEDIO
	SGTM	MEDIO
	Sistema de Trámite documentario	BAJO
	Sistema biométrico	BAJO
	Windows Server 2008 / Windows 10	BAJO

	SQL 2012	ALTO
	Navegador web (Mozilla y Google Chrome)	BAJO
	Microsoft Office 2013	BAJO
Equipos Informáticos	Computadoras personales	BAJO
	Impresora convencional	BAJO
	Servidor (4 rackeables y 3 torres)	ALTO
	Plotters	BAJO
	Ticketera	BAJO
	Router Microtik	MEDIO
Redes de Comunicación	Fibra Óptica (internet)	MEDIO
	Cableado RJ45 (red)	MEDIO
Soporte de información	Disco duro externo	ALTO
	Disco SAS	MEDIO
	CD y DVD	BAJO
	USB (8 gb, 16gb, 32 gb)	BAJO
Equipamiento auxiliar	Aire acondicionado	BAJO
	Ventilador	BAJO
	UPS	BAJO
	Estabilizador	BAJO
	Supresor de pico	BAJO
Personal	Director del área OITC	MEDIO
	Soporte técnico	BAJO
	Especialista de red y sistemas	MEDIO
Instalaciones	Oficina de Informática de Tecnología y Comunicaciones	ALTO

Fuente: Elaboración Propia

LEYENDA

CRITICIDAD	
ALTO	El activo implicado es imprescindible para los procesos de la organización.
MEDIO	El activo implicado involucra un riesgo medio los principios de la seguridad de la información.
BAJO	El activo implicado es requerido, pero ocupa un riesgo bajo en cuanto a los principios de la seguridad de la información.

- Variable: Seguridad de la información con hacking ético.
  Dimensión: Vulnerabilidades y amenazas específicas.
  Indicador: Nivel de riesgo por componentes.

Tabla N° 03.- Nivel de riesgo por componentes:

Centro de datos										
Amenazas	**Probabilidad**	**Degradación**			**Impacto**			**Estimación del riesgo**		
		DC	**D I**	**DD**	**IC**	**II**	**ID**	**RC**	**RI**	**RD**
Daño por agua	3	1	1	4	D	D	C	Bajo	Bajo	Alto
Avería de origen físico o lógico	2	1	1	4	D	D	C	Bajo	Bajo	Medio
Corte del suministro eléctrico	4	1	1	4	D	D	C	Bajo	Bajo	Alto
Errores del administrador	2	2	2	4	MO	MO	C	Medio	Medio	Medio
Errores de mantenimiento / actualización de	2	1	1	3	D	D	C	Bajo	Bajo	Medio

equipos (hardware)										
Caída del sistema por agotamiento de recursos	2	1	1	4	D	D	C	Bajo	Bajo	Medio
Suplantación de la identidad del usuario	3	3	3	1	C	C	D	Alto	Alto	Bajo
Abuso de privilegios de acceso	2	3	3	2	C	C	MO	Medio	Medio	Medio
Red Cableada										
Amenazas	**Probabilidad**	**Degradación**			**Impacto**			**Estimación del riesgo**		
		DC	**D I**	**DD**	**IC**	**II**	**ID**	**RC**	**RI**	**RD**
Fallo de servicios de comunicaciones	2	1	1	4	D	D	C	Bajo	Bajo	Medio
Errores del administrador	2	1	2	4	D	ME	C	Bajo	Bajo	Medio
Fugas de información	2	3	1	1	MO	D	D	Medio	Bajo	Bajo
Caída del sistema por agotamiento de recursos	2	1	1	3	D	D	MO	Bajo	Bajo	Medio
Suplantación de la identidad del usuario	3	3	3	1	MO	MO	D	Medio	Medio	Bajo
Abuso de privilegios de acceso	2	3	3	3	MO	MO	MO	Medio	Medio	Medio
Divulgación de información	2	2	1	1	ME	D	D	Bajo	Bajo	Bajo

Red Inalámbrica										
Amenazas	**Probabilidad**	**Degradación**			**Impacto**			**Estimación del riesgo**		
		DC	**D I**	**DD**	**IC**	**II**	**ID**	**RC**	**RI**	**RD**
Fallo de servicios de comunicaciones	2	1	1	3	D	D	MO	Bajo	Bajo	Medio
Errores del administrador	2	1	2	3	D	ME	MO	Bajo	Bajo	Medio
Alteración accidental de la información	2	1	3	1	D	MO	D	Bajo	Medio	Bajo
Fugas de información	2	2	1	1	ME	D	D	Bajo	Bajo	Bajo
Caída del sistema por agotamiento de recursos	2	1	1	4	D	D	C	Bajo	Bajo	Medio
Suplantación de la identidad del usuario	3	2	2	1	ME	ME	D	Bajo	Bajo	Bajo
Abuso de privilegios de acceso	2	3	3	3	MO	MO	MO	Medio	Medio	Medio
Divulgación de información	2	2	1	1	ME	D	D	Bajo	Bajo	Bajo
Equipos Servidores										
Amenazas	**Probabilidad**	**Degradación**			**Impacto**			**Estimación del riesgo**		
		DC	**IC**	**II**	**IC**	**II**	**IC**	**RC**	**RI**	**RD**
Daño por agua	3	1	1	4	D	D	C	Bajo	Bajo	Alto
Avería de origen físico o lógico	2	1	1	3	D	D	C	Bajo	Bajo	Medio

Corte de suministro eléctrico	4	1	1	4	D	D	C	Bajo	Bajo	Alto
Errores de los usuarios	2	3	3	3	C	C	C	Medio	Medio	Medio
Errores del administrador	2	3	3	4	C	C	C	Medio	Medio	Medio
Errores de configuración	2	1	4	1	D	C	D	Bajo	Medio	Bajo
Escapes de información	2	3	1	1	C	D	D	Medio	Bajo	Bajo
Alteración accidental de la información	2	1	3	1	D	C	D	Bajo	Bajo	Bajo
Fugas de información	2	2	1	1	MO	D	D	Medio	Bajo	Bajo
Errores de mantenimiento/actualización de equipo (hardware)	2	1	1	4	D	D	C	Bajo	Bajo	Medio
Errores de mantenimiento/actualización de equipo (software)	2	1	3	3	D	C	C	Bajo	Medio	Medio
Caída del sistema por agotamiento de recursos	2	1	1	4	D	D	C	Bajo	Bajo	Medio
Suplantación de la identidad del usuario	3	3	3	1	C	C	D	Alto	Alto	Bajo

Abuso de privilegios de acceso	2	3	3	3	C	C	C	Medio	Medio	Medio
Divulgación de la información	2	2	1	1	MO	D	D	Medio	Bajo	Bajo
Manipulación de equipos	2	4	1	4	C	D	C	Medio	Bajo	Medio
Equipos de escritorio										
Amenazas	**Probabilidad**	**Degradación**			**Impacto**			**Estimación de riesgo**		
		DC	**D I**	**DD**	**IC**	**II**	**IC**	**RC**	**RI**	**RD**
Daños por agua	3	1	1	4	D	D	C	Bajo	Bajo	Alto
Avería de origen físico o lógico	2	1	1	4	D	D	C	Bajo	Bajo	Medio
Corte del suministro eléctrico	4	1	1	4	D	D	C	Bajo	Bajo	Alto
Errores del administrador	2	3	3	4	MO	MO	C	Medio	Medio	Medio
Errores de configuración	2	1	3	1	D	MO	D	Bajo	Medio	Bajo
Escapes de información	2	3	1	1	ME	D	D	Medio	Bajo	Bajo
Fugas de información	2	1	2	1	D	ME	D	Bajo	Bajo	Bajo
Errores de mantenimiento/actualización de equipo (hardware)	2	1	1	4	D	D	C	Bajo	Bajo	Medio
Errores de mantenimiento/ac	2	1	2	3	D	ME	MO	Bajo	Bajo	Medio

tualización de equipo (software)										
Caída del sistema por agotamiento de recursos	2	1	1	4	D	D	C	Bajo	Bajo	Medio
Abuso de privilegios de acceso	2	2	3	3	ME	MO	MO	Bajo	Medio	Medio
Manipulación de los equipos	2	3	1	3	MO	D	MO	Medio	Bajo	Medio
Oficina de Informática y Telecomunicaciones										
Amenazas	**Probabilidad**	**Degradación**			**Impacto**			**Estimación de riesgo**		
		DC	**D I**	**DD**	**IC**	**II**	**IC**	**RC**	**RI**	**RD**
Daños por agua	3	1	1	2	D	D	ME	Bajo	Bajo	Bajo
Alteración accidental de la información	2	1	2	1	D	ME	D	Bajo	Bajo	Bajo
Fugas de información	2	3	1	1	MO	D	D	Medio	Bajo	Bajo
Divulgación de información	2	3	1	1	MO	D	D	Medio	Bajo	Bajo
Local Municipal										
Amenazas	**Probabilidad**	**Degradación**			**Impacto**			**Estimación de riesgo**		
		DC	**D I**	**DD**	**IC**	**II**	**IC**	**RC**	**RI**	**RD**
Daños por agua	3	1	1	2	D	D	MO	Bajo	Bajo	Medio
Alteración accidental de la información	2	1	2	1	D	MO	D	Bajo	Medio	Bajo
Fugas de información	2	2	1	1	MO	DE	DE	Medio	Bajo	Bajo

Divulgación de información	2	2	1	1	MO	DE	DE	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**

DEGRADACIÓN

Degradación del valor	Valor
Sin degradación (SD)	1
Bajo (B)	2
Medio (M)	3
Alto (A)	4

IMPACTO

Impacto	Abreviatura	Descripción
Despreciable	D	• No daña la seguridad de la municipalidad. • No perjudica la imagen de la municipalidad antes las partes interesadas. • Produce reprocesos ordinarios. • La información se puede restaurar con la misma cantidad
Menor	ME	• No daña la seguridad de la municipalidad.

		• Perjudica en menor grado la imagen de la municipalidad ante las partes interesadas. • Produce reprocesos menores. • La información se puede restaurar en un tiempo intermedio con la misma calidad
Moderado	MO	• Daña en menor nivel la seguridad de la municipalidad. • Afecta levemente la imagen de la municipalidad ante las partes interesadas. • Genera reprocesos moderados. • La información se puede restaurar sin embargo no en su estado original.
Critico	C	• Perjudica en mayor nivel la seguridad de la información de la municipalidad. • Daña en su mayoría la imagen de la municipalidad ante las partes interesadas. • Produce reprocesos críticos. • Es complicado restaurar la información

El análisis de las vulnerabilidades y amenazas específicas revela el nivel de criticidad de los activos informáticos de la Municipalidad Distrital de San Juan Bautista. Se identificaron activos críticos, como datos del contribuyente y proveedores, con un alto nivel de criticidad. Además, se evaluaron los riesgos por componentes, destacando amenazas como daño por agua, averías físicas o lógicas, corte de suministro eléctrico, errores del administrador, entre otros.

- ✓ **Resultados Objetivo 02:** Evaluar que prácticas y políticas de seguridad de la información se aplican actualmente en la municipalidad, y son efectivas en la protección de datos y sistemas.

- Variable: Seguridad de la información con hacking ético.
  Dimensión: Prácticas y políticas de seguridad de la información.
  Indicador: % de Implementación de controles.

Tabla N° 04.- Implementación de controles:

Nombre	Implementación (%)
Políticas de seguridad de la información	0
Organización de la seguridad de la información	18%
Seguridad en los Recursos Humanos	5%
Gestión de activos	3%
Control de Accesos	9%
Cifrado	0
Seguridad Física y Ambiental	18%
Seguridad en las Operaciones	13%
Seguridad en las Telecomunicaciones	12%
Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información	0
Relación con proveedores	0
Gestión de incidentes en la seguridad de la información	10%
Aspectos de seguridad de la información en la gestión de la continuidad del negocio	0
Cumplimiento	0
Promedio total de implementación de controles	6.2%

Fuente: Elaboración Propia

- Variable: Seguridad de la información con hacking ético.
  Dimensión: Prácticas y políticas de seguridad de la información.
  Indicador: Nivel de riesgo por ataques.

Tabla N° 05.- Nivel de riesgo por ataques:

Ítem	Evaluación	Tipo de Riesgo
1	Enumerar aplicaciones en el servidor web Moderada	Moderada
2	Revisar los comentarios y metadatos de la página web para detectar fugas de información	Importante
3	Marco de aplicación web de huellas digitales	Moderada
4	Aplicación web de huellas digitales	Importante
5	Pruebas de XSS reflejados	Moderada
6	Pruebas de XSS almacenados	Moderada
7	Prueba para inyección SQL	Importante
8	Prueba de fugas HTML	Moderada
9	Prueba de secuencias de comandos XSS basadas en DOM	Tolerable
10	Prueba de ejecución de JavaScript	Tolerable
11	Prueba de inyección HTML	Tolerable
12	Prueba de redireccionamiento de URL del lado del cliente	Tolerable

Fuente: Elaboración Propia

Interpretación: 3 de los 12 tipos de evaluación de ataque han sido considerados con riesgo moderada, 3 de los 12 han sido considerado como riesgo importante 4 de los 12 han sido considerado con riesgo tolerable.

La implementación de controles en diferentes áreas revela un promedio total de implementación del 6.2%. Esta baja implementación sugiere áreas de mejora en políticas de seguridad, organización, gestión de activos, control de accesos, entre otros. Además, se evaluaron riesgos por ataques, identificando niveles de riesgo para diversas pruebas de hacking ético. Es crucial abordar estas vulnerabilidades y fortalecer las prácticas de seguridad para proteger eficientemente la información.

- ✓ **Resultados Objetivo 03:** Evaluar el nivel de conciencia y capacitación en ciberseguridad del personal de la municipalidad, y en qué medida influye en la seguridad de la información.

- Variable: Seguridad de la información con hacking ético.
- Dimensión: Nivel de conciencia y capacitación.
- Indicador: Porcentaje de Evaluación

Tabla N° 06.- Estadísticos descriptivos del nivel de conciencia y capacitación:

Pregunta 1: ¿Cómo definiría usted la "seguridad de la información"?

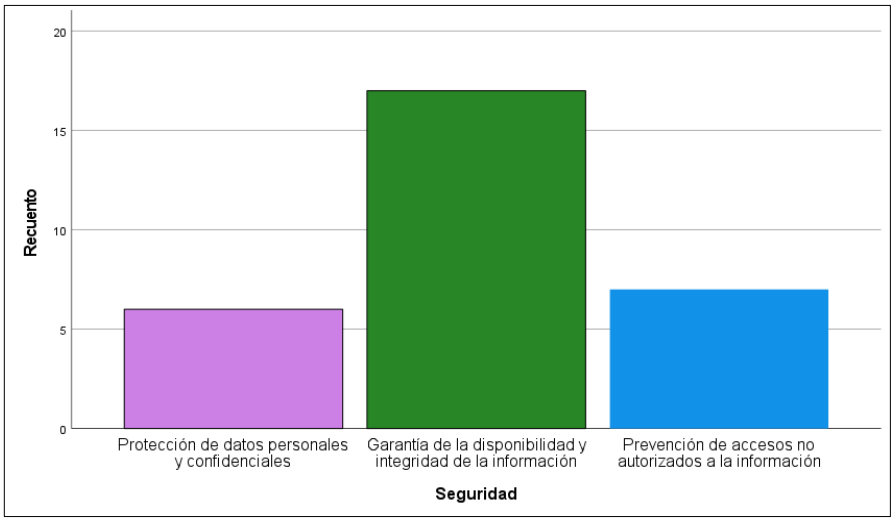
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuestas	Protección de datos personales y confidenciales	6	20,0	20,0	20,0
	Garantía de la disponibilidad e integridad de la información	17	56,7	56,7	76,7

	Prevención de accesos no autorizados a la información	7	23,3	23,3	100,0
	Total	30	100,0	100,0	

Fuente: Elaboración Propia

Figura N° 01.- Estadísticos descriptivos del nivel de conciencia y capacitación:

Pregunta 1: ¿Cómo definiría usted la "seguridad de la información"?



Fuente: Elaboración Propia

Tabla N° 07.- Estadísticos descriptivos del nivel de conciencia y capacitación:

Pregunta 2: ¿Qué riesgos relacionados con la seguridad de la información identifica en su entorno laboral?

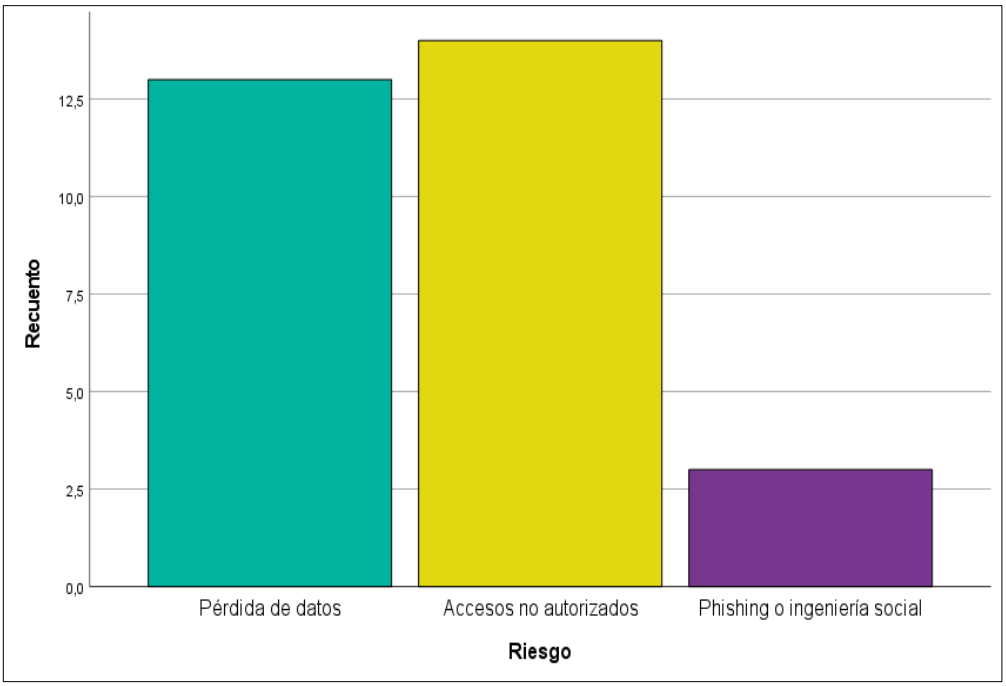
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Pérdida de datos	13	43,3	43,3	43,3

	Accesos no autorizados	14	46,7	46,7	90,0
	Phishing o ingeniería social	3	10,0	10,0	100,0
	Total	30	100,0	100,0	

Fuente: Elaboración Propia

Figura N° 02.- Estadísticos descriptivos del nivel de conciencia y capacitación:

Pregunta 2: ¿Qué riesgos relacionados con la seguridad de la información identifica en su entorno laboral?



Fuente: Elaboración Propia

Tabla N° 08.- Estadísticos descriptivos del nivel de conciencia y capacitación:

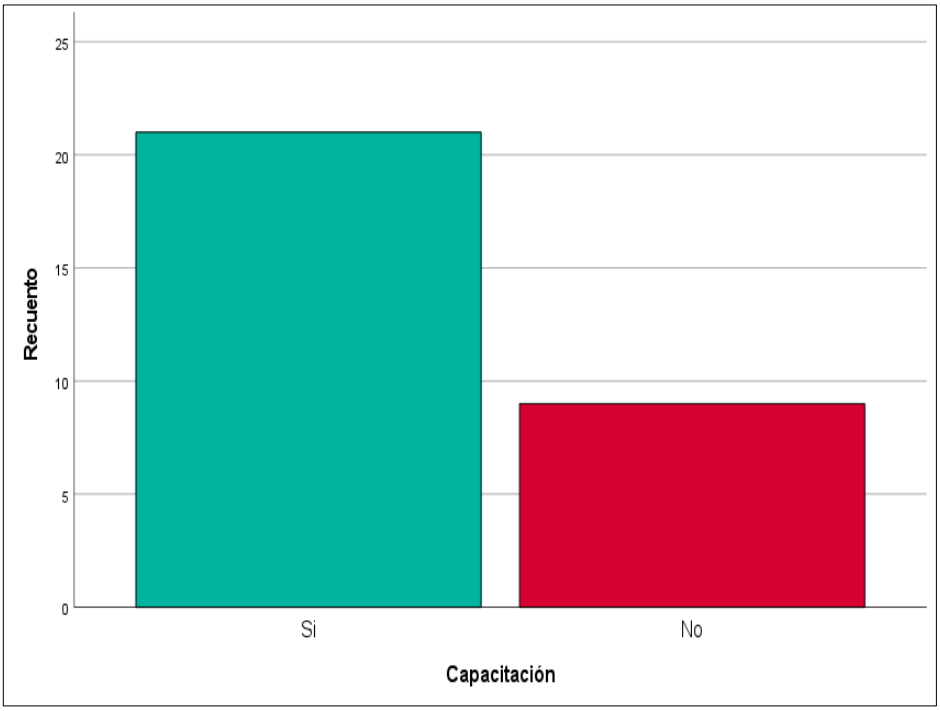
Pregunta 3: ¿Ha recibido alguna capacitación en seguridad de la información en los últimos 12 meses?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Si	21	70,0	70,0	70,0
	No	9	30,0	30,0	100,0
	Total	30	100,0	100,0	

Fuente: Elaboración Propia

Figura N° 03.- Estadísticos descriptivos del nivel de conciencia y capacitación:

Pregunta 3: ¿Ha recibido alguna capacitación en seguridad de la información en los últimos 12 meses?



Fuente: Elaboración Propia

Tabla N° 09.- Estadísticos descriptivos del nivel de conciencia y capacitación:

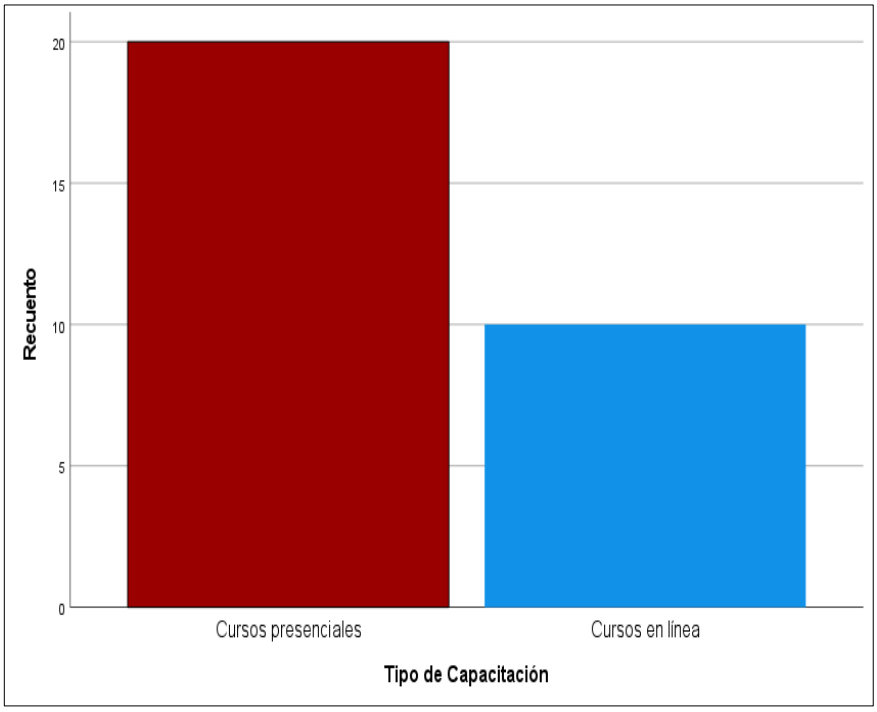
Pregunta 4: tipo de capacitación que ha recibido

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Cursos presenciales	20	66,7	66,7	66,7
	Cursos en línea	10	33,3	33,3	100,0
	Total	30	100,0	100,0	

Fuente: Elaboración Propia

Figura N° 04.- Estadísticos descriptivos del nivel de conciencia y capacitación:

Pregunta 4: tipo de capacitación que ha recibido



Fuente: Elaboración Propia

Tabla N° 10.- Estadísticos descriptivos del nivel de conciencia y capacitación:

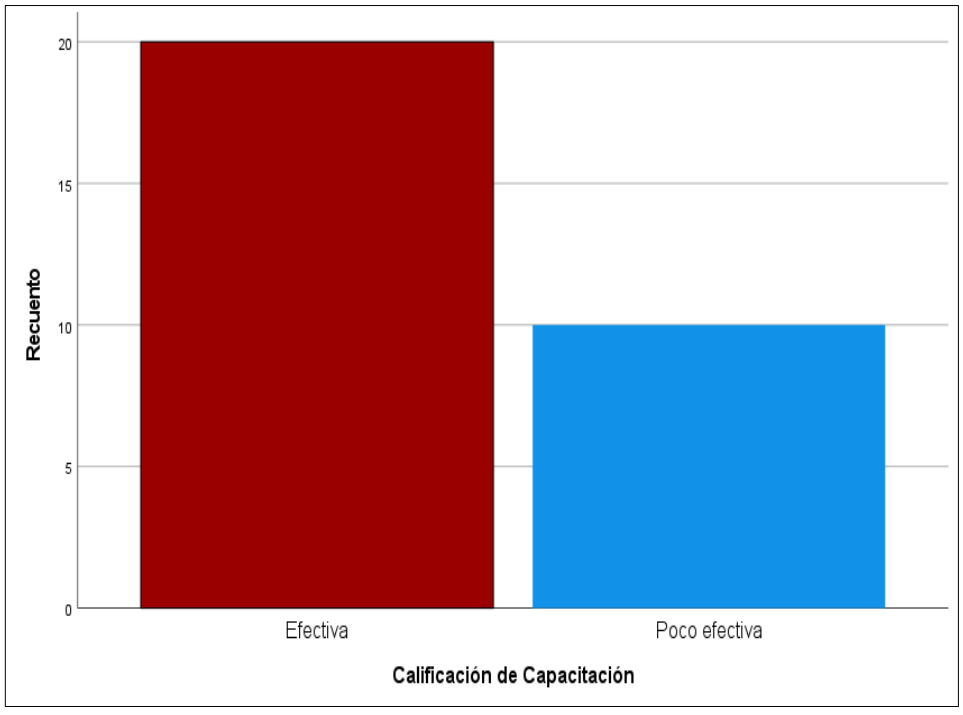
Pregunta 5: ¿Cómo calificaría la eficacia de la capacitación recibida en seguridad de la información?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Efectiva	20	66,7	66,7	66,7
	Poco efectiva	10	33,3	33,3	100,0
	Total	30	100,0	100,0	

Fuente: Elaboración Propia

Figura N° 05.- Estadísticos descriptivos del nivel de conciencia y capacitación:

Pregunta 5: ¿Cómo calificaría la eficacia de la capacitación recibida en seguridad de la información?



Fuente: Elaboración Propia

La evaluación del nivel de conciencia y capacitación revela que la mayoría de los participantes define la seguridad de la información como la protección de datos personales y confidenciales. Se identificaron riesgos percibidos, como la pérdida de datos, accesos no autorizados y phishing. La mayoría de los encuestados 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. Este resultado indica un nivel razonable de conciencia, pero aún existen oportunidades para fortalecer la capacitación y abordar riesgos percibidos.

CAPÍTULO V.- DISCUSIÓN:

- En la evaluación de vulnerabilidades y amenazas específicas, se identificó un conjunto de activos críticos con un alto nivel de criticidad para la Municipalidad Distrital de San Juan Bautista. Esta información proporciona una visión detallada de los riesgos a los que se enfrenta la infraestructura informática y los datos sensibles. La presencia de activos críticos, como los datos del contribuyente y proveedores, resalta la importancia de implementar medidas de seguridad robustas en estos sectores. Las amenazas evaluadas, como daño por agua, errores del administrador y cortes de suministro eléctrico, proporcionan información clave para priorizar las estrategias de mitigación.

- La implementación de controles reveló un bajo promedio total del 6.2%, indicando un área de mejora sustancial en las prácticas y políticas de seguridad de la información en la municipalidad. Es crucial abordar este hallazgo, ya que la baja implementación de controles puede dejar a la organización vulnerable a diversas amenazas. La discusión sobre los riesgos identificados por ataques, con niveles de riesgo para diferentes pruebas de hacking ético, destaca la necesidad de fortalecer las prácticas de seguridad. Se recomienda una revisión exhaustiva de las políticas de seguridad, así como la implementación de controles específicos en áreas críticas, como la gestión de activos y el control de accesos. Este análisis proporciona un marco claro para mejorar la postura de seguridad de la municipalidad.

- La evaluación del nivel de conciencia y capacitación reveló un conocimiento razonable sobre seguridad de la información entre los empleados de la municipalidad. Sin embargo, el análisis de las respuestas indica oportunidades para mejorar la comprensión de

conceptos clave, como la definición de seguridad de la información. La mayoría de los encuestados ha recibido capacitación en seguridad en los últimos 12 meses, lo cual es positivo. La preferencia por cursos presenciales destaca la importancia de la interactividad en el proceso de aprendizaje. La percepción general de la efectividad de la capacitación es positiva, pero es esencial realizar ajustes y personalizar los programas según las necesidades específicas identificadas en la encuesta.

CAPÍTULO VI.- CONCLUSIONES:

- La evaluación de vulnerabilidades destaca activos críticos con un alto nivel de criticidad, lo que resalta la necesidad de fortalecer las medidas de seguridad.

- La implementación de controles revela un bajo promedio total, indicando áreas de mejora en políticas y prácticas de seguridad en la municipalidad.

- Los resultados de conciencia y capacitación muestran un nivel razonable, pero aún hay oportunidades para fortalecer la conciencia y abordar riesgos percibidos.

CAPÍTULO VII.- RECOMENDACIONES:

- Implementar medidas de seguridad específicas para los activos críticos identificados.

- Fortalecer las políticas de seguridad, organización, gestión de activos y control de accesos.

- Realizar evaluaciones periódicas de riesgos y pruebas de hacking ético para mantener una postura proactiva.

- Continuar con programas de capacitación en seguridad de la información, considerando la modalidad en línea para mayor alcance.

- Monitorear constantemente el nivel de conciencia y realizar ajustes en la capacitación según las necesidades identificadas.

CAPÍTULO VIII.- REFERENCIAS BIBLIOGRÁFICAS:

- **PIÑASHCA HUERTA, ROGER JOEL (2022).** Evaluación de técnicas de hacking ético para analizar la seguridad informática de la municipalidad distrital de los Olivos. Lima.

- **BRAVO INDACOCHEA, GABRIELA ELIZABETH & BARRERA LANDIRES, FERNANDO AARÓN (2020).** Auditoría de seguridad informática en la red de datos de una empresa utilizando como mecanismo de hacking ético el sistema operativo kali linux previo a la propuesta de implementación del firewall PFSENSE y correlacionador de eventos SIEM. Tesis Doctoral. Universidad de Guayaquil. Facultad de Ciencias Matemáticas y Físicas. Carrera de Ingeniería en Networking y Telecomunicaciones.

- **HUACON LÓPEZ, HEYNER JOEL (2022).** Vulnerabilidades de la seguridad de la información y su incidencia en el departamento de sistemas del Municipio de Babahoyo. Tesis de Licenciatura. Babahoyo: UTB-FAFI.

- **ECHE PINGO, JORGE LUIS & LIZANO MENDOZA, ANYI EXMIT (2022-2023).** Implementación de seguridad de la información para mejorar la gestión de riesgos de TI en la Municipalidad de Sechura.

- **BORJA, A. I. (2018).** Auditoria de sistemas informáticos en la Empresa Alfatv Cable S.A. dedicada al área de telecomunicaciones en Quito para Quito.

- **CAD, D. J. (2019).** Tecnología Didáctica sobre Seguridad Informática en Formación Profesional. Valladolid-España. López, R.

- **ZAMORA (2018).** Prevención de ataques de Ransomware conocidos en redes informáticas, utilizando la tecnología Check Point Sandblast en el perímetro y en usuarios finales comprendido en el periodo de septiembre del 2017 a abril del 2018. Párraga, C.

ANEXOS:

Anexo 1.- Matriz de consistencia:

PROBLEMA	OBJETIVOS	HIPOTESIS	VARIABLES	DIMENSIÓN	INDICADORES	METODOLOGIA
Problema General ¿Cuál es el estado actual de la seguridad de la información en la Municipalidad Distrital de San Juan Bautista en 2023? **Problema Específicos** ¿Cuáles son las vulnerabilidades y amenazas específicas a las que se enfrenta la Municipalidad Distrital de San Juan Bautista en	**General** Evaluar con hacking ético el estado actual de la seguridad de la información de la Municipalidad Distrital de San Juan Bautista en el Periodo 2023. **Específicos** Evaluar las vulnerabilidades y amenazas específicas a las que se enfrenta la Municipalidad Distrital	No Aplica	Variable: Seguridad de la información con hacking ético.	Vulnerabilidades y amenazas específicas.	Nivel de criticidad de los activos informáticos.	* Tipo de Investigación: - Descriptivo. * El diseño de la investigación: - El diseño de la presente investigación es no experimental de tipo transeccional. * Población y Muestra: - Población: - Para la evaluación con Hacking ético se analizará los activos informáticos y lo
					Nivel de riesgo por componentes.	
					Nivel de riesgo por ataques.	
				Prácticas y políticas de seguridad de la información.	% Implementación.	
				Nivel de conciencia y capacitación.	% de Evaluación.	

cuanto a la seguridad de la información? ¿Qué prácticas y políticas de seguridad de la información se aplican actualmente en la municipalidad, y son efectivas en la protección de datos y sistemas? ¿Cuál es el nivel de conciencia y capacitación en ciberseguridad del personal de la municipalidad, y en qué medida influye en la seguridad de la información?	de San Juan Bautista en cuanto a la seguridad de la información. Evaluar que prácticas y políticas de seguridad de la información se aplican actualmente en la municipalidad, y son efectivas en la protección de datos y sistemas. Evaluar el nivel de conciencia y capacitación en ciberseguridad del personal de la municipalidad, y en qué medida influye en la seguridad de la información.					componentes físicos y lógicos, controles y políticas de seguridad de la información de la Municipalidad Distrital de San Juan Bautista. - Para la encuesta la población para esta investigación estará conformada por el personal que labora y hace uso de un equipo de cómputo en la Municipalidad Distrital de San Juan Bautista. Muestra - Para la evaluación con Hacking ético se analizará 9 activos informáticos y 7 componentes físicos y lógicos, 15 controles y

						políticas de seguridad de la información de la Municipalidad Distrital de San Juan Bautista. - Para la encuesta la muestra es finita y estará compuesta por 30 personas, que serán seleccionadas de manera no probabilística por conveniencia. * Técnica de Recolección de Datos: - Revisión documental. - Identificación de Estratos. - Entrevista. * Instrumento de Recolección de Datos: - Ficha de Observación.

						* Procedimiento de Recolección de Datos: - La Información será procesada en software estadístico, cuyos resultados serán clasificados en tablas estadísticos.

Anexo 2.- Documento de aceptación de la evaluación:

CARTA DE AUTORIZACIÓN

EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN CON HACKING ÉTICO EN LA MUNICIPALIDAD DISTRITAL DE SAN JUAN BAUTISTA – 2023

El que suscribe, Ing. Henry Manuel Orellana Ríos, director de la oficina de informática y telecomunicaciones de la Municipalidad Distrital de San Juan Bautista, autoriza al Bachiller **EDGARD RUBENS RIOS RIOS**, para realizar una EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN CON HACKING ÉTICO, como parte del desarrollo de su tesis titulada "**EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN CON HACKING ÉTICO EN LA MUNICIPALIDAD DISTRITAL DE SAN JUAN BAUTISTA – 2023**", en la facultad de Ciencias e Ingeniería, programa académico de Ingeniería de Sistemas de Información.

San Juan Bautista, 13 de octubre del 2023

Atentamente,

Anexo 3.- Cuestionario para medir el nivel de conciencia y capacitación:

Cuestionario Para Evaluar el Nivel de Conciencia y Capacitación en Seguridad de la Información

Sección 1: Información Demográfica.

1.1. Nombre del Participante: _____

1.2. Cargo/Ocupación: _____

1.3. Tiempo en la Organización: _____

Sección 2: Nivel de Conciencia en Seguridad de la Información.

2.1. ¿Cómo definiría usted la "seguridad de la información"?

Protección de datos personales y confidenciales. ☐

Garantía de la disponibilidad y integridad de la información. ☐

Prevención de accesos no autorizados a la información. ☐

2.2. ¿Qué riesgos relacionados con la seguridad de la información identifica en su entorno laboral?

Pérdida de datos. ☐

Accesos no autorizados. ☐

Phishing o ingeniería social. ☐

Sección 3: Capacitación en Seguridad de la Información.

3.1. ¿Ha recibido alguna capacitación en seguridad de la información en los últimos 12 meses?

Sí ☐

No ☐

3.2. En caso afirmativo, indique el tipo de capacitación que ha recibido:

Cursos presenciales. ☐

Cursos en línea. ☐

Talleres prácticos. ☐

No estoy seguro. ☐

3.3. ¿Cómo calificaría la eficacia de la capacitación recibida en seguridad de la información?

Muy efectiva. ☐

Efectiva. ☐

Poco efectiva. ☐

No puedo evaluar. ☐